



PhD-FDEF-2023-007

The Faculty of Law, Economics and Finance

The Faculty of Law

DISSERTATION

Defence held on 29/03/2023 in Luxembourg

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG
EN DROIT

AND

DOCTOR IN LAW

by

FLORENCE D'ATH

Born on 18 October 1989 in Braine l'Alleud (Belgique)

THE GENERAL DATA PROTECTION REGULATION:
A MULTI-FUNCTIONAL FRAMEWORK FOR THE
DEFENCE OF THE RIGHTS AND FREEDOMS OF DATA
SUBJECTS IN THE DIGITAL SPHERE

Dissertation defence committee

Dr Jörg Gerkrath, dissertation supervisor
Professor, Université du Luxembourg

Dr Maja Brkan, dissertation co-supervisor
Professor, Maastricht University

Dr Mark Cole, Chairman
Professor, Université du Luxembourg

Dr Paolo Balboni
Professor, Maastricht University

Dr Eleni Kosta
Professor, Tilburg University

Dr Orla Lynskey,
Professor, London School of Economics and Political Sciences

Dr Joanna Mendes,
Professor, Université du Luxembourg

Acknowledgments

I would like to express my deepest gratitude to my main supervisor, Prof. Gerkrath, for his continuous guidance and unfailing *bienveillance*, as well as to my co-supervisor, Judge Brkan, for sharing her deep insight into this study and fruitful advice these last four years.

I would also like to express my deepest appreciation to Prof. Cole and Prof. Balboni for their critical and stimulating feedback, as well as for their trust and encouragements throughout this project. My gratitude also goes to Prof. Eleni Kosta and Prof. Orla Lynskey who have kindly accepted to share their expertise to assess my work and be part of my jury.

I would further like to thank Maximilian Schrems, Romain Robert, Stefano Rossetti, Marco Blocher and the entire staff of *noyb* for their warm welcome in Vienna and for having shared their incredible knowledge on GDPR enforcement with me. Part of this thesis is definitely your business.

Finally, I would like to thank my colleagues Frédérique Boulanger, Andrii Hubai and Arron McArdle, as well as all my friends and family, for having endured my weird passion for data protection, for having unapologetically challenged my opinions during our innumerable discussions, and for having provided me with their phenomenal support and affection when I needed it the most. I could not have done it without you.

TABLE OF CONTENT

ABOUT THIS STUDY	9
A. LIST OF ABBREVIATIONS	9
B. BACKGROUND OF THIS STUDY.....	11
C. RESEARCH QUESTION	17
D. SCOPE OF THIS STUDY	18
E. METHODOLOGY.....	21
F. SCIENTIFIC AND SOCIETAL RELEVANCE.....	23
G. STRUCTURE.....	25
INTRODUCTION – THE EVOLUTION OF DATA PROCESSING PRACTICES AND THEIR IMPACT ON THE FUNDAMENTAL RIGHTS AND FREEDOMS OF DATA SUBJECTS	28
A. TERMINOLOGY	29
B. FROM ATOMS TO BITS AND FROM BITS TO ATOMS: UNDERSTANDING THE EXPONENTIAL IMPACT OF DATA PROCESSING PRACTICES ON FUNDAMENTAL RIGHTS.....	33
C. THE NATURE AND EXTENT OF THE IMPACT OF DATA PROCESSING PRACTICES ON FUNDAMENTAL RIGHTS	35
CHAPTER 1 – THE MULTI-FUNCTIONALITY OF THE GDPR FOR THE PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS: A HYPOTHESIS.....	42
1.1. OVERVIEW OF THE NOTION OF ‘EFFECTIVENESS OF THE LAW’	42
1.1.1. <i>Effectiveness in the legal jargon</i>	42
1.1.2. <i>The narrow, broad and wide approach to the effectiveness of the law</i>	43
1.1.3. <i>A goal-oriented approach to legal effectiveness</i>	46
1.1.4. <i>The internal and external factors of legal effectiveness</i>	47
1.2. BEYOND EFFECTIVENESS: DISCUSSION ON THE ‘FUNCTIONALITY’ OF THE LAW	50
1.2.1. <i>Conceptualising ‘legal functionality’: a sui generis definition</i>	51
1.2.2. <i>The factors of legal functionality: focus on the design and the tools of the law</i>	53
1.2.3. <i>Functionality as a sub-category of legal effectiveness</i>	54
1.3. THE GDPR AS A MULTI-FUNCTIONAL FRAMEWORK FOR THE DEFENCE OF FUNDAMENTAL RIGHTS.....	56
1.3.1. <i>A theoretical multi-functionality arising from the ambitious fundamental rights objective of EU data protection law</i>	56
1.3.2. <i>Testing the multi-functionality of EU data protection law in practice: a limited assessment framework</i>	59
CHAPTER 2 – ORIGIN, DEVELOPMENT AND FULFILMENT OF THE FUNDAMENTAL RIGHTS OBJECTIVE OF EU DATA PROTECTION LAW	63
2.1. BACK TO THE ORIGIN OF EU DATA PROTECTION LAW: A FRAMEWORK AT THE SERVICE OF PRIVACY.....	64
2.1.1. <i>A brief overview of the career of the right to privacy from the Hippocratic Oath to the Charter of Fundamental Rights</i>	64
2.1.1.1. The emergence of a right to privacy on the European continent	64
2.1.1.2. Privacy as a human right in international EU treaties	66
2.1.1.3. Privacy as a human right in European treaties.....	69
2.1.2. <i>Pioneering European laws regulating the processing of personal data</i>	72
2.1.3. <i>The internationalisation of data protection law in the 80s as a response to globalisation and digitalisation</i>	80
2.1.3.1. The 1980 OECD Guidelines: reconciling the need to protect privacy with the need to allow the free flow of personal data	80
2.1.3.2. Convention 108 of the Council of Europe: confirmation of the need to ensure the protection of privacy of individuals in the context of data processing	83
2.1.4. <i>Emergence of EU data protection law at the EU level: the 1995 Data Protection Directive</i> ⁸⁶	

2.1.4.1.	The Fundamental Rights Objective of the 1995 Data Protection Directive	87
2.1.4.2.	The transposition of the 1995 Data Protection Directive by Member States and its lack of enforcement ⁸⁹	
2.1.5.	<i>Concluding remark: since its origin, EU data protection law has been conceived as a tool to protect data subjects' fundamental rights, and in particular their right to privacy</i>	91
2.2.	EU DATA PROTECTION LAW IN THE 21ST CENTURY: A FRAMEWORK AT THE SERVICE OF THE FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION	95
2.2.1.	<i>The 'unveiling' of the fundamental nature of the right to personal data protection</i>	95
2.2.2.	<i>The reasons behind the inclusion of Article 8 in the Charter</i>	99
2.2.2.1.	Official reasons behind the inclusion of Article 8 in the Charter	99
2.2.2.2.	Unofficial reasons behind the inclusion of Article 8 in the Charter	104
2.2.3.	<i>Wording, content and scope of the fundamental right to personal data protection</i>	102
2.2.3.1.	Analysis of the Wording of Article 8 of the Charter	107
2.2.3.2.	Analysis of the content of Article 8 of the Charter	108
2.2.3.3.	Analysis of the scope of Article 8 of the Charter and of its overlap with the right to privacy	111
2.2.4.	<i>Preliminary conclusion: the recognition of a fundamental right to personal data protection triggered a shift within the FRO of EU data protection law</i>	117
2.3.	OVERVIEW ON THE FULFILMENT OF THE FUNDAMENTAL RIGHTS OBJECTIVE OF EU DATA PROTECTION LAW	118
2.3.1.	<i>Pre-Lisbon era: interpretation of EU data protection law mainly for the benefit of the right to privacy</i>	118
2.3.1.1.	Rundfunk (2003) – a missed opportunity to exploit the functionality of EU data protection law	119
2.3.1.2.	Lindqvist (2003) – the right to privacy of individuals in the context of blogging	121
2.3.1.3.	Promusicae (2008) – Article 8 of the Charter as a mere cosmetic source	124
2.3.1.4.	Satamedia (2008) – the limits of journalistic freedom in light of the right to privacy	125
2.3.1.5.	Huber (2008) – early evidence of the secondary functionality of EU data protection law	127
2.3.2.	<i>Lisbon era: EU data protection law at the service of Article 7 and 8 of the Charter</i>	129
2.3.2.1.	Volker und Markus Schecke and Eifert (2010) – the coupling of Article 7 and 8 of the Charter	130
2.3.2.2.	Deutsche Telekom (2011) – the start of the emancipation of Article 8 of the Charter	133
2.3.2.3.	Digital Rights Ireland (2014) – evidence of the independent yet connected nature of Article 7 and 8 of the Charter	134
2.3.2.4.	The Schrems saga (2015 – 2020) – additional evidence of the secondary functionality of EU data protection law	138
2.3.3.	<i>GDPR era: towards a more multi-functional use of EU data protection law?</i>	142
2.3.3.1.	Telecommunication surveillance cases in the UK, France and Belgium	142
2.3.3.2.	Facebook Ireland and Others – a reasoning articulated around the broad FRO of EU data protection law	144
2.3.4.	<i>Concluding remarks: understanding the potential causes behind the shortfall in the secondary functionality of EU data protection law</i>	147
2.3.4.1.	Overview of the fulfilment of the FRO of EU data protection law within the case law of the CJEU	147
2.3.4.2.	The national roots of the shortfall of the secondary functionality of EU data protection law	152
2.3.4.3.	Potential causes behind the shortfall of the secondary functionality of EU data protection law	154

CHAPTER 3 – OUTLINING THE MAIN FACTORS OF FUNCTIONALITY OF THE GDPR FOR THE DEFENCE OF DATA SUBJECTS' FUNDAMENTAL RIGHTS AND FREEDOMS157

3.1.	FIRST STRUCTURAL PILLAR OF FUNCTIONALITY OF THE GDPR: A BROAD MATERIAL, PERSONAL AND TERRITORIAL SCOPE	158
3.1.1.	<i>The Material Scope of the GDPR, or the so-called "law of everything"</i>	158
3.1.1.1.	The broad notion of 'processing' and its effect on the functionality of EU data protection law	159
3.1.1.2.	The extensible notion of (special categories of) personal data and its effect on the functionality of data protection law	164
3.1.1.3.	Limitations to the material scope of the GDPR as a way to respect the prerogatives of Member States and balance diverging rights and interests	187
3.1.1.4.	Concluding remarks: the objective and technology-neutral approach to the notion of 'personal data' and of 'processing' as factors of functionality of EU data protection law	195
3.1.2.	<i>The territorial scope of the GDPR, or the law which applies 'everywhere'</i>	197
3.1.3.	<i>The personal scope of the GDPR, or the law which concerns 'everyone'</i>	202
3.1.3.1.	Data subjects as right holders – "data relate to me, therefore I am"	202
3.1.3.2.	Controllers and processors as duty bearers – "I process data, therefore I must"	204

3.1.3.3.	Supervisory authorities as enforcers – “data are being processed, therefore we are competent”	215
3.1.4.	<i>The dialogue between EU secondary and primary law and its effect on the overall scope of EU data protection law</i>	218
3.1.5.	<i>Concluding remarks: the broad material, territorial and personal scope of the GDPR as structural factors of functionality for the defence of data subjects’ rights and freedoms</i>	227
3.2.	SECOND PILLAR OF THE FUNCTIONALITY OF THE GDPR: ITS SET OF PRINCIPLES, RIGHTS AND OBLIGATIONS	230
3.2.1.	<i>First Panel of the PRO Triptych: the key-principles of personal data processing</i>	231
3.2.1.1.	General overview of the key-principles of data processing	231
3.2.1.2.	The factors of functionality of the key-principles of data processing: human-centric approach, interpretative flexibility and reversed burden of proof	237
3.2.2.	<i>Second Panel of the PRO Triptych: the obligations incumbent on controllers and processors</i>	239
3.2.2.1.	General overview of the obligations of controllers under the GDPR and of their relation to the key principles of data protection	240
3.2.2.2.	Focus on specific obligations explicitly concerned with the protection of the fundamental rights and freedoms of data subjects	243
3.2.3.	<i>The Third Panel of the PRO Triptych: the panoply of rights of the data subjects</i>	292
3.2.3.1.	Overview of data subjects’ rights under EU data protection law	292
3.2.3.2.	The non-absolute nature of data protection rights and their relation to other rights and freedoms	294
3.2.3.3.	The functional role of data subjects’ rights within the PRO-triptych of the GDPR	297
3.2.4.	<i>Concluding remark: the synergies between the PRO-triptych as a horizontal factor of the functionality of the GDPR</i>	300
3.3.	THE THIRD PILLAR OF THE FUNCTIONALITY OF THE GDPR: SUPERVISION AND SANCTION WITHIN A MULTI-ACTOR DECENTRALISED SYSTEM	303
3.3.1.	<i>The effective enforcement of the GDPR: between improvements and disillusionment</i>	304
3.3.1.1.	Improvements in enforcement: the impact of the broadening of the investigative and corrective powers of DPAs	305
3.3.1.2.	Disillusionment: general organisational and procedural issues impeding the effective enforcement of the GDPR	313
3.3.2.	<i>The multi-actor enforcement system of the GDPR: a double-edged sword for ensuring the respect of the rights and freedoms of data subjects</i>	319
3.3.2.1.	Data subjects as first-row sentinels: fishing expedition and the facilitation of complaints submission	320
3.3.2.2.	DPOs as compliance insiders and informers: a (dys)functional channel of communication for compliance?	322
3.3.2.3.	Not-for-profit associations or bodies as strongholds and bridges for data protection enforcement and fundamental rights protection	324
3.3.2.4.	DPAs as key actors for the enforcement of the GDPR: discretionary use of their wide powers as factors of (dys)functionality	330
3.3.2.5.	National courts as the last bastion for enforcement: focus on GDPR mechanisms facilitating the exercise of the right to an effective judicial remedy	335
3.3.3.	<i>Concluding remarks: the multi-actor enforcement system of the GDPR as a double-edged sword for the protection of the fundamental rights of data subjects</i>	342
CHAPTER 4 – TESTING THE MULTI-FUNCTIONALITY OF THE GDPR FOR THE DEFENCE OF DIFFERENT FUNDAMENTAL RIGHTS		347
4.1.	HUMAN DIGNITY, INTEGRITY AND FREEDOM OF EXPRESSION IN THE CONTEXT OF ONLINE HARASSMENT	349
4.1.1.	<i>Defining and conceptualising ‘online harassment’</i>	351
4.1.2.	<i>The impact of online harassment on human dignity, integrity and freedom of expression</i>	355
4.1.1.1.	Distinction between the scope and effects of offline and online harassment	356
4.1.1.2.	Outlining the impact of online harassment on human dignity, the right to integrity and freedom of expression	361
4.1.3.	<i>The (lack of) EU or national legislation to tackle online harassment</i>	367
4.1.3.1.	Contractual or self-regulatory norms against online harassment: reliance on a (not-so) gentlemen’s club?	368
4.1.3.2.	National laws against online harassment: a fragmented system in a unified digital world	378
4.1.3.3.	Brief overview of EU instruments for combatting some forms of online harassment	382
4.1.4.	<i>The GDPR as an alternative or complementary framework for combatting online harassment: evidence of the secondary functionality of EU data protection law</i>	388
4.1.4.1.	The applicability of the GDPR to cases of online harassment	389
4.1.4.2.	Functionality of the tools provided by the GDPR to combat online harassment	399

4.1.4.3.	Concluding remarks on the functionality of the GDPR to combat online harassment.....	415
4.2.	NON-DISCRIMINATION IN THE CONTEXT OF E-RECRUITING PRACTICES.....	416
4.2.1.	<i>Defining e-recruitment or e-recruiting practices</i>	418
4.2.1.1.	General e-recruiting practices: conceptualising the notion of ‘e-recruitment’	419
4.2.1.2.	E-recruitment practices qualifying as AIDM under Article 22 of the GDPR	421
4.2.2.	<i>The nature and degree of impact of e-recruitment on non-discrimination</i>	424
4.2.2.1.	The nature of the impact of e-recruiting tools on non-discrimination: allies or trojan horses?	425
4.2.2.2.	The degree of impact of e-recruiting tools on non-discrimination: significant or superficial?	427
4.2.3.	<i>The sources of discrimination in the context of e-recruitment</i>	429
4.2.3.1.	Discrimination stemming from the poor design of e-recruiting tools	430
4.2.3.2.	Discrimination stemming from the misuse of e-recruiting tools by recruiters.....	433
4.2.4.	<i>The scope of discrimination when using e-recruiting tools: focus on several phenomena that can exacerbate discriminatory outcomes</i>	435
4.2.5.	<i>The regulation of e-recruitment practices in the EU through soft and binding law: a brief overview</i>	439
4.2.5.1.	Self-regulation and soft law in the form of ethical standards for the development of e-recruiting tools.....	440
4.2.5.2.	EU anti-discrimination laws against discriminatory practices in the field of recruitment.....	442
4.2.6.	<i>Exploiting the functionality of the GDPR for combatting discrimination in the context of e-recruitment</i>	449
4.2.6.1.	Rights which can be actioned by the data subjects in the context of e-recruitment to combat discriminatory outcomes	449
4.2.6.2.	Main obligations of controllers that may prevent algorithmic discrimination: data protection by design and by default, DPIA, appointment of a DPO and the necessity to have a valid legal basis	456
4.2.6.3.	Investigative and corrective powers of DPAs as essential tools to combat the inbuilt bias or the misuse of e-recruiting tools.....	461
4.2.6.4.	Concluding remarks on the functionality of the GDPR to combat the harmful effects of e-recruitment on equality and non-discrimination	466
CHAPTER 5 – SUMMARY FINDINGS, RECOMMENDATIONS & CONCLUSIONS		468
5.1.	SUMMARY FINDINGS AND RECOMMENDATIONS REGARDING THE MAIN FACTORS OF MULTI- FUNCTIONALITY OF THE GDPR WITH RESPECT TO ITS FUNDAMENTAL RIGHT OBJECTIVE	468
5.1.1.	<i>Summary findings regarding the main factors of multi-functionality of the GDPR</i>	469
5.1.1.1.	With respect to the scope of the GDPR.....	469
5.1.1.2.	With respect to the substance of the GDPR.....	472
5.1.1.3.	With respect to the supervision and sanction system of the GDPR	478
5.1.2.	<i>Summary recommendations on how to preserve and further enhance the multi-functionality of the GDPR</i>	480
5.2.	FINAL REFLECTIONS AND CONCLUSIONS ON THE APPARENT SHORTFALL, LEGITIMACY AND DESIRABILITY OF THE SECONDARY FUNCTIONALITY OF EU DATA PROTECTION LAW	486
5.2.1.	<i>Final reflection and conclusion on the apparent shortfall of the secondary functionality of EU data protection law in light of the case-law of the CJEU</i>	487
5.2.2.	<i>Final reflection and conclusion on the desirability and legitimacy of the secondary functionality of EU data protection law</i>	489
BIBLIOGRAPHY		495

ABOUT THIS STUDY

A. LIST OF ABBREVIATIONS

ADM	Automated Decision-Making
AEDP	<i>Agencia Española de Protección de Datos</i> (i.e., the Spanish DPA)
AI	Artificial Intelligence
AIDM	Automated Individual Decision-Making
AML	Anti-Money Laundering
AMS	Algorithmic Moderation System
BDSG	<i>Bundesdatenschutzgesetz</i> (i.e., the German federal data protection law)
BfDI	<i>Bundesbeauftragte für den Datenschutz und die Informationsfreiheit</i> (i.e., the German federal DPA)
CRM	Customer Relationship Management
CSSF	<i>Commission de Surveillance du Secteur Financier</i> (i.e., the Luxembourg financial supervisory commission)
DDT	Data-Driven Technology
DFR	Different Fundamental Rights (i.e., any fundamental right or freedom other than the fundamental right to privacy or personal data protection)
DPA	Data Protection Authority
DPC	Data Protection Commissioner (i.e., the Irish DPA)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECSC	European Coal and Steel Community
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EPRS	European Parliamentary Research Service

B. BACKGROUND OF THIS STUDY

For the last four decades, rapid technological developments and globalisation have drastically increased the scale of the collection and sharing of personal data. Advances in the field of information and communication technologies ('ICTs'), and the boom of connected portable devices in particular, have profoundly changed individuals' habits. The internet can nowadays be considered as an essential space for individuals to conduct their social, political, financial, educational and professional life.¹ As a consequence, it can be argued that the digital identity of each individual has become an important alter ego to one's physical self.² Digital identities offer many practical advantages but – as countless affairs and scandals have shown since the advent of the internet – they can also be subject to data-driven discrimination, data theft and other unlawful practices that may ultimately harm the fundamental rights and freedoms of the individuals to whom these digital identities belong.

At the EU level, protecting the privacy of individuals against invasive data processing practices had already become a concern at the beginning of the 70s.³ The first legislative steps in the field of data protection were however only taken by the European Commission (hereafter, the Commission) in 1990, when the latter adopted a package of proposals relating to the protection of personal data.⁴ At the same time, as more and more businesses became dependent on ICTs to conduct their activities, it clearly appeared that restricting the free flow of personal data between Member States could hinder the proper functioning of the common market. In 1995, drawing on prior international and national examples, the EU legislator therefore adopted a Directive aiming at reconciling these seemingly conflicting objectives: *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (hereafter, the 1995 Data Protection Directive).⁵ The same year as the adoption of this Directive, Nicholas Negroponte, architect, author and founder of the Media Lab at the Massachusetts Institute for Technologies (MIT), published a book titled "Being Digital". In this book,

¹ Dutton, W. H. & Graham, M. (2014). *Society and the Internet: How Networks of Information and Communication are Changing our Lives*. M. Graham and W. H. Dutton (eds). Oxford University Press.

² As Karel De Gucht, former Prime Minister of Belgium, once stated: "*the twenty-first century citizen (...) seems to develop a digital person that becomes increasingly part of his individual social identity. From this perspective, control over personal information is control over an aspect of the identity one projects in the world.*" De Gucht, K. (2009). Foreword. In: Gutwirth, S. *Reinventing data protection?* Berlin: Springer, p. vi.

³ See Section 2.1.2, below.

⁴ This package included, most notably, a Proposal for a Council Directive Concerning the Protection of Individuals in relation to the Processing of Personal Data (COM (1990) 314 - 2: Procedure 1990/0287/COD).

⁵ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, *OJ L 24, 30.1.1998, p. 1–8*.

Negroponte foresaw the massive digitalisation of human societies and argued that “*the change from atoms to bits is irrevocable and unstoppable*”.⁶

Today, globally, individuals are undeniably more connected than ever. The once common action to buy a newspaper turned for many into the habit of reading online press articles, sharing tweets from journalists, or scrolling down their Facebook newsfeeds. The time-consuming process of writing and posting letters has been almost entirely replaced by the use of emails or other instant messaging technologies. Buying a new pair of shoes no longer entails having to leave one’s home and go shopping outside; almost all types of goods can now be bought online.⁷ Some goods, such as books or movies, have even been dematerialised and can now be consumed exclusively in digital format.⁸ Social connections and interactions between individuals also increasingly occur online, from finding a date,⁹ to chatting with friends, or sharing experiences or opinions on social media.¹⁰ Money itself has gradually left the material world to enter the digital one, as reflected by the rise of online banking, cryptocurrencies and the diminishing amount of cash that people carry.¹¹ Overall, as Negroponte foresaw it, the world of living individuals has gradually been shifting from atoms to bits through technological developments and innovations. Data, and in particular *personal* data, became a crucial part of this new world.¹²

The objective of the 1995 Data Protection Directive was precisely to protect the fundamental rights of individuals with respect to the processing of their personal data, while ensuring the free flows of those data between EU Member States.¹³ For this purpose, the Directive already recognised a few specific rights to individuals (referred to as ‘data subjects’) with respect to the processing of their personal data, such as the right to information, the right to rectification, or the right to object to the processing of their personal data. In December 2000, the EU also expressly recognised the fundamental nature of the right to personal data protection by

⁶ Negroponte, N. (1995). *Being digital*. New York: Alfred A. Knopf, p. 4.

⁷ Amazon is the leading e-commerce platform for consumers in the EU. As of April 2019, the platform Amazon.com (for the US alone) had a total of 119.28.851 *products* (source: <https://www.scrapehero.com/number-of-products-on-amazon-april-2019/>).

⁸ As an illustration, the company *Audible* offers digital audio books since 1995. The company was bought by Amazon on January 31, 2008. Today, users have the possibility to purchase a monthly abonnement. Similarly, the company *Netflix* offers a monthly abonnement giving access to an online library of movies, series and TV shows.

⁹ In 2019, it is estimated that 50 million people worldwide use the dating app *Tinder* (source: <https://www.businessofapps.com/data/tinder-statistics/>).

¹⁰ On 24 July 2019, Mark Zuckerberg posted a message on its Facebook wall, announcing: “*There are now more than 2.7 billion people using Facebook, Instagram, WhatsApp and messenger each month, and more than 2.1 billion people using at least one of our services each day*”.

¹¹ Press release by mastercard on 24/10/2016, “*Britons now carry less than £5 in cash in their wallets. Wallets and purses falling out of favour as cash gives way to card, research shows*” (source: <https://newsroom.mastercard.com/eu/press-releases/britons-now-carry-less-than-5-in-cash-in-their-wallets/>).

¹² The International Data Corporation (IDC) predicts that our global datasphere will grow from 40 to 175 zettabytes in 2025 (source: IDC White Paper, Data Age 2025: <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>).

¹³ Article 1 of the 1995 Data Protection Directive.

enshrining it in the Charter of Fundamental Rights of the European Union (hereafter, the 'Charter').¹⁴ Since the inclusion of the right to personal data protection in the Charter, one could have thought that individuals would enjoy a high level of protection with respect to the processing of their personal data in the EU. It soon appeared however that the existing legislative framework was failing to effectively address the challenges that new ICTs were posing to the rights and freedoms of data subjects. Slowly but surely, EU data protection law was turning into a 'dead letter' – a framework with no or little effect on data processing practices.¹⁵ On 18 June 2012, during a speech given in Luxembourg at a large forum on digitalization, the Justice Commissioner Viviane Reding herself admitted that EU data protection needed to be reformed.¹⁶ She explained this need by stressing out that the 1995 Data Protection Directive had been adopted at a time when data-driven technologies had not yet invaded our daily lives. In 1995 indeed, only 1% of the EU population was using the internet; e-commerce companies such as Amazon or eBay were barely emerging; the giant Google, which now dominates the online advertising industry, still had not launched its famous search engine; and Mark Zuckerberg, the founder of Facebook, was only 11 years old.¹⁷ Less than two decades later however, those big tech companies had become dominant and were already profoundly impacting the world, both economically and socially, through the collection and use of massive amount of data. These rapid changes did not escape the attention of regulatory bodies.¹⁸ During the second decade of the 21st century, the Commission therefore undertook an ambitious legislative modernisation of EU data protection law. The adoption, in 2016, of the EU General Data Protection Regulation¹⁹ (the 'GDPR') in replacement of the 1995 Data Protection Directive was a central piece of this process.²⁰

The need for a reform of EU data protection law principally stemmed from the fact that personal data had become an ever-more valuable commodity sought by both private companies and public authorities. One of the regulatory responses given by the EU legislator was thus to increase the degree of control exercised by data subjects over their own personal data. When the GDPR became applicable on 25 May 2018, the rights of data subjects were broadened to reinforce their capacity to

¹⁴ The Charter was first proclaimed during the European Council meeting in Nice on 7 December 2000. On this topic, see the Background Note of the European Parliament, "EU Charter of Fundamental Rights – Proclamation at Parliament in Strasbourg 12 December 2007". 20071127BKG13869 (source: [https://www.europarl.europa.eu/RegData/press/pr_dossier/2007/EN/03A-DV-PRESSE_BKG\(2007\)11-27\(13869\)_EN.pdf](https://www.europarl.europa.eu/RegData/press/pr_dossier/2007/EN/03A-DV-PRESSE_BKG(2007)11-27(13869)_EN.pdf))

¹⁵ Koops, B.-J. (2014). The trouble with European Data Protection Law. *International Data Privacy Law*, 4(4):250-261, p. 250.

¹⁶ See Viviane Reding Vice-President of the European Commission, *EU Justice Commissioner Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world*, Digital Enlightenment Forum, Luxembourg, 18 June 2012 (source: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_464).

¹⁷ *Ibid.*

¹⁸ Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford Studies in European Law, p. 2.

¹⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

²⁰ Kosta, E. (2014). The future of data protection: Collapse or revival? *International Review of Law, Computers & Technology*, 28(2):115.

determine *when, how and for what purposes* information about them was being processing.²¹ In parallel, more stringent obligations were also imposed on public or private persons that process personal data in the course of their activities. The GDPR also introduced specific enforcement mechanisms and deterrent administrative sanctions, which undeniably contribute to the effectiveness of this protective framework. The adoption of the GDPR can therefore be seen as a turning point for the enjoyment and safeguarding of the fundamental right to personal data protection.

At the time the GDPR was adopted, the author of this study was working in the litigation and risk management department of an international law firm in Brussels. In May 2016, in the aftermath of the entry into force of the GDPR, this department was suddenly overwhelmed with data protection-related questions from a large number of clients operating in diverse sectors, from data brokers to fashion retailers, and from insurance companies to food manufacturers. In today's world indeed, it can be argued that not one single company is *not* processing personal data. As a result, all businesses were concerned by the entry into force of the GDPR and needed advice on compliance. Because of this growing demand, a specialised team was created within the law firm: the Benelux Data Protection Team. After a few months, this team was composed of more than 30 lawyers and staff members from the Brussels, Luxembourg, Rotterdam and Amsterdam offices, including the author of this study, whose working hours were almost entirely dedicated to advising clients with respect to GDPR compliance.

A quick look into the history of the relations between these clients and the law firm showed that most of these companies had not really cared about data protection law before 2016 (i.e., before the adoption of the GDPR). After that date, however, data protection compliance had suddenly become a boardroom topic due to the high administrative sanctions that data protection authorities ('DPAs') could impose on companies in the event of a breach of the GDPR rules. In order to offer a comprehensive and flexible compliance solution, the law firm put into place a 'GDPR Toolkit': a secured online platform providing the clients with a set of documents (including guidelines, sample clauses, draft processing agreements, etc.) in order to help them achieve compliance with the GDPR. This Toolkit quickly became a success, with dozens of subscriptions from new or existing clients of the firm every month. In the mind of the author of this study, two main reasons could explain this success: first, as already mentioned, these clients were terribly afraid of the fines that they could incur in case of non-compliance; and second, they did not want to lack behind and see their competitors harvest the benefits of having a better data governance in

²¹ Bellinger, A. and Krieger, D. (2018). *Network Publicity Governance. On Privacy and the Informational Self*. Bielefeld: Transcript Verlag.

place. In other words, they wanted to be compliant to avoid sanctions, and they wanted to be compliant to be competitive.²²

After the 25th of May 2018, the focus gradually shifted from compliance to dispute management. Issues relating to data breaches or difficulties in fulfilling requests from data subjects started arising. This was a very interesting period for legal practitioners in the field of data protection, as they could test and assess first-hand how well the 'GDPR machinery' was going to work, and how functional it would be. And in many aspects, it was functioning well: data breaches were reported; requests from data subjects were being answered; data protection impact assessments were thoroughly conducted; etc. Yet, in some instances, negligence or divergences in the interpretation to be given to the GDPR led to disputes between data subjects and third parties processing their personal data (referred to as 'controllers' or 'processors'). Beginning of 2019, the author of this study was confronted with a particularly interesting case. The dispute at stake was opposing a Dutch investment bank (i.e., the 'controller') to one its former clients – a wealthy individual residing outside of the EU (i.e., the 'data subject'). An investigation had been conducted by the Dutch bank in accordance with its anti-money laundering ('**AML**') obligations, following which the bank had decided to momentarily freeze the client's assets, put an end to their contractual relationship, and report suspicious financial transactions to the competent authority. The former client, however, decided to fight back – not on the basis of banking law or contractual law, as one could have been expecting, but on the basis of EU data protection law. In particular, the former client requested to have access to the personal record that the bank had created on him by invoking Article 15 GDPR ('Right of access by the data subject'). Being provided with a copy of this record would have enabled him to prepare his defence in the context of the proceedings that the competent financial authorities were about to initiate against him. After being denied access to this record by the bank, the former client filed a complaint with the Dutch data protection authority – the *Autoriteit Persoonegevens*. Rather than the outcome of this case, what appeared particularly interesting to the author of this study was the way that this former client had relied on EU data protection law to protect interests that were not directly related to his right to privacy or his right to personal data protection. Indeed, his access request was not motivated by the desire to protect his informational rights, but rather by his desire to ensure the respect of due process and, ultimately, of his right to property.

A few months later, another interesting case ended up on the desk of the author of this study. This case concerned a Mexican couple who had invested into a Luxembourg fund; both the wife and her husband were considered as the Ultimate Beneficial Owners ('**UBOs**') of this fund under the applicable law. Since they were indirectly benefiting from this fund, their names and address had to be published for

²² On how data protection can be seen as a tool for competitiveness, see: Balboni, P. (2019). *Personal data protection as the new competitive edge: Generating socially responsible corporate behaviour*. Maastricht University.

transparency reasons in the Luxembourg Register of Beneficial Owners²³ – a register managed by the Luxembourg financial authority (in French, the '*Commission de Surveillance du Secteur Financier*' or '**CSSF**'). However, instead of the professional address of the couple, the CSSF had published the address of their family home in Mexico. According to the couple, this represented a serious threat to the safety and physical integrity of their family, and in particular of their children, since various criminal groups based in Mexico were known for abducting children of wealthy families, and then exercising pressure on the parents to obtain a ransom. Fearing for the safety of their children, the couple sought advice on how to obtain the erasure of this address from the Luxembourg Register of Beneficial Owners. From all the legal means available, it quickly appeared that the GDPR could be the most functional for obtaining the deletion of such data. And indeed, after a few calls and email exchanges, the CSSF agreed to erase the personal address of the Mexican couple in application of Article 17 of the GDPR (the 'Right to erasure'). It had been agreed, *inter alia*, that there was no overriding legitimate ground for the CSSF to publish the *personal home* address of these individuals since the objective of the law was to guarantee a certain level of transparency which could also be achieved by publishing their *professional* address. In particular, the CSSF agreed that the safety and physical integrity of the concerned individuals were prevailing over the public interest at stake, and that the publication of the home address of these individuals had therefore no valid legal basis. What the author of this study had found particularly interesting about that case was not so much the interpretation that had been given to Article 6 of the GDPR, but rather how rapidly and conveniently a satisfactory outcome had been reached. Furthermore, the GDPR had once again been successfully mobilised not only to ensure the respect of the fundamental right to personal data protection or privacy of the individuals concerned, but also the respect of different fundamental rights, i.e., their right to safety and physical integrity. The manner in which the GDPR had been instrumentalised in these two cases hence triggered the interest of the author of this study with respect to the functionality of EU data protection law. It was becoming clear indeed that the GDPR was offering practical and convenient tools for individuals to defend various rights and interests in the context of the processing of their personal data, beyond their right to privacy or personal data protection.

In parallel to this however, journalists, scholars and practitioners were also starting to question the effectiveness of EU data protection law for guaranteeing the respect of fundamental rights and freedoms against novel types of technologies. Behavioural micro-targeting, algorithmic decision-making or the unfettered collection of information by 'Big data' actors were increasingly being perceived as serious threats to individual freedoms. Between 2015 and 2019, several affairs widely covered by the media also showed in a very concrete manner the negative impact that novel

²³ The law establishing a Register of Beneficial Owners for Luxembourg-registered entities was adopted on 13 January 2019 and came into force as of 1 March 2019. The beneficial ownership register is based on Article 30 of Directive (EU) 2015/849. Its aim is to prevent money laundering and terrorist financing.

data processing practices could have on individual fundamental rights. Among others, one may refer to the *Cambridge Analytica* scandal,²⁴ the embarrassing ‘Gorilla’ incident revealing racist bias in Google’s search algorithm,²⁵ or the complaint brought against Facebook in the US for housing advertising discrimination²⁶ Through the large media coverage of these affairs, as well as several mainstream Netflix documentaries covering these topics, such as *The Social Dilemma*,²⁷ *The Great Hack*²⁸ or *Coded Bias*,²⁹ the general public increasingly gained awareness on the danger that novel technologies could pose to an array of fundamental rights and freedoms, far beyond privacy and data protection. While most of these press articles and documentaries were pointing out in an alarming manner all the existing and future risks that ICTs could pose for human rights, few if no solutions were actually being discussed. Yet, individuals do not stand powerless against the potential harmful use of novel technologies by state authorities or big corporations. Legislative protection already exists, including in the form of the GDPR. This led the author of this study to reflect on the functionality of EU data protection law, and in particular of the GDPR, in addressing and combatting some of the most pressing threats weighing upon fundamental rights in the digital sphere.

C. RESEARCH QUESTION

Before 2000, data protection law had been described as a ‘dead letter’ and the fundamental right to personal data protection did not even exist at the EU level.³⁰ Today, personal data protection seems to have become a ‘super’ fundamental right,³¹ supported by a comprehensive set of EU regulations and directive, including

²⁴ *Cambridge Analytica* is a British tech company involved in the theft of millions of Facebook profiles in order to use them to build a powerful software program to predict and influence the choice of US voters during the 2016 US presidential election. Source: The Guardian Cambridge Analytica Files. *The Guardian*. <https://www.theguardian.com/news/series/cambridge-analytica-files>.

²⁵ In 2015, it was found out that Google’s algorithm for image-recognition auto-tagged pictures of black people as ‘gorillas’. To put an end to this bias, Google temporarily removed the term ‘gorilla’ from searches and image tags. Source: Hern A. (2018, January 12). Google’s solution to accidental algorithmic racism: ban gorillas. *The Guardian*. <https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people>.

²⁶ In 2019, the U.S. Department of Housing and Urban Development issued an administrative complaint according to which Facebook violated the Fair Housing Act because its ad system allowed advertisers to exclude certain audiences, such as families with young children or disabled people, from seeing housing ads. Source: Nix N. & Dvoskin E. (2022, June 21). Justice Department and Meta settle landmark housing discrimination case. *The Washington Post*. <https://www.washingtonpost.com/technology/2022/06/21/facebook-doj-discriminatory-housing-ads/>.

²⁷ *The Social Dilemma*, a Netflix documentary directed by Jeff Olowski, released on 9 September 2020. For more information, please refer to: www.thesocialdilemma.com.

²⁸ *The Great Hack*, a Netflix documentary directed by Karim Amer and Jehane Noujaim, released on 26 January 2019.

²⁹ *Coded Bias*, a Netflix documentary directed by Shalini Kantayya, released on 26 January 2020.

³⁰ Koops, B.-J. (2014), *op. cit.*, p. 250.

³¹ This expression was first coined in 2014 by Prof. Christopher Kuner (Kuner C. (2014, June 28). A ‘Super-right’ to Data Protection? The Irish Facebook Case and the Future of EU Data Transfer Regulation. *The International Forum for Responsible Media Blog*. <https://inform.org/2014/06/28/a-super-right-to-data-protection-the-irish-facebook-case-and-the-future-of-eu-data-transfer-regulation-christopher-kuner/>) and in 2015 by Prof. Daniel Sarmiento (Sarmiento, D. (2015). What Schrems, Delvigne and Celaj tell us about the state of fundamental rights in the EU. *Verfassunblog*. <https://verfassungsblog.de/category/focus/the-schrems-case-en/>). Prof. Sarmiento used the term ‘super’ to describe the right to privacy as interpreted by the CJEU together with the right to personal data protection.

the GDPR, which has been described as “*the most consequential regulatory development in information policy in a generation*”.³² This somewhat spectacular ascent of EU data protection raised multiple questions in the mind of the author: what is the original objective of EU data protection law? How did it evolve over the years? Is EU data protection law a legitimate legislative framework for the protection of fundamental rights? And most importantly, is EU data protection law *truly* fitted for protecting fundamental rights against modern data processing practices?

After reviewing the existing literature, the author decided to focus her study on unveiling the characteristic elements which make of data protection a multi-functional framework for the protection of fundamental rights in the area of information technologies, as well as the limits of such multi-functionality. Since the GDPR is the most important piece of EU legislation in the field of data protection, most analysis will revolve around the origin, substance, and application of the GDPR and of its predecessor, the 1995 Data Protection Directive. This study will thus first theorise about the notion of legal multi-functionality before putting the GDPR to the test and formulating recommendations on how to potentially maximize its positive effects for the benefit of the fundamental rights of data subjects. The overreaching research question of this study can thus be summarized as follows:

How multi-functional is EU data protection law, and the GDPR in particular, for protecting data subjects’ fundamental rights and freedoms, beyond data protection or privacy, against novel and potentially harmful data processing practices in the digital sphere?

D. SCOPE OF THIS STUDY

This study focuses on the protection of EU fundamental rights through the application of EU primary and secondary law in the field of data protection, as well as Member States’ data protection law. The scope of this study will therefore be limited to the EU legal order.

As far as EU primary law is concerned, particular attention will be put on Article 8 of the Charter on the right to personal data protection in terms of scope and content, as well as Article 16 of the Treaty on the Functioning of the European Union (hereafter, the ‘**TFEU**’) which compels the EU to adopt legislation in the field of data protection. With respect to Article 8 of the Charter, it must be pointed that the substantive content of the Charter has been inspired by and must be interpreted in accordance with the Convention for the Protection of Human Rights and Fundamental Freedoms (more commonly referred to as the European Convention on

³² Hoofnagle, C. J., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019) The European Union General Data Protection Regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1):65-98.

Human Rights or the 'ECHR'), and the case law of the European Court of Human Rights (hereafter, the 'ECTHR'). The ECHR and the case-law of the ECTHR will therefore be analysed where relevant for answering the research question of this study.

As far as EU secondary law is concerned, the author will focus on one piece of legislation in particular: the GDPR. The GDPR regulates the processing of personal data by both public and private entities and can be considered as the main piece of EU legislation in the field of data protection. As a consequence, the functionality of the GDPR indirectly reflects the functionality of EU data protection law as a whole. When necessary to answer the research question of this study, other EU legislative acts regulating the processing of personal data will be touched upon, and mainly: (i) the e-Privacy Directive;³³ (ii) the Regulation on Personal Data Processing by EU Institutions;³⁴ and (iii) the Directive Protecting Individuals with regard to the Processing of their Personal Data by Police and Criminal Justice Authorities (commonly referred to as the 'Data Protection Law Enforcement Directive', or more simply the 'Law Enforcement Directive' or 'LED').³⁵ When analysing EU primary and secondary law in the field of EU data protection law, due regard shall be given to the guidelines, opinions and decisions of EU bodies that are competent to interpret and/or apply EU data protection law, and in particular the European Data Protection Board³⁶ (the EDPB), the European Data Protection Supervisor (EDPS) and of the Court of Justice of the European Union (CJEU).

EU legislation in the field of data protection is being implemented and interpreted at Member States level by national legislators, courts and DPAs. Each Member State has established at least one DPA on its territory that is competent to enforce EU data protection law.³⁷ National acts implementing EU data protection law, as well as decisions and opinions rendered by national courts or DPAs therefore form an integral part of the interpretation or application of EU data protection law. Conducting a thorough review of these national sources across the 27 Member

³³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *OJ L 201*, 31.7.2002, p. 37–47. This Directive is to be replaced by the upcoming e-Privacy Regulation: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (COM/2017/010 final - 2017/03).

³⁴ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, *OJ L 295*, 21.11.2018, p. 39–98.

³⁵ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119*, 4.5.2016, p. 89–131.

³⁶ The EDPB is an independent body based in Brussels whose main task is to contribute to the consistent application of EU data protection law throughout the territory of the EU Member States, and to promote cooperation between national data protection authorities. The EDPB is established by Article 68 GDPR.

³⁷ The obligation for each Member State to establish an independent DPA already existed under the 1995 Data Protection Directive and has been reaffirmed under Article 51 GDPR.

States would however go beyond the scope of this study. The analysis of national legislation, judicial decisions and/or decisions rendered by DPAs will thus be limited to what is both possible and relevant for answering the research question of this study, taking into account, *inter alia*, the available databases, the knowledge of the author with respect to the relevant jurisdictions as well as her linguistic capabilities (English, French, Dutch and German). It is important to note that this study focuses on the functionality of EU data protection law, and of the GDPR in particular, to defend the rights and freedoms of data subjects. Hence, the author does not intend to compare the different national systems that implement or enforce the GDPR, but rather will rely on national examples to illustrate how the GDPR is implemented and enforced in practice. In other words, analysis of national sources of law will mainly have an illustrative purpose to assess the varying degree of multi-functionality of the GDPR.

This study is construed around the hypothesis that EU data protection law is a multi-functional framework for the protection of fundamental rights in the context of personal data processing. The author will attempt at showing the extent but also the limits of such multi-functionality by testing the capability and handiness of the GDPR to address the challenges raised by modern and potentially harmful data-driven technologies (hereafter, 'DDTs'). Of course, there are numerous data processing practices relying on DDTs which can put individuals' fundamental rights and freedoms at risk, such as identity theft, behavioural targeting, cyber-bullying, illegal geo-blocking, mass surveillance by state authorities, unlawful tracking of workers by employers, or political micro-targeting, just to name a few. In the context of this study, it is however neither feasible nor necessary to study all of these harmful data processing practices in order to demonstrate the extent and limits of the functionality of EU data protection law, and of the GDPR in particular. Instead, two different data processing practices have been selected on the basis of their scope, topicality and the severity of their consequences on fundamental rights and freedoms. These two practices are, specifically:

- 1) Online harassment:** online harassment has become widespread in the digital sphere, with around 41% of internet users having experienced some forms of verbal or graphic abuse. Online harassment can take different forms, such as cyberbullying, targeted hate speech, impersonation or 'revenge porn'.³⁸ Online harassment, because of the profound negative impact that it can have on the life of victims, threatens various fundamental rights and freedoms, such as human dignity, the right to the integrity of the person and, in some instances, freedom of expression.

³⁸ 'Revenge porn' is the practice of disclosing sexually explicit images or videos of a person on the internet without the consent of that person (Oxford Languages definition). Legally speaking, revenge porn is usually referred to as the non-consensual publication or dissemination of sexually explicit images.

- 2) E-recruitment:** e-recruitment refers to the use of DDT and in particular algorithmic decision-making to support or replace human-decision making in the field of recruitment. If poorly designed or implemented, e-recruiting DDTs can put at risk, in particular, the principle of equality and non-discrimination.

These two ‘test areas’ will provide a framework to both test and illustrate the extent and limits of the functionality of EU data protection law for protecting data subjects’ fundamental rights and freedoms against modern and potentially harmful data processing practices, with a view of formulating specific recommendations on how to further enhance this functionality.

Finally, and most importantly, the author of this study acknowledges that, in some instances, EU data protection law can be used by data subjects as a weapon to restrict the exercise of the rights and freedoms of other persons. As an example, when a data subject invokes data protection law against a controller to prevent the latter from publishing information, including, as the case may be, information that promotes transparency or participates to an important public debate, such action may interfere with the fundamental rights of the controller and of third parties, such as the right to a good administration or freedom of expression and information. In line with Article 52(1) of the Charter, Member States and EU institutions have normally a duty to establish a balance between conflicting rights and freedoms. It is thus their duty to ensure that EU data protection law is implemented and interpreted in a way that is compatible with other rights and freedoms, in accordance with the principle of proportionality. Although the author of this study acknowledges the inherent risk that the abusive instrumentalization of EU data protection law can pose for the rights and freedoms of controllers or third parties, the focus of this study is limited to understanding the functionality of EU data protection law as far as it may serve the rights and freedoms of the *data subjects*. Hence, for the sake of relevance and conciseness, this study will not explore the reverse question of how EU data protection law can be interpreted or applied in a way that could interfere with the rights and freedoms of others, including, as the case may be, the freedom of expression of controllers or third parties.

E. METHODOLOGY

This study aims at unveiling the elements that could explain the multi-functional nature of EU primary and secondary law in the field of data protection, before putting it to the test and formulating recommendations for enhancing such multi-functionality and better protect fundamental rights against modern and potentially harmful data processing practices. This study thereby combines a more theoretical approach in the tradition of legal positivism, and a more practical approach based on case-studies. For this purpose, the author will combine theoretical, historical, analytical and empirical research methodologies.

In particular, in the first Chapter of this study, the author will analyse the existing literature on the notion of the effectiveness of the law with a view of creating the outlines of her research question. Relying on a theoretical approach, the author will discuss the notion of 'effectiveness' and distinguish it from the notion of 'functionality'.

In the second Chapter of this study, the author will first adopt a historical approach by retracing the origin and foundations of EU data protection law from the 50s. After this purely historical analysis, the author will focus on the case-law of the CJEU in the field of data protection. In particular, the author will analyse to the benefit of which fundamental rights and freedoms EU data protection law has been interpreted so far. This entails a systematic analysis of the entire corpus of decisions rendered by the CJEU on the interpretation of the 1995 Data Protection Directive and of the GDPR. Adopting a theoretical approach, the author will then draw her first conclusions and spell out sub-questions relating to her hypothesis according to which EU data protection law, and the GDPR in particular, would be a multi-functional framework for the defence of data subjects' fundamental rights.

In a third Chapter, the author will analyse the text of the GDPR itself with a view of identifying its main internal factors of functionality. For that purpose, the author will systematically analyse all the provisions of the GDPR on the basis of a textual, descriptive and diagnostical approach. Particular emphasis will be put on provisions of the GDPR which put at their centre the need to ensure the protection of the fundamental rights and freedoms of data subjects in the context of the processing of their personal data by controllers or processors. Based on this analysis, the author will draw conclusions on which provisions of the GDPR appear particularly functional to achieve the fundamental rights objective of EU data protection law and organise her findings around what she considers to be the three structural pillars of the GDPR: (1) its scope, (2) its substance in terms of rights and obligations and (3) its system of supervision and sanctions.

In a fourth Chapter, the author will test her hypothesis within the two areas described under point D here above, i.e., online harassment and e-recruitment. For this purpose, the author will undertake a literature review. On the basis of a theoretical and analytical approach, the author will first define 'online harassment' and 'e-recruitment' from the perspective of EU data protection law and explain the impact that each practice can have on data subjects' fundamental rights. The author will then undertake a short and general review of the main laws that already regulate these practices at the EU and Member States level, besides EU data protection law. Adopting a more practical approach, the author will then analyse how EU data protection law, and the GDPR in particular, could complement these laws, or be used as an alternative source of law for combatting the harmful effects of online harassment and e-recruitment on individual rights and freedoms. For that purpose, the author will analyse the most relevant case-law of national DPAs or

national courts concerning some forms of harassment or e-recruitment. For finding this relevant case-law in both test areas, the author will rely on one specific database in particular: the GDPRhub.³⁹ In order to gain insight into the way this database is being populated and being organised, the author will complete an internship at *noyb* – *European Center for Digital Rights*, the NGO that created and is still managing the GDPRhub.⁴⁰

Finally, adopting a prescriptive approach, the author will spell out her conclusions and recommendations on how to further enhance the multi-functionality of EU data protection law the benefit of data subjects' fundamental rights in the digital sphere.

F. SCIENTIFIC AND SOCIETAL RELEVANCE

By conceptualising, discussing and testing the functionality of the GDPR, the author wishes to contribute in an innovative way to the scientific debates on the effectiveness of the law and on the effective protection of fundamental rights in the digital sphere. Furthermore, by assessing and revealing how the multi-functionality of the GDPR could be further enhanced to adequately address the risks posed by modern and potentially harmful data processing practices, the author wishes to concretely contribute to the betterment of fundamental rights protection in the digital sphere, for the benefit of individuals as well as society as a whole.

Regarding the scientific relevance of this study in particular, the author hopes to contribute to scientific debates in the field of legal theory by exploring the notion of *legal functionality*. The author also hopes to contribute to scientific debates in the field of fundamental rights law by exploring how the GDPR can be mobilised for the benefit of various fundamental rights. So far indeed, EU data protection law has mainly been studied in relation to the right to privacy,⁴¹ its legal consequences in a specific area or sector, or a specific issue (e.g., terrorism surveillance, behavioural targeting, etc.).⁴² However, there is little research on the effects of EU data protection law from the perspective of fundamental rights law beyond the spectrum of the right to privacy. One notable exception is the book of Gloria González Fuster,

³⁹ This database is freely accessible via www.gdprhub.eu.

⁴⁰ This internship took place between 1st of September 2021 and 1st of January 2022. During these 4 months, the author of this study has mainly been in charge of populating the database by writing summaries of case-law in the field of data protection law or supervising the writing of such summaries by external volunteers throughout the EU.

⁴¹ Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy*. Springer; Gutwirth, S., Leenes, R., de Hert, P. de & Poulet, Y. (2012). *European data protection: In good health?* Dordrecht: Springer; Hess, B. & Mariottini, C. (2015). *Protecting privacy in private international and procedural law: European and American Developments*. Baden-Baden: Nomos.

⁴² Tzanou, M. (2017). *The fundamental right to data protection: normative value in the context of counter-terrorism surveillance*. Oxford: Hart Publishing; Boehm, F. (2012). *Information sharing and data protection in the area of freedom, security and justice: towards harmonised data protection principles for information exchange at EU-level*. Berlin: Springer; Zuiderveen Borgesius, F. J. & Poort, J. (2017). Online Price Discrimination and EU Data Privacy Law. *Journal of Consumer Policy*, 40(3):347-366.

which explores the coming into being of the fundamental right to data protection.⁴³ Fuster's study is however limited to the emergence of the fundamental right to data protection itself through the lens of legislative texts. It neither includes an in-depth analysis on the fundamental right objective of EU data protection law, nor examines the characteristic elements that could explain its multifunctional nature. Furthermore, most of the literature on the fundamental right to data protection has been published before 25 May 2018, i.e., before the GDPR started applying in the EU. Additional research is thus needed to understand how the GDPR may be used as a tool to (r)e(i)nforce the overall protection of EU fundamental rights in the digital sphere.

Regarding the social relevance of this study, it cannot be denied that ICTs have radically transformed the way that natural persons share information or interact with each other. By greatly facilitating the free flow of personal data, technological developments have created new opportunities for strengthening democracy and human rights but have also created novel risks with respect to the processing of personal data. Political micro-targeting, digital discrimination or personal data leaks are examples of relatively novel issues threatening the rights and freedoms of individuals. The Council of Europe and the EU have taken steps to address these issues in the form of reports, declarations, or recommendations.⁴⁴ As far as the right to personal data protection is concerned, a major legislative step was taken by the EU with the adoption of the GDPR. Yet, neither the EU nor the Member States have been able to decide whether each modern threat to democracy and human rights in the information society should be met with a similar regulatory response and, in the affirmative, how to articulate such a response. Rather than adopting new laws, a more efficient solution might be to maximize the benefits of existing legislation. This study precisely aims at analysing how EU primary and secondary law could be used to its fullest potential in order to address the challenges posed by novel data protection practices and DDTs. Combatting and preventing harmful data processing practices will enable individuals to enjoy the many benefits of new ICTs and DDTs without fearing to be discriminated, manipulated or subject to unlawful surveillance. This should in turn strengthen democracy and the rule of law. From a societal point

⁴³ González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer International Publishing.

⁴⁴ Among the recent publications of the EU institutions and the Council of Europe, see, inter alia: Bychawska-Siniarska, D. (2017). *Protecting the Right to Freedom of Expression under the European Convention on Human Rights, A handbook for Legal Practitioners*. Council of Europe. <https://edoc.coe.int/en/fundamental-freedoms/7425-protecting-the-right-to-freedom-of-expression-under-the-european-convention-on-human-rights-a-handbook-for-legal-practitioners.html>; Rokša Zubčević, A., Bender, S. & Vojvodić, J. (2017). *Media Regulatory Authorities and Hate Speech*. Council of Europe. <https://edoc.coe.int/fr/medias/7431-media-regulatory-authorities-and-hate-speech.html>; Council of Europe (2014, April 16). *Guide to human rights for Internet users*. Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31>; European Parliament (2018, December 13). *Report on the situation of fundamental rights in the European Union in 2017 (2018/2103(INI))*; Martens, B., Aguiar, L., Gomez-Herrera, E. & Mueller-Langer, F. (2018, April). *The digital transformation of news media and the rise of disinformation and fake news*. European Commission. JRC Technical Report 2018-02. https://ec.europa.eu/jrc/communities/sites/jrccties/files/dewp_201802_digital_transformation_of_news_media_and_the_rise_of_fake_news_final_180418.pdf

of view, the author of this study believes that her findings could contribute in an innovative way to the body of work that aims at enhancing the protection of fundamental rights in the area of information technologies.

G. STRUCTURE

This study will be divided into six parts:

- In the **Introduction**, the positive or negative impact that data processing practices can have on the fundamental rights and freedoms of data subjects will generally be explained. For this purpose, important terms that will be used throughout this study will first be defined, such as ‘data processing practices’, ‘data-driven technologies’, ‘hardware’, ‘software’, ‘algorithms’, ‘artificial intelligence’, etc. The author of this study will then highlight how technological developments and changes in social habits have broadened and deepened the impact of data processing practices on the fundamental rights and freedoms of the data subjects.
- In a **first chapter**, entitled “THE MULTI-FUNCTIONALITY OF EU DATA PROTECTION LAW FOR THE PROTECTION OF FUNDAMENTAL RIGHTS: A HYPOTHESIS”, the author of this study will formulate the hypothesis according to which EU data protection law would be an effective and functional legislative framework for the protection of multiple fundamental rights in the digital age. For this purpose:
 - In a first section, the author will discuss the notion of the *effectiveness* of the law by relying on existing scholarly works and explain why, in her opinion, effectiveness alone falls short of characterising EU data protection law;
 - In a second section, the author will then develop the idea that some laws, beyond being effective, are particularly *functional*, and explain how functionality fits into the existing theories on the effectiveness of the law;
 - Finally, in a third section, the author will formulate and explain the hypothesis according to which EU data protection law would be a *multi-functional* framework for the protection of fundamental rights against potentially harmful data processing practices. A distinction will be made between the primary and secondary functionality of EU data protection law. The author of this study will then set the scope within which such hypothesis will be tested.

- In a **second chapter**, entitled “ORIGIN, DEVELOPMENT AND FULFILMENT OF THE FUNDAMENTAL RIGHTS OBJECTIVE OF EU DATA PROTECTION LAW”, the author of this study will retrace the source of EU data protection law, and in particular of its objective to protect the fundamental rights and freedoms of data subjects. It will then be examined to what extent EU data protection law is (or has failed to be) a multi-functional tool for the defence of the fundamental rights and freedoms of the data subject. Through a legislative and case-law analysis, it will be shown in particular that EU data protection law was primarily designed as a bi-functional tool to protect (i) the fundamental right to privacy and/or (ii) the fundamental right to personal data protection. Over the years, its function progressively evolved and was expanded, along with technological developments, to serve other fundamental rights and freedoms of data subjects, such as non-discrimination, freedom of expression or the right to an effective remedy.

- In a **third chapter**, entitled “OUTLINING THE MAIN FACTORS OF FUNCTIONALITY OF THE GDPR FOR THE DEFENCE OF THE FUNDAMENTAL RIGHTS AND FREEDOMS OF DATA SUBJECTS”, the discussion will focus on the main internal factors which – in theory – could make of the GDPR a (multi-)functional legislative framework for the defence of various fundamental rights of the data subjects. Three different pillars of EU data protection law will be analysed in particular (the three “S”): (1) its Scope; (2) its Substance in terms of principles, rights and obligations; and (3) its Supervision and sanction system. In particular:
 - In a first section, this study will focus on the scope of the GDPR and highlight that both the broadness and clarity of that scope, centred around the objective notions of ‘personal data’ and ‘processing’, participate to the overall functionality of EU data protection law.

 - In a second section, this study will focus on the *substance* of the GDPR. In particular, the author will argue that the set of principles, rights and obligations that it contains can be mobilised not only for the benefit of personal data protection, but also for the benefit of other fundamental rights.

 - In a third section, the author will focus on the *supervision and sanction system* of the GDPR, in an attempt to demonstrate that existing control mechanisms allow to detect and put an end not only to infringements of the right to privacy and personal data protection, but also other fundamental rights.

- In a **fourth chapter**, entitled “TESTING THE MULTI-FUNCTIONALITY OF THE GDPR FOR THE DEFENCE OF DIFFERENT FUNDAMENTAL RIGHTS”, the discussion will focus on the

extent and limits of the multi-functionality of EU data protection law by concretely analysing the impact of the GDPR within two ‘test areas’. In particular, the author will define, conceptualise and explain the potential harmful effects of the following data processing practices for individuals’ rights and freedoms: (1) online harassment and related practices, which may interfere with human dignity, the right to the integrity of the person, as well as freedom of expression; and (2) automated decision-making in the field of recruitment, which may interfere with the right to equal treatment and non-discrimination.

- In the **fifth and final chapter**, entitled “SUMMARY FINDINGS, RECOMMENDATIONS & CONCLUSIONS”, the author of this study will summarise her main findings, spell out recommendation and draw conclusions on the legitimacy and desirability of the multi-functionality of the GDPR. This last Chapter will be structured around the following questions in particular:
 - What are the main factors of multi-functionality of EU data protection law, and how to preserve and enhance such multi-functionality? (i.e., summary findings and recommendations).
 - Is it legitimate and desirable to further exploit this secondary functionality for the defence of data subjects’ interests, rights and freedoms, beyond the right to privacy or data protection? (i.e., final reflections and conclusions).

INTRODUCTION – THE EVOLUTION OF DATA PROCESSING PRACTICES AND THEIR IMPACT ON THE FUNDAMENTAL RIGHTS AND FREEDOMS OF DATA SUBJECTS

From the perspective of human rights law, the processing of personal data of individuals is traditionally associated with potential interferences with the right to respect for private and family life (Article 7 of the Charter, also referred to as the ‘right to privacy’) and the right to personal data protection (Article 8 of the Charter). Typical examples of processing practices that may interfere with those two rights include massive surveillance of telecommunication channels by state authorities, or the accidental disclosure of sensitive personal data to the public by private entities. From an historical point of view, the first laws regulating the processing of personal data were thus mainly adopted with a view to protecting individuals against such interferences. Today, this objective is still strongly embodied in EU data protection law, which directly refers to the need to guarantee the respect of the right to privacy and personal data protection.⁴⁵ Besides this strong regulatory framework, the CJEU has also often interpreted EU data protection law in a way that reinforced the protection of the fundamental right to privacy and personal data protection of data subjects (as discussed in Section 2.3, below).

Beyond these two fundamental rights, data processing practices have also started to exponentially affect other fundamental rights. These last two decades, new threats have emerged along with technological developments and changes in social habits. Nowadays, a wide range of DDTs have integrated almost all aspects of our life, thereby broadening the potential situations where fundamental rights can be negatively affected in the context of data processing. When looking for a holiday house on Airbnb, for example, one may be rejected by potential hosts based on a profile picture or a foreign-sounding name, in violation of the right not to be discriminated (Article 21 of the Charter).⁴⁶ By sharing a caricature or a sarcastic opinion on Facebook, one may be subject to automated censorship, which can unduly restrict freedom of expression and information (Article 11 of the Charter).⁴⁷ By looking for ecologically responsible clothing online, one may be micro-targeted by advertisers showing misleading advertising on alleged ‘eco-fashion’, in violation of

⁴⁵ Recital 4 and Article 1(2) GDPR.

⁴⁶ Edelman, B. and Luca, M. (2014). Digital discrimination: the case of Airbnb.com. *Harvard Business School. NOM Unit Working Paper 14-054*; Rutkin A. (2016). Digital discrimination. *The New Scientist*, 231(3084):18-19, p. 18-19.

⁴⁷ Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press; Jhaver, S., Ghoshal, S., Bruckman, A., & Gilbert, E. (2018). Online Harassment and Content Moderation. *ACM Transactions on Computer-human Interaction*, 25(2):1-33

the fundamental right to consumer protection (Article 38 of the Charter).⁴⁸ And through the sharing of personal data on social media, one may suddenly become the centre of a brutal and persistent online harassment campaign which may severely affect their mental well-being,⁴⁹ push them to withdraw from the online world,⁵⁰ or even lead to the death of the victim;⁵¹ hence, online abuses can erode human dignity, freedom of expression, and in most severe cases the right to the integrity of the person (Articles 1, 11 and 3 of the Charter, respectively). These few examples show the diversity of fundamental rights which can be negatively affected by modern data processing practices, beyond the right to privacy and personal data protection. To better understand this phenomenon, the below introductory sections will first clarify some terms and then generally discuss the impact that data processing practices can have on various fundamental rights.

A. TERMINOLOGY

Terms that have been specifically defined in EU data protection law, such as ‘**data subject**’, ‘**personal data**’, ‘**processing**’, ‘**controller**’ or ‘**processor**’ will have the same meaning as the one ascribed to them in the relevant legislation, and in particular Article 4 of the GDPR. With respect to *sui generis* expressions as used in this study, it must be clarified that:

- the expression ‘**data processing practice**’ must be understood as any common practice involving one or multiple operations on personal data by one or various actors through different technological means. For example, sharing videos on social media is a type of data processing practice that includes, at least, (i) the recording of a video by an individual, (ii) the act of uploading it on a social media platform, (iii) its storage by the social media company, and potentially (iv) its sharing among internet users.
- The expression ‘**data-driven technology**’ (**DDT**) must be understood as referring to the technological means behind the processing of personal data. For example, a smart software used by an insurance company to determine

⁴⁸ Turow, J. (2006). *Niche Envy. Marketing Discrimination in the Digital Age*. MIT Press Books; White, R. (2002). Environmental Harm and the Political Economy of Consumption. *Social Justice*, 29(1/2 (87-88)), 82–102.

⁴⁹ As an illustration, one may refer to the ‘Mila affair’ in France. See, among others: Safe A. (2021, June 4). Mila’ trial: 13 in the dock over threats to French teenager who insulted Islam. *The Times UK*. <https://www.thetimes.co.uk/article/mila-trial-13-in-the-dock-over-threats-to-french-teenager-who-insulted-islam-j9pm3rcw8> ; Garaicoechea M. (2021, June 2) Mila vit, à plus grande échelle, ce que vivent toutes les victimes de cyberharcèlement. *Libération*. https://www.liberation.fr/societe/police-justice/mila-vit-a-plus-grande-echelle-ce-que-vivent-toutes-les-victimes-de-cyberharcèlement-20210602_FUGOK3SNIRCIPNZZU74LRNKRGE/.

⁵⁰ See for example the case of Julie Hainaut discussed in Section 4.1, below.

⁵¹ As an illustration, one may refer to the tragic assassination of the French teacher Samuel Paty following a violent online harassment campaign against him. See: Willsher, K. (2021, March 8). Samuel Paty Murder-How a teenager’s lie sparked a tragic chain of events. *The Guardian*. <https://www.theguardian.com/world/2021/mar/08/samuel-paty-how-a-teenagers-lie-sparked-a-tragic-chain-of-events>.

the insurance premiums to be paid by its clients based on a specific set of personal data is a type of ‘data-driven technology’.

- DDTs often include both **hardware** and **software** technologies. The term ‘hardware’ refers to the machinery and electronic parts of the device(s) necessary to perform one or a set of processing operation(s) (e.g., a camera, a USB flash drive, ethernet cables, etc).⁵² The term ‘software’ refers to the programs installed on the device(s) that will initiate and guide these operations.⁵³ For example, to be able to edit and upload a photo on Facebook from a smartphone, both the camera of the smartphone (the hardware) and a photo editing software (the software) are necessary.
- Among software technologies, the term ‘**algorithm**’ is commonly used to describe a set of rules or instructions that a machine (such as a computer) follows to achieve a particular goal.⁵⁴ A *search algorithm*, for example, is a set of rules that allows to search for specific information in a database on the basis of various criteria, and to retrieve such information from the existing mass of data. An *encryption algorithm* is a set of rules that allows to encode information so that unauthorized persons cannot read them.⁵⁵ A *facial recognition algorithm* is a set of rules that allows to analyse photos to identify individuals on the basis of their facial features.⁵⁶ A *categorisation algorithm* may further suggest adding information about *when* or *where* the photo has been taken, based on the digital print attached to the concerned picture.⁵⁷ Algorithms exist independently from any kind of computer or other hardware technologies upon which they may be implemented.⁵⁸ Furthermore, one single software can include many different algorithms. A Customer Relationship Management system, for example (usually referred to as CRM system) may include (i) a search algorithm that enables to quickly retrieve the profiles of a specific customers on the basis of their names, as well as (ii) a product recommendation algorithm that highlights which

⁵² Oxford Advanced Learner’s Dictionary, 10th edition (online).

⁵³ Oxford Advanced Learner’s Dictionary, 10th edition (online).

⁵⁴ Merriam-Webster dictionary (online).

⁵⁵ These two examples are taken from the Merriam-Webster dictionary for the word ‘algorithm’.

⁵⁶ This feature enables Facebook to identify individuals on pictures or videos and – if these individuals have turned on their facial recognition setting – to alert them that a material in which they appear has been uploaded. Individuals may therefore review material uploaded by other users in which they appear. Facebook Help Center explains in this respect: “*Face recognition is used to analyze the photos and videos we think you’re in on Facebook, such as your profile picture and photos and videos that you’ve been tagged in, to make a unique number for you, called a template. When you turn your face recognition setting on, we create your template and use it to compare to other photos, videos and other places where the camera is used (like live video) to recognize if you appear in that content.*” Source: <https://www.facebook.com/help/122175507864081>.

⁵⁷ Facebook Help Center explains in this respect: “*When you take photos, some cameras and cameras on phones add information about where you are, along with the time and date.*” Source: <https://www.facebook.com/help/387124901306972>.

⁵⁸ Sandvig, C., Hamilton, K., Karahalios, K. & Langbort, C. (2016). When the Algorithm Itself Is a Racist: Diagnosing Ethical Harm in the Basic Components of Software. *International Journal of Communication*, 10:19, p. 4976.

customers in the database may be interested in buying a new products on the basis of past purchases, and (iii) a data removal algorithm which automatically delete profiles of customers after a certain period of inactivity.

- Technologies whose aim is to mimic and sometimes surpass the human mind belongs to the field of **Artificial Intelligence (AI)**. Literally, AI refers to the intelligence of machines by contrast to human intelligence.⁵⁹ In the field of computer sciences, AI has been more specifically defined as a “*system’s ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation*”.⁶⁰ Over the last three decades, many different types of AI technologies have been elaborated to support or replace human activities in a wide range of sectors. Examples of AI technologies include robots such as PARO (an advanced interactive robot in the form of a furry seal used for therapeutic purpose),⁶¹ as well as algorithms which have been trained to play chess,⁶² create abstract pieces of art⁶³ or detect tumorous cells by examining images of tissues.⁶⁴
- A ground-breaking advance in the field of AI technology has been to provide machines with the *ability to learn* – a trait which, for long, had only been attributed to living beings. The expression ‘**machine learning**’ precisely refers to AI technologies that are able to automatically learn from past applications and experiences without being explicitly programmed by humans to do so.⁶⁵ Software technologies that have this learning ability are sometimes referred to as ‘smart’ or ‘self-learning’ algorithms.⁶⁶

⁵⁹ In a briefing note, the European Parliamentary Research Service explains in this respect: “*AI has become an umbrella term which can refer to a wide range of methods, both current and speculative. It applies equally well to tools that help doctors to identify cancer as it does to self-replicating robots that could enslave humanity centuries from now.*” See Boucher P. (2019). How artificial intelligence works. EPRS Briefing Note, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI\(2019\)634420_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI(2019)634420_EN.pdf), p. 1.

⁶⁰ Kaplan, A. & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62 (1): 15–25.

⁶¹ Source: <http://www.parorobots.com/>.

⁶² Numerous chess-playing computer software with AI components exist. One of the first is IBM’s Deep Blue supercomputer, who defeated the chess champion Kasparov on 12 May 1997. See Harding, L. & Barden L. (1997, May 12). Deep Blue win a giant step for computerkind. *The Guardian*. <https://www.theguardian.com/theguardian/2011/may/12/deep-blue-beats-kasparov-1997>.

⁶³ Karras & al. (2019). A Style-Based Generator Architecture for Generative Adversarial Network. *ArXiv*. [arXiv:1812.04948v3](https://arxiv.org/abs/1812.04948v3). Using generative adversarial networks (GAN), algorithms may be trained to create realistic looking images of faces, art, cats, etc. The website <https://thisartworkdoesnotexist.com> provides for an infinite number of examples.

⁶⁴ Noorbakhsh-Sabet N., Zand R., Zhang Y., Abedi V. (2019). Artificial Intelligence Transforms the Future of Health Care. *The American Journal of Medicine*, 132(7):795-801.

⁶⁵ The expression ‘machine learning’ is attributed to Arthur Samuel, a pioneer in the field of computer science and artificial intelligence (See Samuel, A. L. (1959). Some Studies in Machine Learning Using the Game of Checkers. *IBM Journal of Research and Development*, 44: 206–226).

⁶⁶ Lonza, A. (2019). *Reinforcement Learning Algorithms with Python: learn, understand and develop smart algorithms for addressing AI challenges*. Packt Publishing.

- **Self-learning algorithms** or **smart algorithms** are initially dependent on humans to gain the ability to learn. Usually, computer scientists feed an algorithm with a huge quantity of data, to which different labels are attached (for example, 10 years-worth of CVs of employees labelled as bad, average or good employees). The algorithm then analyses all these data to discover patterns or correlations between certain **features** or **attributes**, and a pre-defined outcome of interest, usually referred to as the 'target' or '**target variable**' (for example, candidates that are likely to become above-average employees). The set of discovered correlations – which is usually hidden from human sight – is often called a '**predictive model**'.⁶⁷ This predictive model can then be applied on a new set of data (for example, CVs of new candidates) with a view of discovering the sought target. In order to distinguish the target variable from the rest of the data, the algorithm is dividing the data into mutually exclusive categories called '**class labels**' (for example, CVs are either assigned to category A, B, or C, corresponding respectively to the category of 'likely under-average performer', 'likely average performer' or 'likely above-average performer'; then, within category C, the algorithm may further create two mutually exclusive sub-categories, corresponding respectively to 'likely transient employee' or 'likely long-lasting employee').⁶⁸
- The metaphor of the **black box** refers to the lack of transparency of self-learning algorithms.⁶⁹ Indeed, one of the most discussed issues relating to self-learning algorithms is the fact that the data on the basis of which a predictive model is created remain hidden from human sight. This is because, in the process of their development, smart algorithms can become so complex that they become unreadable. As a result, in some instances, only the input and output data can be analysed, but not the in-between process. For example, if a recruiter relies on a smart software to hire new employees, this recruiter will have an overview of all the CVs that have been uploaded into the software (input data) and of the final classification of these CVs as 'good' or 'bad' by the algorithm (output data) but may not know on the basis of which criteria such classification was made by the software. In this example, the in-between process thus remains hidden from human sight, as if taking place in an impenetrable black box.

It is important to clarify at this point that none of the terms listed above appear in the text of the GDPR or any other EU legislation in the field of data protection

⁶⁷ Barocas, S. & Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review*, 104:671, p. 678.

⁶⁸ *Ibid.*

⁶⁹ The black box metaphor dates back to the early days of cybernetics and behaviourism, at the time of the 'Skinner box' experiment realised by Harvard University Prof. B. F. Skinner. Today, it typically refers to a system for which we can only observe the inputs and outputs, but not the internal workings. See, in this respect, Cauer, W. (1941). *Theorie der linearen Wechselstromschaltungen*. Akademische Verlags-Gesellschaft Becker & Erler. Leipzig. ; Ashby, W. R. (1956). *An introduction to cybernetics*. London: Chapman & Hall, pp. 86–117; Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

law.⁷⁰ This is because EU data protection law has been purposefully designed as a technology-neutral framework. Rather than regulating a specific type of technology, it regulates the processing of personal data of natural persons. For this reason, it is said that the GDPR has a human-centric rather than a technology-centred approach.⁷¹ This – together with other elements discussed below – can be seen as a transversal factor contributing to its overall functionality with respect to the defence of human rights.

B. FROM ATOMS TO BITS AND FROM BITS TO ATOMS: UNDERSTANDING THE EXPONENTIAL IMPACT OF DATA PROCESSING PRACTICES ON FUNDAMENTAL RIGHTS

In the 70s, at a time where society was facing its first wave of digitalisation, the main legal challenges relating to the use of computers was to determine “*who has the right to know what about whom*”.⁷² At the very outset of computing technologies, one of the main risks associated with the collection of personal data was the mass surveillance of citizens by state authorities. This risk used to crystallise most of the fears and concerns in relation to computer systems and remains today an important subject of debates.⁷³ As a consequence, the first national laws regulating the processing of personal data largely revolved around setting rules and standards to address this risk and protect the right to privacy of citizens. These concerns were reflected in the wording of 1995 Data Protection Directive (replaced today by the GDPR) as well as in the case-law of the CJEU in the field of data protection law. In all these texts and judgments, particular emphasis is indeed put on the necessity to shield the right to privacy and personal data protection of individuals against intrusive or unlawful data processing practices.

While it is true that, at the end of the 20th century, data processing practices were still quite limited – and largely confined to the collection of personal data of citizens by public actors –, the situation has dramatically changed over the last two decades. During that period, technological developments in the field of computer sciences have not only increased the scale of the collection and sharing of personal data but have also profoundly changed the practices of public authorities, private entities and individuals in relation to those data. The gradual and unstoppable shift “*from atoms*

⁷⁰ As also noted by Boucher P. (2019). How artificial intelligence works. *EPRS Briefing Note*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI_\(2019\)634420_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI_(2019)634420_EN.pdf), p. 1.

⁷¹ European Commission’s High Level Expert Group on Artificial Intelligence (2019, 8 April). Ethics Guidelines on Trustworthy AI. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419, p. 10.

⁷² In French: « *Il y a un problème moral dans ces questions; c’est de savoir qui a le droit de savoir quoi sur qui.* » (Source : interview with Jacques Desabie on 17 September 1975. *Le Journal A2 20H. Informatique : un risque pour les libertés individuelles ?*, archive available at <https://sites.ina.fr/cnil-40-ans/focus/chapitre/2/medias/CAB7501179101>).

⁷³ See, for example, CJEU, Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12, para. 25-28. Incidentally, states’ surveillance also interferes with freedom of expression, as individuals under surveillance might be reluctant to express their opinion by fear of discrimination or retaliation.

to bits” foreseen by Negroponte in its 1995 book “Being Digital”⁷⁴ exponentially went forward.

To better grasp the Negroponte shift, the following numbers can be considered in particular:

- the amount of digital data that is created and stored worldwide is exponentially increasing and is doubling at least every two years;⁷⁵
- in 2021, the share of households with internet access in the EU has risen to 92% (compared to only 70 % in 2011), and more than 94 % of young people in the EU make *daily* use of the internet;⁷⁶
- in the EU, 73 % of individuals aged 16 to 74 have a connected mobile device, such as a smartphone, laptop or tablet computer;⁷⁷
- the proportion of individuals aged 16 to 74 in the EU who ordered or bought goods or services over the internet for private use stood at 66 % in 2021 (compared to only 48 % in 2014);⁷⁸
- in the EU, 57 % of individuals aged 16 to 74 regularly use the internet for social networking on websites such as Facebook, Twitter, Instagram or Snapchat, for sharing personal data with other internet users.⁷⁹

Because of these technological and social changes, DDTs have gradually become essential tools for many individuals who rely on them to conduct their social, financial, educational and/or professional lives.⁸⁰ The COVID-19 pandemic seems to have further accelerated the on-going digital transition of our society out of necessity: private individuals, professionals, public authorities, companies, educational institutions or associations have all started to heavily rely on DDT to continue conducting their activities as normally as possible during the recurring lockdowns which were imposed by state authorities between 2019 and 2021. Today

⁷⁴ Negroponte, N. (1995), *op. cit.*, p. 4.

⁷⁵ This formula is usually referred to as Moore’s Law on computational progress. See Moore, G. E. (1965, April 19). Cramming more components onto integrated circuits. *Electronics*, 38:8.

⁷⁶ Source: Eurostat. Digital economy and society statistics. Households and individuals. <https://ec.europa.eu/eurostat/statistics-explained/>.

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*

⁷⁹ *Ibid.* Among the most popular social media platform, Facebook has around 2.7 billion monthly active users and, on average, more than 300 million photos get uploaded on Facebook every day; similarly, Instagram has more than 1 billion active monthly users, and more than 95 million photos are uploaded on Instagram every day. Source: www.facebook.com.

⁸⁰ Dutton, W. H. & Graham, M. (2014), *op. cit.*

more than ever, digital identities have therefore become important alter egos to one's physical self.⁸¹

It is undeniable that DDT enabling individuals to build a digital identity offer many practical advantages – especially in the midst of a global pandemic – but they can also become a vector for harming individuals through the unlawful use of their personal data. Data leakage, cyber-bullying, online discrimination and behavioural micro-targeting are a few examples of data processing practices that may interfere with data subjects' fundamental rights and freedoms, such as privacy, human dignity, integrity, non-discrimination, consumer protection or freedom of expression and information. In other words, any harm done on personal data in the digital world do not remain within the realm of bits but may reverberate on the atoms; hence, the shift from atoms to bit, rather than being a shift, should be seen as a continuum.

C. THE NATURE AND EXTENT OF THE IMPACT OF DATA PROCESSING PRACTICES ON FUNDAMENTAL RIGHTS

Many data processing practices relying on novel DDTs aim at improving or facilitating processes in various sectors, such as medical care, education, finance, justice or employment, but also entertainment, mobility or consumer's experience. In many cases, DDTs are implemented by private or public actors to increase cost-effectiveness or performances, for example by increasing the accuracy of predictions in the field of healthcare (e.g., a smart algorithm designed to detect cancerous cells in radiographic images of tissues with more accuracy than doctors)⁸² or by assisting teaching staff in the field of education (e.g., an algorithm which detects plagiarism and reduces the workload of the teaching staff).⁸³ Improved performances do not however always imply better protection for individual rights. This is because a lot of DDT are not conceived with the primary objective to ensure the respect of the rights of the data subjects but rather to better serve the interests of the controller. Hence, the impact of DDTs on fundamental rights can either be neutral, positive or negative, depending on their design, purpose or concrete use. As an illustration, a microblogging app such as Twitter can either been seen as a neutral tool allowing various actors to communicate among themselves, as a positive tool which enhances freedom of expression by enabling individuals to share critical opinions with the rest of the world, or on the contrary as a dangerous tool which may allow hate speech or disinformation to proliferate.

⁸¹ As Karel De Gucht, former Prime Minister of Belgium, once stated: "*the twenty-first century citizen (...) seems to develop a digital person that becomes increasingly part of his individual social identity. From this perspective, control over personal information is control over an aspect of the identity one projects in the world.*" See De Gucht, K. (2009). Foreword. In. Gutwirth, S. *Reinventing data protection?* Berlin: Springer, p. vi.

⁸² Svoboda E. (2020). Deep learning delivers early detection. *Nature*, 587:20-22.

⁸³ Both Maastricht University and Luxembourg University, like a majority of universities in the EU, have recourse to anti-plagiarism algorithms. This study itself has been proofed by a plagiarism detection tool called 'iThenticate'.

It is also important to stress at this point that the impact of a DDT may be drastically different from the one that was originally intended by its creator. DDTs that were supposed to have a positive impact on individuals' fundamental rights may end up affecting them negatively if they have been poorly designed or misused. The *Cambridge Analytica* scandal, where thousands of US voters may have been manipulated into voting for Donald Trump,⁸⁴ the *Target* incident, where the pregnancy of a teenage daughter was inadvertently revealed to her father by an algorithm before she could tell him,⁸⁵ or the complaints brought against Facebook for housing advertising discrimination⁸⁶ are obvious examples of how DDT can negatively affect individuals' fundamental rights and freedoms in ways that were not specifically foreseen by their creators. These three examples mainly concerned US citizens rather than EU data subjects. Yet, concerns over the negative effects of such practices and DDTs are vastly shared on the other side of the Atlantic, with academics, businesses, journalists and policymakers issuing many warnings in this respect.⁸⁷

Besides the nature of the impact that a specific DDT may have on a fundamental right (i.e., neutral, positive or negative), the extent of that impact can also greatly vary depending on the situation in which the DDT is being used. Beyond the primary function of the DDT, one must also consider the sector concerned, the specific application at stake, or the existence of particular safeguards. In order the generally

⁸⁴ *Cambridge Analytica* is a British tech company involved in the theft of millions of Facebook profiles in order to use them to build a powerful software program to predict and influence the choice of US voters during the 2016 US presidential election. Source: The Guardian Cambridge Analytica Files. *The Guardian*. <https://www.theguardian.com/news/series/cambridge-analytica-files>.

⁸⁵ In 2012 already, Target – a US retail stores company – was using algorithm that could assign to each female shopper a 'pregnancy prediction score' based on their purchases. Target would then send to those women coupons for baby products. One day, an angry father walked into a Target outside Minneapolis and demanded to see the manager because his teenage daughter had received such coupons, which could be interpreted as a marketing campaign encouraging teen pregnancy. The manager apologised for the error and called the father one week later to reiterate his apologies. However, the father admitted that, in the meantime, he had found out that his daughter was actually pregnant. Source: Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times*. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&hp=&pagewanted=all.

⁸⁶ The U.S. Department of Housing and Urban Development issued an administrative complaint according to which Facebook violated the Fair Housing Act because its targeting systems allow advertisers to exclude certain audiences, such as families with young children or disabled people, from seeing housing ads. Source: Associated Press (2022, June 22). Facebook to axe 'discriminatory' algorithm in US government settlement. *The Guardian*. <https://www.theguardian.com/technology/2022/jun/21/facebook-lawsuit-settlement-advertising-lookalike-audience-doj>

⁸⁷ See, for example, Council of Europe (2019, February). Conference report on impacts of artificial intelligence development on human rights, democracy and the rule of law. <https://rm.coe.int/conference-report-28march-final-1-168093bc52>; European Political Strategy Centre. (2018, March). The Age of Artificial Intelligence. European Commission. https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf; European Union Agency for Human Rights (2019, June). Paper on Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf; Zuiderveen Borgesius, F. J. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe. <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> ; AlgorithmWatch (2019, January). Automating Society: Taking stock of Automated Decision Making in the EU. https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf; Yavuz, C. (2019). *Machine Bias: Artificial Intelligence and Discrimination*. Web version. doi: 10.13140/RG.2.2.10591.61607; Kari, P. (2019, April 17). 'Disastrous' lack of diversity in AI industry perpetuates bias, study finds. *The Guardian*. <https://www.theguardian.com/technology/2019/apr/16/artificial-intelligence-lack-diversity-new-york-university-study>.

illustrate the various levels of impact posed by the same DDT depending on the overall context, one may refer to classification and recommendations algorithms in two different sectors: the entertainment sector on the one side, and criminal justice on the other side.

In the entertainment sector, companies like Spotify, Audible or Netflix have developed classification and recommendation algorithms that analyse their subscribers' profile and preferences with a view of recommending new products. Similarly, in the sector of media, including social media, the content and structure of news report or so-called 'newsfeed' may be personalised depending on the profile and interests of each user, on the basis of selected preferences or previous 'clicks'. These classification and recommendation algorithms – because of their function and the sectors concerned – do not seem to pose serious or immediate threats for individuals' rights and freedoms. It has been argued, however, that they could participate to the creation of "filter bubbles".⁸⁸ This expression refers to a digital state where users always get what they want to see, read or hear and are therefore not confronted with novelty or contradicting viewpoints, which may in turn cause a state of intellectual isolation.⁸⁹ In the political sphere, for example, such filter bubbles could exacerbate polarisation and thus be detrimental to healthy democratic debates. EU experts and scholars are however challenging the idea of completely 'closed' filter bubbles where individuals would be hopelessly trapped in an echo chamber. In most instances indeed, users remain free to disregard recommendations or to deactivate content personalisation.⁹⁰ Furthermore, individuals' preferences or opinions do not exclusively develop within the digital sphere, but also in the physical one – for example, through interactions with colleagues, family members, and friends, or via traditional media, such as newspaper or national TV news. According to experts, the negative effects of classification and recommendation algorithms in the media and entertainment sectors would thus remain relatively benign as far as individuals' rights are concerned,⁹¹ or may even be positive when they trigger more engagement or subsequent exposure to diverging views.⁹²

⁸⁸ The term was first coined by Internet activist Eli Pariser (Pariser, E. (2012). *The Filter Bubble, How the new personalized web is changing what we read and how we think*. Penguin Random House).

⁸⁹ Zuiderveen Borgesius, F. J., Trilling, D., Möller, J., Bodó, B., de Vreese, C. H. & Helberger, N. (2016). Should we worry about filter bubbles? *Internet Policy Review*, 5(1). DOI: 10.14763/2016.1.401

⁹⁰ *Ibid.* See also: Hosanagar K., Fleder D., Lee D. & Buja A. (2013). Will the Global Village Fracture into Tribes? Recommender Systems and their Effects on Consumers. *Management Science*, 60:4; Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter Bubbles, Echo Chambers, and Online News Consumption. *Public Opinion Quarterly*. 80:298–320.

⁹¹ From the perspective of competition law, however, recommendation algorithms may procure an unfair competitive advantage which would negatively affect the market and thus ultimately consumers' rights. Google search algorithms (displaying the most relevant results based on the individual's location, language preferences, search history, etc.) or Amazon recommendation algorithm (which recommend new items based on past purchases). Furthermore, the psychological and societal impact of recommendations algorithms as a vector of polarization between different groups is also deemed important.

⁹² Fletcher, R. & Jenkins, J. (2019, March). Study on polarisation and the news media in Europe. EPRS. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU\(2019\)634413_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU(2019)634413_EN.pdf).

By contrast, in other sectors such as medical care or justice, recommendation or classification algorithms may have a substantial impact on individuals' rights and freedoms, especially when they can influence or even determine the result of a decision-making process which will have consequences on the life of the data subjects. Decision-making processes ruled by algorithms are usually referred to as "*algorithmic decision-making*" (ADM).⁹³ A well-known example of ADM which has been widely covered by the media is the software COMPAS. This algorithm is used by several criminal courts in the US in order to assess the likelihood of a defendant becoming a recidivist. For each defendant, COMPAS analyses more than 100 personal entries such as the age, civil status or criminal background of the defendant, but notably excluding race. Based on these data, the algorithm then assigns to each defendant a personalised 'risk score' from 1 to 10, i.e., from low to high risk of recidivism. When defendants are assigned a medium to high-risk score between 5 and 10, judges are logically more likely to take harsher bail or sentencing decisions. It is important to specify that COMPAS does not replace the judge but rather makes suggestion to the latter and can thus be qualified as a mere recommendation or classification algorithm. Yet, it must be acknowledged that – because of its influence on the decision of the judge –, this DDT is likely to significantly affect the life of the defendants concerned. Any flaw in COMPAS could thus potentially systematised a discriminatory system of bail and sentencing decision. This was highlighted by two journalists of the newsroom ProPublica⁹⁴ who, after analysing the cases of about 5000 defendants who were assigned a risk score by COMPAS, concluded that the algorithm was biased, as it was more likely to give a high-risk score to African-American defendants who did not reoffend than to white defendants who did not reoffend. In other words, the African-American community was experiencing a higher rate of 'false positives' than other communities. The journalists pointed out that an algorithm designed to bring more consistency and fairness into the criminal justice system should not make such errors more frequently for one race group than for another.⁹⁵

Following the publication of ProPublica's article, other journalists and scholars looked into the issue. Some pointed out that achieving full equality in the level of false positives in different race groups might not be possible without creating reverse discrimination issues, given that the actual number of offenders in different

⁹³ This expression is used in particular by the Council of Europe in its study on algorithms and human rights: Council of Europe (2017). Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>. In the EU, when an ADM produce legal effects or similarly significant effects on the individuals concerned, it will qualify as "*automated individual decision-making*" (AIDM) as regulated under Article 22 GDPR. See section 3.2.2.2(v), below.

⁹⁴ *ProRepublica* presents itself as an independent, non-profit newsroom that produces investigative journalism in the public interest. See more at www.prorepublica.org.

⁹⁵ The company that elaborated COMPAS (Equivant) refuted *ProRepublica*'s findings but refused to disclose the details of its proprietary algorithm. Source: <https://www.equivant.com/response-to-propublica-demonstrating-accuracy-equity-and-predictive-parity/>.

race groups was not equal in the field.⁹⁶ Furthermore, despite the existence of potential flaws, it was also pointed out that the use of COMPAS could remain beneficial to defendants compared to situations where a human judge would be deciding each case without any recommendation algorithm. Human judges have indeed proven to suffer from many biases and/or to take inconsistent decisions depending on external factors, such as whether they had an empty stomach at the time of ruling on a case.⁹⁷ Hence, even if COMPAS was producing ‘false positives’ and ‘false negatives’, its use by criminal courts helped decreasing the overall number of inconsistent or discriminatory decisions made by human judges.

Regardless of the possible flaws of COMPAS and of its overall positive or negative impact for the right to due process or non-discrimination of defendants, this example clearly shows that, depending on the sector in which they are used, mere classification and recommendation algorithms can still significantly affect protection of individuals’ rights and freedoms.

⁹⁶ Flores, A., Bechtel, K. & Lowekamp, C. (2016). False Positives, False Negatives, and False Analyses: A Rejoinder to ‘Machine Bias. *Federal Probation Journal*, 80:2.

⁹⁷ A study from Columbia University found that the likelihood of a favourable ruling is greater at the very beginning of the workday of the judge or after a food break than later in the sequence of cases. See Danziger, S. & al. (2011). Extraneous Factors in Judicial Decisions. Daniel Kahneman (ed.). *Proceedings of the National Academy of Sciences of the United States*, 108: 17, pp. 6889–6892.

TABLE 1

The below table⁹⁸ give examples of different DDT used to support or replace human decision-making. The level of risk for individuals (white = low risk; yellow = medium risk; orange = serious risk) has been assessed on the basis of three criteria (1) the possibility to depart from the decision (cf. recommendation vs binding decision) ; (2) the legal effect or similarly significant effects that the decision can have on the individuals (e.g. the conclusion of a contract); and (3) the number and/or complexity of the factors that have been used to reach a decision, as it may increase the chance of errors (e.g. inaccurate data) or lead to a lack of transparency (e.g. unknown factors).

Level of risks association with DDT used to support or replace human decision-making						
	Education	Entertainment	Healthcare	HR	Insurance	Mobility
Classify	Rank students on the basis of their grades	Analyze & classify music preferences depending on users' profile	Classify medical research on a topic by relevance / quality	Classify employees by level of seniority	Classify insurers by risk profiles (based on age, gender, etc.)	Search all the possible itineraries to go from point A to point B.
Recommend	Recommend study tracks to students based on their skills, preferences and competences.	Recommend movies, music or (audio) books to customers/ subscribers based on their profile	Recommend treatment(s) to patients based on symptoms and other health data	Recommend jobs to individuals / employees to companies based on their competences	Recommend an insurance scheme to a person based on his/her profile (age, gender, etc.)	Recommend the best itinerary based on the price, duration or environmental impact
Match	Distribute graduates among various universities	Match people based on their affinities (dating website)	Match patients with a special diet to help them in their recovery	Match job seekers with potential employers	Match an individual with a proper pension plan	Match a driver with passengers travelling in the same direction
Predict	Predict failure rate for the coming year	Predict the number of subscribers of a media-services provider in the next year	Predict risks of developing a specific cancer	Predict the need to hire new employees in the future	Predict the costs of specific groups of insured persons (e.g., smokers)	Predict traffic based on data from previous days/years
Decide	Accept / reject the application of prospective students	Automatically order the next book/movie to be delivered to the subscriber	Sort patients depending on the type of emergency ("triaging")	Accept / reject an application for a job	Accept / reject an application for an insurance	Activate the brake of a vehicle because an obstacle has been detected

⁹⁸ This table has been largely inspired by a table published by the CNIL in a 2017 report, although the sectors have been altered and the examples modified by the author of this study (see CNIL (2017, December). Comment Permettre à l'Homme de Garder la Main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf, p. 22.

Because EU data protection law regulates the processing of personal data and because all DDTs involve by default some sort of personal data processing, EU data protection law could potentially be used to detect, prevent and/or combat the harmful effects of DDTs on any fundamental right of the concerned data subjects. On the basis of this preliminary assumption, the first Chapter of this study, here below, will spell out more specifically the hypothesis that EU data protection law could be used as a multi-functional framework for fundamental rights protection in the digital sphere.

CHAPTER 1 – THE MULTI-FUNCTIONALITY OF THE GDPR FOR THE PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS: A HYPOTHESIS

Foreword

The notion of ‘legal functionality’ has been imagined by the author with a view of better understanding and characterising EU data protection law. Hence, it is important to clarify what is meant by it. For this reason, this Chapter will first discuss the notion of the *effectiveness* of the law, as defined in the relevant literature (section 1.1), before putting it in relation with the notion of the *functionality* of the law (section 1.2). Subsequently, the hypothesis according to which EU data protection law could be used as a multi-functional framework for fundamental rights protection will be spelled out, along with a distinction between the primary and secondary functionality of EU data protection law (section 1.3).

1.1. OVERVIEW OF THE NOTION OF ‘EFFECTIVENESS OF THE LAW’

1.1.1. Effectiveness in the legal jargon

In the field of public international law, the term ‘effective’ is primarily used in relation to the recognition, by the international community, of statehood, nationality, territorial occupation, annexation or maritime blockade.⁹⁹ In this context, effectiveness is thus understood as the factual existence of a given situation. Having a stable and *effective* government, for example, is one of the conditions for a state to be recognised as such under public international law.¹⁰⁰ In the field of EU law, by contrast, effectiveness is usually understood as the concrete application of EU law *itself* on the territory of the Member States. Indeed, if EU law would neither be respected nor applied by Member States, it would be ineffective in the sense that the objectives of the EU could not be achieved.¹⁰¹ Since the 60s, different principles elaborated by the Court of Justice of the European Union (CJEU)¹⁰² have participated to the effectiveness of EU law. Among those principles, one may point out in particular: the principle of primacy of EU law,¹⁰³ the principle of direct effect of EU law¹⁰⁴ and the principle of state liability.¹⁰⁵ If

⁹⁹ Shaw, M. (2017). *International law* (8th ed.). Cambridge: Cambridge University Press.

¹⁰⁰ Cohen, R. (1961). The Concept of Statehood in United Nations Practice. *University of Pennsylvania Law Review*, 109(8), pp. 1127-1171.

¹⁰¹ One of the original and primary objective of the EU being the establishment and functioning of an EU-wide market where goods, services and workers can freely move in accordance with a harmonized set of rules.

¹⁰² The CJEU was previously called the European Court of Justice. For the sake of clarity, however, the author will use the abbreviation ‘CJEU’ to refer to this institution, regardless of the period concerned.

¹⁰³ According to which, in the event of a conflict between an EU norm and a national norm, the EU norm must prevail. CJEU, Judgment of 15 July 1964, *Flaminio Costa v E.N.E.L.*, Case 6/64.

the effectiveness of EU law had not been built and reinforced on the basis of these principles, the EU Treaties might have become a dead letter rather than the textual foundations of a new legal order.

For the purpose of clarity, a sharp distinction must be drawn between the meaning of 'effectiveness' under public international law and under EU law. In the case of public international law, the notion of effectiveness is not attached to the application of the law itself, but to the existence of *a factual situation* which – if 'real' or sufficiently substantiated by facts – may then be granted a legal qualification. In the second case, by contrast, the idea of effectiveness of EU law is attached to the concrete application of EU law *itself*.¹⁰⁶ In this Chapter, the term effectiveness must be understood in this second sense. Indeed, this Chapter will discuss the effectiveness of *the law itself*, with a view of further developing a related notion, i.e., the functionality of the law.

1.1.2. The narrow, broad and wide approach to the effectiveness of the law

In its traditional narrow sense, the effectiveness of the law is understood as the actual application of the law by the concerned actors.¹⁰⁷ Concrete application entails that the persons to whom the law is addressed *comply* with it, and that the competent authorities *enforce* it. Therefore, if the provisions of a law are fully respected by the concerned persons, or if their violation gives rise to a sanction, it could be concluded that the law is effective. By contrast, if a law is being widely infringed, circumvented or ignored, and if the authorities fail to ensure its respect by issuing injunctions or pronouncing sanctions, it could be argued that the law is not properly applied and is therefore ineffective. In accordance with that traditional approach, the effectiveness of any norm can thus be assessed on the basis of two aspects of its application: the compliance aspect (i.e., do people respect the law?), and the enforcement aspect (do the competent authorities, including the courts, control the respect of the law and pronounce sanctions where necessary?).¹⁰⁸ Regarding sanctions in particular, their primary function is often perceived as ensuring the respect of the law through their deterrent effect, or as re-establishing

¹⁰⁴ According to which any norm of EU law which is binding, clear and unconditional can be directly invoked before and applied by national courts. CJEU, Judgment of 5 February 1963, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration*, Case 26/62.

¹⁰⁵ According to which Member States can be held liable for any of their actions or omissions infringing EU law. CJEU, Judgment of 19 November 1991, *Francovich*, Joined cases 6/90 and 9/90.

¹⁰⁶ The effectiveness of EU law should not be confused with the principle of effectiveness and equivalence under EU law, which are concerned with the right to effective judicial protection and the right to remedies of natural and legal persons in the case of an infringement of EU law, in adherence to the principle of procedural autonomy of national courts. See for this purpose: CJEU, Judgment of the Court of 16 December 1976, *Comet v Produktschap*, Case 45/76 ; CJEU, Judgment of the Court of 16 December 1976, *Rewe v Landwirtschaftskammer Saarland*, Case 33/76, para 8.

¹⁰⁷ Rangeon F. (1989). *Réflexions sur l'effectivité du droit*. Danièle Lochak & al. *Les usages sociaux du droit*. Paris : P.U.F., pp. 126-146.

¹⁰⁸ Kelsen H. (1962). *Théorie pure du droit*. Paris : Dalloz, p. 15 ; Leroy, Y. (2011). La notion d'effectivité du droit. *Droit Et Société*, 79(3), p. 719.

compliance with the law by punishing infringers.¹⁰⁹ In that sense, the existence of a solid supervision and sanction system is often considered as a determining factor for ensuring the effectiveness of a law.

As duly noted by Yann Leroy however, this narrow approach of the effectiveness of the law is somewhat reductive, since it presupposes that all legal norms are imperative.¹¹⁰ Having regard to the immense variety of existing laws, one must however admit that not all norms are mandatory, and that not all norms are accompanied by sanctions.¹¹¹ As an illustration, corporate law does not impose on people the obligation to set up a limited liability company, and family law does not oblige individuals to marry. Rather, these rules offer to individuals the *possibility* to do so. Furthermore, if a married couple wishes to divorce, no sanction will be inflicted on them for failure to stay together. Similarly, if a company files for bankruptcy, no sanction will be pronounced against the managers or directors for failure to keep the business afloat. Data protection law itself includes non-imperative provisions which do not need to be backed up by sanctions. Binding corporate rules (BCR), for example, is a system that corporations may decide to adopt in order to secure intra-group transfers of personal data.¹¹² Adopting BCR is however not an obligation but rather an option. Hence, the decision *not* to adopt BCR, or the decision to dissolve BCR and adopt another regime for international data transfers, will not lead to any sanction.¹¹³ Yet, it would also be incorrect to conclude that norms on divorce, bankruptcy or BCR are ineffective because they are not imperative. The effectiveness of legal norms can thus not exclusively be assessed on the basis of *compliance or enforcement*.

On this basis, some authors have proposed a broader approach to the notion of the effectiveness of the law, which is not exclusively linked to its effects in terms of compliance or enforcement. François Rangeon, for example, argues that assessing the effectiveness of a law requires an analysis of its overall social uses – i.e., the behaviour of societal actors toward the law.¹¹⁴ Opting for a sociological approach rather than a purely legalistic one, he argues in particular that legal norms also produce *symbolical* effects that are not always tangible or measurable,¹¹⁵ but which may explain why legal norms are sometimes spontaneously or unconsciously adopted or used by their addressees.¹¹⁶ Therefore, according to Rangeon, the effectiveness of a law should be assessed by taking into account its various effects on

¹⁰⁹ Le Fur, L. (1935). Les caractères essentiels du droit en comparaison avec les autres règles de la vie sociale. *Archives de philosophie du droit*, p. 7 ; in the area of criminal law, see in particular Foucault, M. (1989). *Surveiller et punir : Naissance de la prison*. Paris: Gallimard.

¹¹⁰ Leroy, Y. (2011), *op. cit.*, p. 719-720.

¹¹¹ Leroy, Y. (2011), *op. cit.*, p. 722, referring to Troper, M. (2003). *La philosophie du droit*. Paris : PUF, p. 70.

¹¹² Article 4(20) of the GDPR defines binding corporate rules (BCR) as personal data protection policies which are adhered to by a controller or a processor located in the EU for transfers of personal data to one or multiple controller(s) or processor(s) which are part of the same group but which are located in a third country.

¹¹³ Article 46 and 47 of the GDPR further explain the specificities of this regime for data transfers, if adopted

¹¹⁴ Rangeon F. (1989), *op. cit.*, p. 134.

¹¹⁵ *Ibid.*, p. 130 and 138.

¹¹⁶ *Ibid.*, p. 144.

society, including its visible effects, symbolical effects, undesired effects or unforeseen effects.¹¹⁷ Rangeon warns, however, that not all the effects of a law must be considered as evidence of its effectiveness.¹¹⁸ On the contrary, some effects may demonstrate a *lack* of effectiveness. As an illustration, if the main effect of a law is that social actors creatively put in place various mechanisms in order to circumvent it (e.g., because compliance with the law is too burdensome), this will participate to the *ineffectiveness* of that law in the long run.¹¹⁹

Finally, a minority of legal scholars have proposed an even wider approach to the notion of effectiveness, by arguing that *all* the effects of a law should be regarded as evidence of its effectiveness, including negative or perverse effects.¹²⁰ If that definition would be accepted, the notion of *effectiveness* of the law would merge with the notion of the *effects* of law.¹²¹ Indeed, any effect would be a sign of effectiveness, regardless of whether this effect would be good or bad for achieving the intended results of the law. According to this interpretation, the fact that some actors would try to circumvent a specific tax rule, for example, would constitute evidence of its effect or influence on society, and therefore of its effectiveness. This very wide approach to the notion of legal effectiveness is however questionable if one keeps in mind the original meaning of the word. As already mentioned above indeed, 'effectiveness' is generally defined as *the degree to which something is successful in producing a desired result*. Two elements therefore appear particularly important to structure any reflection around the notion of effectiveness of a legal norm: (a) what was the *desired result(s) of the legal norm*?; and (b) were these results achieved to a *successful extent* because of the effects that the law had on society?

In line with Rangeon's approach, Yann Leroy also defends the idea that the effectiveness of a legal norm ultimately depends on the successful fulfilment of its objective(s).¹²² In accordance with this goal-oriented approach, a law will be considered more or less effective depending on whether its overall effects have enabled the achievement of its intended results. For this purpose, one must consider the various effects that the law had on the concerned actors or on society as a whole.¹²³ All types of effects can be taken into account: intended or unintended effects, foreseeable or unforeseeable effects, measurable or symbolic effects, etc. Among those effects however, only those which have participated to the achievement of the objectives of the law should be considered as *increasing* its

¹¹⁷ *Ibid.*, p. 140.

¹¹⁸ *Ibid.*, p. 128.

¹¹⁹ *Ibid.*, p. 140-142.

¹²⁰ Valérie Demers and Guy Rocher are two scholars who seem to defend this wider notion of effectiveness. See in particular, Rocher G. (1998). *L'effectivité du droit*. Lajoie, A. & al. *Théories et émergence du droit : pluralisme, surdétermination et effectivité*. Montréal: Thémis, p. 134 ; Demers, V. (1996). *Le contrôle des fumeurs. Une étude d'effectivité du droit*. Montréal : Thémis, p. 3.

¹²¹ This is also noted by Leroy, Y. (2011), *op. cit.*, p. 729.

¹²² Leroy, Y. (2011), *op. cit.*, p. 730.

¹²³ This approach corresponds to the approach of Yann Leroy, but also to some extent of François Rangeon or Geneviève Pignarre.

effectiveness. By contrast, perverse or negative effects that are at odds with the objectives of the law should be considered as *decreasing* its effectiveness.

1.1.3. A goal-oriented approach to legal effectiveness

In the context of this study, the author believes that the goal-oriented approach to legal effectiveness is the most valid approach for several reasons. First, this approach is undeniably more in line with the original and general meaning of the word 'effectiveness', which relates to the degree to which something is successful in achieving a *desired result*. In the opinion of the author, the 'desired result' of a law can be found by looking into its objectives, as spelled out by the legislator or the courts. Such objectives can indeed either be explicitly laid down in the text of the law itself or implicitly be found in the relevant case-law.¹²⁴ In both cases, a law should be considered as *effective* if its overall effects have enabled the achievement of those explicit or implicit objectives. In that sense, the goal-oriented approach to legal effectiveness matches the terminological meaning of 'effectiveness'. Second, this approach tends to reconcile the classical approach with the more modernist approach to the notion of legal effectiveness, by englobing the first into the second. Under the traditional approach, the effectiveness of a law is assessed based on two aspects of its application: compliance and enforcement. Those aspects are also covered by the modernist approach. However, the modernist approach does not only examine the effects of a law in terms of compliance or enforcement but also *any other effects* that contribute to the achievement of the objectives of the law. The modernist approach is thus more englobing because it enables to assess the effectiveness of legal norms that do not necessarily impose obligations on persons, or that are not necessarily accompanied by sanctions. Since non-imperative norms form an integral part of many laws, the modern approach to legal effectiveness enables to apprehend each law in its entirety, rather than focusing on imperative norms only. In the field of data protection, for example, there exist several non-imperative norms, such as the possibility for group of companies to adopt BCR (as mentioned above) or the possibility for controllers or processors to voluntarily appoint a data protection officer even when they are not under the obligation to do so.¹²⁵ Third, this goal-oriented approach seems to offer a better framework for methodological research, since it circumscribes the appreciation of legal effectiveness to the concrete fulfilment of the objectives of a law, rather than to the unlimited field of its direct or indirect effects on society. At the same time, this

¹²⁴ Over time, depending on the interpretation given by the competent courts, the objectives of a law may vary, and new objectives may be revealed. As an illustration, the object of right to privacy (enshrined in Article 8 of the European Convention of Human Rights and in Article 7 and in the EU Charter of Fundamental Rights) was primarily envisaged as protecting individuals from illegitimate surveillance or disproportionate intrusion by the state into their private life. Over time however, the object of this right was broadened by the European Court of Human Rights to include, inter alia, a right to establish and maintain relationships with other individuals, or a right to informational self-determination. Today, the question whether the right to privacy is an effective right or not will therefore depend on whether such a right enables the achievement of its original but also of its 'novel' objectives.

¹²⁵ With respect to the possibility to appoint a DPO, please see Article 37(4) GDPR.

notion of effectiveness remains flexible since it allows to take into account the different objectives pursued by a law (e.g., explicit or implicit, unitary or multiple, complementary or divergent, etc). Data protection law, for example, pursues various objectives, and the effectiveness of each set of data protection rules should therefore be appreciated in light of the objectives that they each pursue respectively.¹²⁶ Finally, according to this goal-oriented approach, the extent to which an objective has been successfully achieved can be appreciated taking into account the various effects of the law, as well as the internal or external factors that may have influenced such effects (e.g. clarity of the text, existence of stringent sanctions, material or procedural obstacles, social or cultural context, corruption among controllers, etc). In conclusion, the goal-oriented approach to legal effectiveness, by encouraging to look into the effects of legal norms from an inter-disciplinary perspective, enables to establish a more comprehensive and accurate picture of the strong or weak points of any law in achieving its objective(s).

1.1.4. The internal and external factors of legal effectiveness

Agreeing on a conception of effectiveness does not mean that the effectiveness of legal norms can be assessed on the basis of a fixed set of criteria or a unique method. This is because the factors behind legal effectiveness are not systematically the same. Due to the immense variety of legal norms, the relevance of some factors as well as their degree of influence on the achievement of those norms' objectives can indeed greatly differ. Quite obviously, one does not measure the effectiveness of the EU Charter of Fundamental Rights in the same way than a Regulation fixing the export refunds on raw sugar.¹²⁷

In the opinion of the author, among the factors that may influence the effects of a law, a further distinction can be drawn between *internal* or *external* factors of effectiveness. For the sake of clarity, 'internal factors' should be understood as any factors which may be found *in the text of the law itself* and which participate to its effectiveness, such as the clarity of its content or the existence of deterrent sanctions. 'External factors', by contrast, should be understood as any facts or circumstances that cannot be found in the legal text itself but that will positively or negatively influence the effectiveness of that law, such as the social customs and legal culture of a country, or the resources given to the public authorities in charge of enforcing the law. Among those external factors, some may furthermore be

¹²⁶ The 1995 Data Protection Directive, and later the GDPR, have been pursuing the two main objectives: (1) the protection of individuals' fundamental rights, and in particular their right to privacy and data protection and (2) ensuring the free flows of personal data between Member States. Some provisions of data protection law therefore aim at ensuring the respect of the fundamental right to personal data protection, while other tend to facilitate the free flow of personal data. In between, many provisions aim at reconciling both objectives by allowing data flows while providing for strict safeguards in this respect. See Article 1 of the 1995 Data Protection Directive and Article 1 of the GDPR.

¹²⁷ By analogy to Rangeon, *op. cit.*, p. 134 (« *On ne mesure pas l'effectivité d'un article de la Déclaration des droits de l'homme de la même manière qu'on mesure celle d'une loi technique concernant la commercialisation des céréales* »).

horizontal, in the sense that they will not only affect the effectiveness of *one* law but of a wide variety of laws (for example, the fact that the judicial system of a given country is characterized by high-costs and backlogs), or *vertical*, in the sense that they would only affect a specific type of laws (for example, a high level of voluntary compliance with norms on gender equality may be less common in a culturally patriarchal society than in a culturally egalitarian society). When drafting a legal text, a legislator should thus have an accurate picture of all the external factors that could influence the functioning of that law in order to adapt its content as much as possible to the concerned sector or jurisdiction in a manner that could maximize its effectiveness.

Both internal and external factors can be determining in understanding the effectiveness of legal norms. Analysing *all* the factors that can influence the effectiveness of a legal norm may however prove to be impossible, since external factors in particular are potentially unlimited and are likely to evolve over time. When assessing the effectiveness of a given norm, it is therefore important to establish a limited scope with respect to (1) the legal *objectives* under scrutiny and (2) the *main factors* which have proven to influence the fulfilment of those objectives. As noted by Rangeon, if the assessment framework is too broad or unspecific, it might become unsuitable to draw valid conclusions. By contrast, if the assessment framework is too restrictive or inadequate, it could lead to partial or misleading conclusions.¹²⁸ Before looking into the factors that affect the effectiveness of a law, a pre-observational phase is thus necessary, during which the objectives of the law as well as its most conspicuous flaws should be identified.¹²⁹ This, in turn, should allow to limit the scope of the research on identifying the factors causing those flaws. Such observations can be made on the basis of existing empirical data (for example, statistical data computed by the relevant authorities that show low rate of compliance and/or enforcement) or new empirical data (for example, by conducting a survey on the clarity of the law, or by analysing how the law is enforced in case-law). The more empirical data may be used to identify the effects of a given law, the more accurately those preliminary observations can be made, which in turn should help establishing an adequate assessment framework.

Despite the difficulties that it entails, assessing the effectiveness of the law is one of the traditional missions of legal scholars.¹³⁰ Effectiveness becomes an object of concern in particular for scholars who wish to close the gap between legal theory and practice, abstraction and reality.¹³¹ Their purpose is usually to identify shortages or obstacles that restrain the effectiveness of a law before formulating recommendations in order to improve the fulfilment of its objectives (for example, by proposing amendments to the law, highlighting state-of-the-art practices or

¹²⁸ Rangeon F. (1989), *op. cit.*, p. 137.

¹²⁹ *Ibid.*, p. 139.

¹³⁰ Rangeon F. (1989), *op. cit.*, p. 135.

¹³¹ Jeammaud A. (2006). Le concept d'effectivité du droit. Ph. Auvergnin (ed.). *L'effectivité du droit du travail : à quelles conditions ?* COMPTRASEC, p. 34.

encouraging the reform of enforcement procedures). Besides scholars, governmental and non-governmental organisations also often seek to identify ineffective laws in an attempt to stir reforms. As far as non-governmental organisations (NGOs) are concerned, denouncing ineffective laws and calling for reforms is usually an important part of their activities.¹³² As far as governments or public authorities are concerned, ensuring the effectiveness of the laws and policies that they have adopted is usually part of their mandate, and may also play a major role in whether such a mandate will later be renewed by their electorate.¹³³ At the EU 'governmental' level, the REFIT programme offers an illustration of this quest for legal effectiveness.¹³⁴ REFIT stands for *Regulatory Fitness and Performance Programme*. Through this programme, the Commission evaluates EU regulations, directives and other instruments of EU law in selected policy fields in order to ensure that they deliver their intended benefits. Effectiveness is one of the key aspects of this evaluation.¹³⁵ For this purpose, workshops and roundtables are organised, surveys are carried out, studies from expert groups are requested, consultancy firms or research institutes are mandated, and the opinions of relevant authorities, citizens and other stakeholders are collected. Based on these data, recommendations are then issued by the REFIT Platform to the Commission with a view of stirring appropriate reforms.¹³⁶ In the field of data protection law for example, the e-Privacy Directive¹³⁷ has been subject to such an evaluation.¹³⁸ Among

¹³² In its yearly reports, Amnesty International regularly points out the (lack of) legislative reforms in countries where human rights are violated. In the EU, the Fundamental Rights Agency (FRA) also writes reports and deliver advice to policy makers in the EU and its Member States. On the subject of NGOs lobbying for legal changes, see, for example: Cáceres, S. B. (2012). NGOs, IGOs and International Law: Gaining Credibility and Legitimacy through Lobbying and Results. *Georgetown Journal of International Affairs*, 13.1: 79-87; Murazzani, M. (2009). NGOs, Global Governance and the UN: NGOs as "Guardians of the Reform of the International System". *Transition Studies Review* 16.2: 501-09; Nurse, A. Privatising the Green Police: The Role of NGOs in Wildlife Law Enforcement. *Crime, Law and Social Change* 59.3 (2013): 305-18; Longhofer, W., Schofer E., Miric N. & Frank D. J. (2016). NGOs, INGOs, and Environmental Policy Reform, 1970–2010. *Social Forces* 94.4: 1743-768.

¹³³ When a new government from an opposition party is elected, however, its intent might be to deconstruct what the previous government has achieved in terms of legal reforms. In that case, it is likely that no reform will be undertaken to ensure the effectiveness of previous laws. On the contrary, the new government might be tempted to slow down control or enforcement to later argue that the laws adopted by its predecessor have failed to fulfil their objectives.

¹³⁴ The REFIT programme is part of the Commission's better regulation agenda and is thus pursued by the European Commission with the assistance of Member States' governments, experts and stakeholders.

¹³⁵ Evaluations under the REFIT programme cover 5 key aspects: (1) effectiveness, i.e., whether the EU action reached its objectives; (2) efficiency, i.e., what are the costs and benefits; (3) relevance, i.e., whether it responds to stakeholders' needs; (4) coherence, i.e., how well it works with other actions and legislation; and (5) EU added value, i.e., what are the benefits of acting at EU level rather than at the national level. Source: https://ec.europa.eu/info/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-and-less-costly_en.

¹³⁶ The REFIT platform was set up in May 2015 by the Better Regulation Communication (COM(2019) 178 final). Its mission is to advise the Commission on how to make EU regulation more efficient and effective. The REFIT Platform consists of a Government Group, with one seat per Member State and a Stakeholder Group with 18 members and two representatives from the European Social and Economic Committee and the Committee of the Regions.

¹³⁷ Directive 2002/58/EC (the e-Privacy Directive) ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector. It is considered a *lex specialis* to the 1995 Data Protection Directive, replaced in 2016 by the GDPR.

the factors that had negatively impacted the effectiveness of the e-Privacy Directive, the REFIT Platform identified one external factor in particular: the technological and economic developments which had taken place in the market since the last revision of the e-Privacy Directive in 2009.¹³⁹ More specifically, the REFIT Platform found that the e-Privacy Directive was no longer achieving its objective to fully protect individuals' right to privacy in light of the wide use of cookies and third-parties cookies for profiling purpose on the internet. The REFIT Platform thus recommended to enhance the effectiveness of individuals' protection against unsolicited marketing by amending the existing law and adding exceptions to the 'consent' rule for cookies.¹⁴⁰ Although the functioning of the REFIT programme can be criticised in some respects,¹⁴¹ it offers an interesting example of a goal-oriented assessment framework where factors of (in)effectiveness are analysed from an interdisciplinary perspective with the view of enhancing the benefits of the concerned laws.

1.2. BEYOND EFFECTIVENESS: DISCUSSION ON THE 'FUNCTIONALITY' OF THE LAW

At the very beginning of her doctoral research, the author of this study had formulated the hypothesis that personal data protection had become some sort of a 'super fundamental right' because of the growing number of cases where the CJEU was interpreting EU data protection law, read in light of Article 7 and 8 of the Charter, in a way that was restricting processing activities (usually to the detriment of controllers) and reinforcing the protection of personal data and privacy (usually to the benefit of data subjects). In parallel, the author of this study was observing in her own work that the GDPR was increasingly being used for defending a wide variety of rights and interests other than data protection and privacy (cf. the two examples mentioned in the Introduction, under point B, "Background of this study"). Based on these preliminary observations, the author of this study had come to wonder whether data protection had not become a 'super fundamental right', which could be characterised by a higher degree of effectiveness than other rights or freedoms. After researching on the topic however, the author came to realise that the notion of effectiveness alone was probably not sufficient to explain the 'handiness' of EU data protection law for protecting the rights or interests of data subjects in a variety of

¹³⁸ In order to better understand the effects of the e-Privacy Directive, the European Commission organised several public or ad hoc consultations, two surveys, two workshops, a round table as well as various meetings with relevant stakeholders. It also mandated several studies from different consultancy firms. For an overview, please refer to the Commission Staff Working Document SWD/2017/05 final - 2017/03 (COD) (Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, Accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC).

¹³⁹ Reproduced in Annex III of Commission Staff Working Document SWD/2017/05 final - 2017/03 (COD), pp. 92-96.

¹⁴⁰ Refit Scoreboard in the area of Communication Networks, Content and Technology. Evaluation: Finalised, 10.01.2017, SWD (2017) 5 final. Commission Proposal: Adopted, January 2017, COM (2017) 10 final 2017/0003 (COD).

¹⁴¹ Burnay, M. & Schmitt, p. (2018). Regulatory Fitness and Performance (REFIT) Programme: EU Regulatory Bottlenecks and Administrative Burdens at Local and Regional Level. Brussels: European Commission; Laulom, S. (2018). Better regulation and the social acquis: Is the REFIT fit for purpose? *European Labour Law Journal*, 9(1), pp.7–23; Sirakova, I. (2016). EU-Food Law after REFIT: Better Regulations or More of the Same. *European Food and Feed Law Review* 11.6 (2016): 531-33.

situations. Indeed, not all effective laws have the capability to achieve a wide variety of purposes or offer convenient tools for right holders to enforce their rights. Rather, only laws which are *designed* to fulfil (multiple) objectives and provide convenient legal venues to their right holders have the potential to become '(multi-)functional'. On this basis, the author further analysed the specificities of EU data protection law and started articulating the hypothesis that EU data protection law had been designed as a multifunctional framework for fundamental rights protection.

While the previous section of this study gave an overview of the notion of legal effectiveness as already theorised in the literature, this section will conceptualize the notion of legal functionality in a *sui generis* manner. The relation and meeting points of both notions will then be highlighted. This reflection will further serve as a steppingstone to articulate the hypothesis according to which EU data protection law would be a multi-functional framework for fundamental rights protection.

1.2.1. Conceptualising 'legal functionality': a *sui generis* definition

In its common sense, 'functionality' can be defined as "*the quality of being useful*" or "*practical*" with respect to "*the purpose for which something was made.*"¹⁴² Functionality can also be described as the quality of an object or a thing to be "*very suitable for the purpose it was designed for*".¹⁴³ When a thing is said to be functional, it usually means that it fulfils the function for which it was created in a convenient way. To some extent, functionality is thus often associated with the notion of convenience or practicality.¹⁴⁴

To determine whether a thing is more or less functional, three elements must usually be considered together: first, the actual function or purpose of the thing. Second, the extent to which the thing serves that function or purpose. And third, the handiness or practicality of the thing for its users. Keeping these elements in mind, it is apparent that both *effectiveness* and *functionality* can be appreciated on the basis of the ability of a thing to achieve the objectives for which it was built, designed or conceived. The term 'functionality' however put emphasis on an additional element: the users' experience. Not only must the intended objective be successfully achieved, but it must also be easy, practical or handy for its users. This is most likely the reason why the quality of being 'functional' is often attributed to tools or devices, i.e., instruments designed to achieve one or several purposes, whose fulfilment ultimately depends on the actions of external users. In other words, the more a tool is functional, the easier it is to use it.

¹⁴² Cambridge dictionary (online).

¹⁴³ Oxford Advanced Learners' dictionary (online).

¹⁴⁴ Ibid.

Although the functions of the law is a topic that has been explored by many philosophers and legal scholars,¹⁴⁵ the term ‘functionality’ is rarely used to describe legal norms.¹⁴⁶ Using the key-word ‘functionality’ in any academic database reveals that this term mainly belongs to the field of biotechnology, computer sciences or pharmacology.¹⁴⁷ Furthermore, after limiting those search results to the legal field, it appears that appreciating the quality of a law on the basis of its functionality is not a common thing. Therefore, before dwelling on the research question of this study, it seems essential to first clarify the meaning that the author wishes to attach to the notion of ‘legal functionality’.

As said above, functionality in its common sense is a quality that entails three elements: (i) the ability of a thing designed for one or more specific *purposes* (ii) to *serve* or *fulfil* those purposes (iii) in a way that is *handy* or *practical* for its *users*. Exploring the concept of functionality with respect to legal norms, it could therefore be argued that a law would only be functional when it offers practical or convenient tools for its addressees to mobilise that law, so that the objectives of that law can be achieved through them. The ‘addressees’ may include the persons whose behaviours or activities are regulated (the ‘duty bearers’), the persons who benefit from specific rights under that law (the ‘right holders’), and/or the authorities that are in charge of its control and enforcement (the ‘control and enforcement authorities’). Therefore, when assessing the functionality of a law, particular emphasis should be put on the *design* of the law (e.g., its scope, the control mechanisms put in place, etc.) as well as on the specific *tools* that this law offers and which facilitate its use by the *addressees* (e.g. a simplified complaint procedure; a reversed burden of proof for the benefit of right holders; etc).

As an example, one may refer to a national law aiming at closing the gender pay gap. Such a law could be described as being particularly ‘functional’ if the rights holders (i.e., mainly, female employees), the duty bearers (i.e., the employers) and the

¹⁴⁵ Jones, H. W. (1963). *The Creative Power and Function of Law in Historical Perspective*. *Vanderbilt Law Review*, 17:135-139; Raz, J. (1979). *The Authority of Law: Essays on Law and Morality*. Oxford: Oxford University Press; Chemillier-Gendreau, M. (1995). *Humanité et souverainetés: Essai sur la fonction du droit international*. Paris: La Découverte. Allott, P. (1998). *The True Function of Law in the International Community*. *Indiana Journal of Global Legal Studies*, 5:391-395; Crepeau, P.-A. (1998). La fonction du droit des obligations. *McGill Law Journal*, 43(4):729; Sunstein, C. R. (2019). *On the Expressive Function of Law*. *University of Pennsylvania Law Review*, 144:2021; Burchardt, D. (2019). The Functions of Law and their Challenges: The Differentiated Functionality of International Law. *German Law Journal*, 20:409-429; Gerkrath, J. (2009). Signification et fonctions d'une constitution. *Forum, Zeitschrift für Politik, Gesellschaft und Kultur in Luxemburg*, 286:23-26.

¹⁴⁶ The term functionality is however sometimes used by scholars to qualify the *low* functionality of law enforcement system and/or of the judiciary. See, for example, Školkay, A. (2016). Can a ‘Lone wolf’ quasi-investigative journalist substitute the low functionality of the law enforcement system? *Central European Journal of Communication*, 9:197-212; Suominen, A. (2014). Effectiveness and Functionality of Substantive EU Criminal Law. *New Journal of European Criminal Law*, 5(3): 388-415.

¹⁴⁷ On 1 July 2020, the author has entered the keyword ‘functionality’ in the search engine of the Luxembourg academic database ‘a-z.lu’ and has analysed the first 100 results. The first 20 results show academic publications in the field of biotechnology (7 out of 20), ICT (6 out of 20), health/pharmacology (3 out of 20), social sciences (3 out of 20), and environmental studies (1 out of 20). Out of the 100 first results, only 1 publication was in the field of law. However, the term functionality was not used to characterize legal norms.

competent public authorities (i.e., such as MEGA¹⁴⁸ in Luxembourg) are able to practically mobilise that law in order to limit discriminatory practices within the private or public sector and promote gender equality across the board in employment matters. By contrast, the same law could be described as dysfunctional where its content or design is so poor that it does not offer any convenient and effective tools for the persons concerned to detect and put an end to discriminatory practices (for example, if the law only applies to the public sector while most discrimination appear to take place in the private sector, or if the law does not contain any transparency obligation on the part of the employers with respect to salaries paid to men and women, thereby preventing the concerned actors to detect any discriminatory practices in this respect).

In accordance with this idea of functionality, the law is thus not perceived as an autonomous entity but rather as an instrument which can be used by external actors to achieve specific purposes, and which – depending on its content and the overall context in which it applies – can prove to be more or less functional for those actors.

1.2.2. The factors of legal functionality: focus on the design and the tools of the law

It has already been highlighted in the previous section of this study that assessing the effectiveness of a law can be a particularly challenging exercise due to the various factors that may influence such effectiveness. Logically, the same is true with respect to legal functionality, potentially even to a greater extent. Beyond assessing whether a law fulfils its objectives, additional focus must indeed be put on the *practicality* of the design and of the tools that the law offers to its addressees. Many factors may thus influence the level of functionality of a law. Contrary to legal effectiveness however, it is argued that legal functionality mainly derives from *internal* factors, in the sense that it mostly depends on the *content* of the law itself, rather than on external circumstances. This is because the notion of legal functionality as defined in this study is intrinsically attached to the *design* and actual *content* of the law – i.e., the way that it was conceived and the tools it offers. As a consequence, factors of functionality would mainly derive from provisions within a law that facilitate the use, application, compliance or enforcement of that law by its addressees.

In order to identify the internal factors of functionality of a given law, one should thus identify the purposes and categories of addressees of that law, as a first step, and then look which provisions appear to facilitate the application of that law for each category of addressees, as a second step. All in all, when assessing the functionality of a given law, one must thus look into how practical it is for right

¹⁴⁸ MEGA is the Luxembourg Ministry for equality between men and women (*Ministère de l'égalité entre les femmes et les hommes*). It has been established by the *Arrêté grand-ducal du 5 décembre 2018 portant constitution des ministères*.

holders to exercise their rights, for duty bearers to respect their obligations, or for the competent authorities to enforce the applicable rules under that law. The more practical and convenient the law appears to be for each category of actors, the more functional that law would be. As far as the GDPR is concerned, factors of functionality could, for example, include (i) the possibility for data subjects to bring proceedings before the Member State courts where they have their habitual residence (even if the controller is established somewhere else),¹⁴⁹ (ii) the possibility for duty bearers to consult the authorities on a compliance question and enter into a dialogue with them (to the extent the concerned DPA responds in a timely and collaborative manner),¹⁵⁰ or (iii) the large investigative and corrective powers of DPAs, which have the possibility to conduct dawn-raids and or to ban a given data processing practice.¹⁵¹

1.2.3. Functionality as a sub-category of legal effectiveness

From the outset, it must of course be acknowledged that legal functionality and effectiveness are inter-related notions. This is because they are both concerned with the end-result of a law. Some factors may thus contribute to both the effectiveness and functionality of a law. The clarity and readability of a norm, for example, is a prerequisite for the effectiveness and functionality of that norm. Norms that are too complicated or unclear are indeed more likely to be relinquished by their addressees, precisely because they are too ambiguous to be applied or even understood. However, while legal effectiveness is exclusively concerned with the *end-result* of a law (i.e., *is the objective of the law successfully achieved?*), legal functionality is concerned with both the *end* and the *means* available to the addressees of a law (i.e., *is the law practical enough for its addressees to fulfil its function?*).

Keeping this in mind, it can be inferred that functionality supports effectiveness, and vice-versa. If a law is highly functional, individuals will probably mobilise it more, which should in turn increase the application of or compliance with the law. Hence, factors that enhance the functionality of a law will proportionally contribute to its effectiveness. In the same vein, the more a law is effective (for example, because the rules are very clear and it provides for deterrent sanctions in the event of an infringement), the more likely its addressees will be tempted to rely on it; the legal, social and enforcement 'know-how' that will ensue from the regular interpretation and application of that law (including society's awareness of certain rights, the

¹⁴⁹ Article 79(1) of the GDPR.

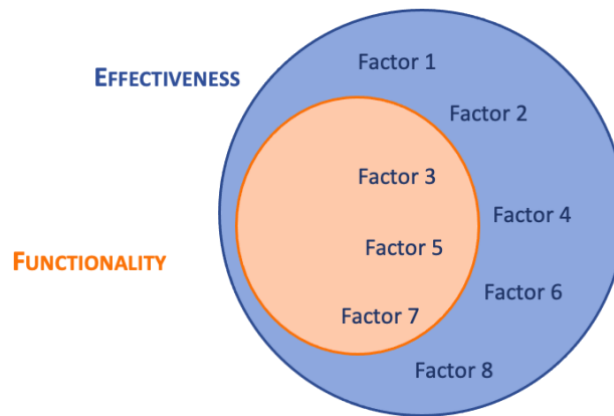
¹⁵⁰ See, in particular, Article 36 of the GDPR on prior consultation with respect to the necessity to conduct a data protection impact assessment. The author of this study acknowledges however that few controllers make use of this possibility, since some DPAs appear reluctant to adopt the role of 'advisors' but remain instead confined to their role as enforcers. This may deter controllers from willingly sharing potentially sensitive information on envisaged data processing practices with DPAs by fear to face a categoric negative opinion on the matter, or to attract their attention on a potential breach of the GDPR.

¹⁵¹ Article 58(1)(b), (e) and (f) of the GDPR.

consolidation of a consistent and rich case-law, etc.) may further facilitate its use by other actors, thereby increasing its overall functionality.

Yet, legal effectiveness and functionality should not be considered as interchangeable notions. Some laws can indeed be effective while lacking functionality. This is the case, in particular, when the objectives of a law are successfully achieved *despite* the fact that the law offers no easy or practical means for the persons concerned to use or mobilise that law. The effectiveness of such laws would then mainly derive from external factors that contribute to legal effectiveness but not to legal functionality. A profound social change, for example, can be a factor boosting voluntarily compliance with the law, thereby making it more effective, despite the fact that many procedural hurdles persist when it comes to its enforcement.¹⁵² By contrast, it is difficult to imagine a law that would be functional but ineffective. This is because, from a conceptual point of view, the notion of legal functionality *encompasses* the fulfilment of a law's objective. In other words, while not all effective laws are functional, all functional laws are necessarily effective. Because the more a law is functional, the more its level of effectiveness will increase, one may be tempted to infer that functionality is a *factor* of effectiveness. However, according to the definition proposed above, legal functionality should not be considered as a factor of effectiveness in itself, but rather as a theoretical framework under which multiple specific factors may be regrouped, and in particular factors relating to the practical design or tools of a given law. As a consequence, functionality can be considered as regrouping a specific sub-category of factors *within* the broader notion of legal effectiveness. The below model illustrates the interconnected nature of effectiveness and functionality in a visual way.

¹⁵² At the time the author is writing those lines, the Black Lives Matter (BLM) movement is raging in the US, following the killing of George Floyd in Minneapolis (Minnesota, US), and the killing of Rayshard Brooks in Atlanta (Georgia, US). The social protests and demonstrations that have followed those two tragic events have sent a shock wave across the globe. Demonstrators and sympathisers are calling for police reform and more effective legislation to address racial inequality. An important aspect of the issue in the US is *qualified immunity*; under this doctrine, policemen are immune from any lawsuit when acting in the course of their duty unless they violated one or several "*clearly established statutory or constitutional rights of which a reasonable person would have known*" (Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982)). In practice, qualified immunity makes it extremely difficult for plaintiffs to sue a policeman (for a complete analysis, see Reuters report by Chung, A., Hurley, L., Botts, J., Januta, A., and Gomez, G., (2020, June 12). Special Report: For cops who kill, special Supreme Court protection, <https://www.reuters.com/investigates/special-report/usa-police-immunity-scotus/>). The demonstrations taking place in the US and around the world against police brutality have urged the competent police departments to adopt sanctions against the policemen involved in those killings and conduct thorough investigations whenever a claim is filed on the basis of police brutality. Ultimately, social protests and social changes may thus help increase the *effectiveness* of legal norms whose aim is to prevent or punish police brutality. Those external factors may however not lead to any increase with respect to *functionality* if the doctrine of qualified immunity is not revised. This shows that effectiveness and functionality are not interchangeable notions, and that the first may grow without the second.



1.3. THE GDPR AS A MULTI-FUNCTIONAL FRAMEWORK FOR THE DEFENCE OF FUNDAMENTAL RIGHTS

As already spelled out above, the overarching research question of this study can be summarised as follows:

How multi-functional is EU data protection law, and the GDPR in particular, for protecting data subjects' fundamental rights and freedoms, beyond data protection and privacy, against various novel and potentially harmful data processing practices?

Now that the notion of functionality has been explained, the hypothesis under scrutiny may appear more clearly. Before attempting to answer this question however, it is necessary to first clarify the notion of 'multi-functionality', as well as delimiting the assessment framework within which the author will test this hypothesis.

1.3.1. A theoretical multi-functionality arising from the ambitious fundamental rights objective of EU data protection law

Generally speaking, 'multi-functional' is an adjective used to describe the capacity to perform "*more than one function*"¹⁵³ or to perform "*many functions*".¹⁵⁴ Multi-functionality is thus a characteristic attached to a tool which has "*several different uses*".¹⁵⁵ A multifunctional space, for example, could be a space that is used as a bedroom at night, as an office during the day and as a relaxation room during the evening. On this basis, *legal* multi-functionality could be understood as the quality or suitability of a law to effectively achieve *multiple* objectives in a manner that is practical or convenient for its addressees.

¹⁵³ Merriam-Webster dictionary (online).

¹⁵⁴ Collins dictionary (online).

¹⁵⁵ Cambridge dictionary (online).

Quite logically, the broader the objectives of a law are, the more challenging it is to ensure their achievement.¹⁵⁶ Adopting ambitious legal objectives without the appropriate tools will automatically lead to a dysfunctional or ineffective law. This is probably the reason why EU laws – especially EU directives or regulations – are usually designed to regulate one determined behaviour and/or to protect a certain right (sometimes even only in a specific field or sector). This seems especially the case when the aim of a directive or a regulation is to protect a fundamental right. As an illustration, non-discrimination is a fundamental right that was given expression in several EU directives. Among those directives, one may cite, for example, Directive 2006/54/EC, whose aim is to guarantee equal treatment for men and women in matters of employment and occupation. Similarly, Directive 2000/43/EC prohibits discrimination on grounds of race and ethnic origin in the field of employment, vocational guidance, social protection, education or access to goods and services. Both directives are therefore concerned with the principle of non-discrimination, which is enshrined in Article 21 of the Charter. In the same vein, Regulation (EU) 2019/125¹⁵⁷ gives expression to the prohibition of torture and inhuman or degrading treatment by prohibiting the trade of goods which could be used for capital punishment or torture. This Regulation thus tackles a very specific issue (i.e., the production of instruments of torture or lethal means used for the death penalty) with a view of protecting *one* fundamental right in particular (i.e., the prohibition of torture and inhuman or degrading treatment, enshrined in Article 4 of the Charter).

Taking this pattern into account, one could have expected the objective of EU data protection law to be exclusively centred around the protection of the fundamental right to privacy and personal data protection. If one looks at the letter of the law, however, EU data protection law appears far more ambitious. Since the adoption of the 1995 Data Protection Directive, two objectives can be distinguished in particular:

- 1) on the one side, EU data protection law aims at ensuring the free flows of personal data among EU Member States and beyond (the ‘Internal Market Objective’ or ‘**IMO**’); and
- 2) on the other side, EU data protection law aims at ensuring the protection of the fundamental rights and freedoms of natural persons in the context of the processing of their personal data (the ‘Fundamental Right Objective’, or ‘**FRO**’).

¹⁵⁶ As an illustration, an EU Regulation that would have as primary objective the creation of a database to monitor the level of heavy metals pollution in rivers across the EU would have more chance to succeed in this objective than a Regulation that would aim at eradicating water pollution in the EU within 12 months of its application.

¹⁵⁷ Regulation (EU) 2019/125 of the European Parliament and of the Council of 16 January 2019 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment, OJ L 30, 31.1.2019, p. 1–57.

With respect to this second objective, the 1995 Data Protection Directive explicitly states in its very first Article that “*Member States shall protect **the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data***” (emphasis added).¹⁵⁸ Although that Article expressly mentions the right to privacy (as already enshrined, at the time, in Article 8 of the ECHR), the general objective of the Directive was thus to ensure the respect of *all* fundamental rights and freedoms of natural persons in the context of personal data processing. With the adoption of the GDPR, the wording of this FRO was slightly amended to reflect the recognition and inclusion of the fundamental right to personal data protection in the Charter in 2000. Hence, Article 1 GDPR provides: “*This Regulation protects **fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data***” (emphasis added).¹⁵⁹ Today, the emphasis is thus put on the right to personal data protection itself rather than the right to privacy. This shift will be further explained in the second Chapter of this study. What is important to already note at this stage however is that, in both cases, the explicit objective of EU data protection law, besides ensuring the free flows of personal data, has always been to ensure the respect of the fundamental rights and freedoms of natural persons in the context of the processing of their personal data.

From the outset, one may be struck by the ambitious scope of this FRO, especially if one adopts a literal approach, as it would mean that EU data protection law is meant to protect all the fundamental rights and freedoms of data subjects, from human dignity,¹⁶⁰ to privacy,¹⁶¹ to environmental protection,¹⁶² or freedom of movement and residence.¹⁶³ In practice, however, only situations which fall within the material scope of EU data protection law could trigger its application and allow for the fulfilment of this broad FRO. In other words, the interference with a fundamental right must necessarily involve the processing of personal data for EU data protection law to become applicable in the first place, which limits *de facto* the situations in which a fundamental right or freedom would benefit from such an application. Also, at the time of the drafting of the GDPR, the EU legislator had probably not fully anticipated the extent to which such regulation would later apply or be mobilised for rights and freedoms *other* than privacy or data protection.¹⁶⁴ As discussed in the introductory part of this study indeed, the risks pertaining to data processing have risen exponentially over the years along with technological and societal developments. As individuals share more and more personal data, and as public or

¹⁵⁸ Article 1(1) of the 1995 Data Protection Directive, entitled (“Object of the Directive”).

¹⁵⁹ Article 1(2) of the GDPR.

¹⁶⁰ Article 1 of the Charter.

¹⁶¹ Article 7 of the Charter.

¹⁶² Article 37 of the Charter.

¹⁶³ Article 45 of the Charter.

¹⁶⁴ Recital 75 of the GDPR, for example, specifically refers to the need to protect the right to privacy, data protection and non-discrimination in the context of personal data processing, but does not mention other rights which could be similarly affected, such as freedom of expression, the presumption of innocence, consumer protection, etc.

private parties find more and more ways to use them, there has been an increase and diversification of both the positive and detrimental effects that data processing practices can have on individuals and society in general. This increase and diversification of risks have become more and more apparent in recent years through various scandals widely covered in the media. The 2019 *Cambridge Analytica* scandal already mentioned above, for example, clearly shed light on the fact that the unlawful processing of personal data could impact not only the right to privacy and data protection of the individuals concerned, but could also dangerously interfere with freedom of information, the right to vote and the democratic process as a whole.

Keeping this in mind, the decision of the EU legislator to inscribe the protection of data subjects' fundamental rights and freedoms as one of the main objectives of EU data protection law appears both relevant and desirable, even if the modern scope of that objective had probably not been fully envisaged at the time of the drafting of the 1995 Data Protection Directive. A distinction could therefore be made between the primary functionality of EU data protection law with respect to its FRO (i.e., mainly, the protection of the right to privacy and data protection of individuals, as primarily envisaged) and the secondary functionality of EU data protection law (i.e., the protection of other rights, freedoms and interests of data subjects, whose relevance grew over the last two decades). This distinction between the primary and secondary functionality of EU data protection law will be further discussed in the following Chapter of this study, by highlighting the origin, development and fulfilment of the FRO of (EU) data protection law from the 60s to the present time.

1.3.2. Testing the multi-functionality of EU data protection law in practice: a limited assessment framework

As already discussed above, a wide range of factors can contribute to or, to the contrary, hinder the effectiveness or functionality of a given law. The same is true with respect to the *multi*-functionality of a law. If the assessment framework is too broad or unspecific, it might become unsuitable to draw valid conclusions. By contrast, if the assessment framework is too restrictive or inadequate, it could lead to partial or misleading conclusions.¹⁶⁵ Due to the immense variety of potentially relevant factors as well as the relativity of their impact, assessing the multi-functionality of EU data protection law can thus be a challenging exercise. This is why setting a clear assessment framework is essential.

In this study, the author has decided to focus on assessing the multi-functionality of EU data protection law with respect to one of its objectives in particular: its fundamental right objective. The assessment framework of this study will thus be limited to the FRO of EU data protection law and will only incidentally touch upon its

¹⁶⁵ Rangeon F. (1989), *op. cit.*, p. 137.

internal market objective. The author is however fully aware that the functionality of EU data protection law vis-à-vis its FRO may be affected by the existence of this parallel IMO. Both objectives co-exist and sometimes conflict with one another. The *Schrems* saga is an example of this inevitable tension between the need to protect the fundamental rights of data subjects on the one side,¹⁶⁶ and the willingness to facilitate data flows for economic or innovation purposes (and in particular, as far as the *Schrems* saga is concerned, exchanges of information between data exporters located in the EU and data importers located in the US). While remaining aware of this tension and its consequences, the author has consciously decided to limit her analyses to the functionality of EU data protection with respect to its FRO – i.e., whether the data protection toolbox is really practical enough for data subjects, data protection authorities and other stakeholders who seek to ensure the respect of fundamental rights in the digital age.

For the sake of relevance and conciseness, the multi-functionality of EU data protection law with respect to its FRO cannot be tested in relation to each fundamental right or freedom enshrined in the Charter. Rather, this study will focus on rights and freedoms which have proven to be particularly vulnerable to novel and potentially harmful data processing practices in the digital age. As shown in the second Chapter of this study, the right to privacy (Article 7 of the Charter) and the right to personal data protection (Article 8 of the Charter) are incontestably relevant in this respect, since the CJEU has almost systematically interpreted and applied EU secondary law in the field of data protection both *in light* and *to the benefit* of these two rights. One can therefore argue that the primary functionality of EU data protection law has already been proven. In recent years however, other important rights and principles have started to suffer from troubling interferences in the context of personal data processing. In order to test the secondary functionality of EU data protection law for these other rights, the author will rely on two different ‘test areas’. Taking into account the development of new DDTs, the legal challenges posed by certain data processing practices, as well as their impact on different fundamental rights, the author has decided to focus on the following test areas in particular: (1) the rise of online harassment, and its impact on human dignity, integrity and freedom of expression (Articles 1, 3 and 11 of the Charter, respectively), and (2) recourse to ADM by the public or private sector in the field of recruitment, and the impact of such practice on non-discrimination (Article 21 of the Charter). Within this assessment framework, the author will attempt to formulate opinions and recommendations on how to improve the multi-functionality of EU data protection law for the benefit of various fundamental rights which have proven to be vulnerable to modern data processing practices.

¹⁶⁶ And particular, how the transfer of personal data by Facebook Ireland to Facebook Inc (in the US) is affecting the right to privacy (Article 7 of the Charter), the right to personal data protection (Article 8 of the Charter) and the right to effective judicial protection (Article 47 of the Charter) of the concerned data subjects, taking into account the surveillance practices of US intelligence agencies such as the CIA.

While EU data protection as a whole includes various directives and regulations, the author has willingly decided to focus on one piece of legislation in particular: the GDPR. As discussed above indeed, the GDPR is the main EU instrument in the field of data protection. As a result, assessing the multi-functionality of the GDPR with respect to its FRO may help drawing conclusions on the multi-functionality of EU data protection law as a whole. For the sake of relevance and conciseness, the assessment framework of this study will thus be limited to the GDPR, and only touch upon other instruments of EU data protection law when deemed relevant.

Finally, the assessment framework will be limited with respect to the personal scope of the FRO of the GDPR. In particular, the multi-functionality of EU data protection law will be appreciated with respect to its handiness in protecting the fundamental rights of the *data subjects* only – and not of third-party individuals. The author of this study is aware however that EU data protection law can sometimes be applied in a way that restricts the freedoms and rights of third parties, including persons processing personal data or persons indirectly benefitting from such processing. As an illustration, one may refer to the *Lindqvist* case,¹⁶⁷ which opposed Mrs Lindqvist (in her capacity as a controller) to her colleagues (in their capacity as data subjects). Mrs Lindqvist had published information about her colleagues on a publicly accessible blog without their permission. In particular, she had described, in a mildly humorous manner, the jobs held by her colleagues, their hobbies as well as other more sensitive personal matters relating to their family or health.¹⁶⁸ When the case escalated and ended up before the Swedish courts, Mrs Lindqvist argued that EU data protection law ought to be interpreted in a manner which was compatible with her freedom of expression. The prosecutor, on the other side, stressed the importance to interpret EU data protection law in a manner which protected the right to privacy of the data subjects concerned, i.e., the colleagues of Mrs Lindqvist. In the end, the CJEU interpreted EU data protection law in a manner that was favourable to the data subjects' rights to privacy, and therefore agreed that Mrs Lindqvist's freedom of expression would be partly restricted. The purpose of this study however is not to analyse the potential conflicts which may arise among the conflicting fundamental rights of data subjects and controllers or third parties, or to provide guidance on how to establish a fair balance between those conflicting rights. Rather, the purpose of this study is to test how handy EU data protection law can be for ensuring the respect of the fundamental rights of the *data subjects*. As a consequence, this study will not look into the possibility to rely on EU data protection law for the defence of third parties' fundamental rights.

As announced under point G, "Structure", the second Chapter of this study will look into the origin and development of the FRO of data protection law at the national and EU level, and highlight, each step of the way, the progressive reinforcement of the multi-functionality of EU data protection law for fundamental rights protection.

¹⁶⁷ CJEU, Judgment of 6 November 2003, *Lindqvist*, Case C-101/01.

¹⁶⁸ *Ibid.*, pt. 13.

The purpose is to understand *when* and *how* EU data protection law became a framework at the service of privacy, data protection, as well as other fundamental rights and freedoms of the data subjects. For this purpose, a brief historical analysis will be presented on the development of (EU) data protection law from the 60s to the present days. In parallel, the author will attempt to assess the degree of fulfilment of the FRO of EU data protection law through a case-law analysis at the level of the CJEU. The purpose of such analysis is to highlight to *what extent* EU data protection has already been successfully used for the defence of the right to privacy and data protection (primary functionality), or for the defence of other rights and freedoms (secondary functionality).

CHAPTER 2 – ORIGIN, DEVELOPMENT AND FULFILMENT OF THE FUNDAMENTAL RIGHTS OBJECTIVE OF EU DATA PROTECTION LAW

Foreword

In this Chapter, the author will analyse the origin, development and degree of fulfilment of the FRO of EU data protection law. Keeping the research question of this study in mind, particular attention will be paid to whether EU data protection law has been interpreted and applied for the benefit of fundamental rights.

With this objective in mind, this Chapter will first explore the emergence, in Europe, of legislative instruments regulating the collection and digitalization of personal data. Through this historical analysis, it will be shown in particular how data protection law has been conceived, since its genesis, as a tool to protect the fundamental rights of the data subjects, and in particular their right to respect for private and family life (in short, the 'right to privacy'), as enshrined in Article 8 of the ECHR and later on in Article 7 of the Charter.

Secondly, this chapter will explore the evolution, over the years, of the Fundamental Rights Objective of EU data protection law along with technological, legislative and jurisprudential developments in that field. Within this analysis, particular attention will be paid to the inclusion of a self-standing fundamental right to *personal data protection* in Article 8 of the Charter, and to the impact to such an inclusion had on the FRO of EU data protection law in general.

Thirdly, and most importantly, the degree of fulfilment of the FRO of EU data protection law will be discussed. For this purpose, the author will analyse the case-law of the CJEU in the field of EU data protection law, since the adoption of the 1995 Data Protection Directive until today, with a view of assessing how often EU data protection law has been mobilized for the defence of the right to privacy, of personal data protection and/or any other fundamental right or freedom of the data subject.

At the end of this Chapter, it will be concluded that, while the *literal* and *explicit* objective of EU data protection law has always been to protect the fundamental rights of natural persons, and of data subjects in particular, these rules have so far mainly been interpreted and applied for the benefit of only two (closely related) fundamental rights: the right to privacy, on the one side, and the right to the protection of personal data, on the other side. This will lead the author to question whether the functionality of EU data protection would not suffer from a shortfall, in the sense that it would constitute a *bi-functional* framework rather than a *multi-functional* framework with respect to its FRO. In order to outline further avenues for

reflections, the author will then spell out the potential causes behind such a phenomenon.

2.1. BACK TO THE ORIGIN OF EU DATA PROTECTION LAW: A FRAMEWORK AT THE SERVICE OF PRIVACY

The below historical analysis will show that the first laws that were adopted in Europe in the field of data protection were primarily conceived as a tool to protect the privacy of citizens against state surveillance. Given the importance that the right to privacy has played and continues to play in the interpretation and application of EU data protection law, it seems important to first introduce briefly that right.

2.1.1. A brief overview of the career of the right to privacy from the Hippocratic Oath to the Charter of Fundamental Rights

“I never said, 'I want to be alone.' I only said 'I want to be let alone!' There is all the difference.” – Greta Garbo, 1955, LIFE Magazine

2.1.1.1. The emergence of a right to privacy on the European continent

The origin of the right to privacy – or rather of its normative counterpart, i.e., the notion of private life – can be traced back to ancient Greece, and more specifically to the Hippocratic Oath (500-300 BC).¹⁶⁹ Young physicians taking this oath would indeed swear: *“And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets.”*¹⁷⁰ Through this oath, physicians were thus committing to keep confidential or secret the information entrusted to them by their patients. This translates an early recognition of the necessity to protect some sensitive information relating to individuals, and more specifically medical information about patients. Yet, ancient Greek societies did not recognise to individuals a general right to privacy. As a matter of facts, most aspects of individuals’ life at the time were falling under public scrutiny. In his famous *De Legibus*,¹⁷¹ Plato even expressed criticism about the idea of having a ‘private life’, which he considered as a threat to the good society.¹⁷²

¹⁶⁹ Miller, J. (2010). Locking Down Privacy. *Managed Healthcare Executive*, 20(3), p. 12; Edelstein, L. (1943). *The Hippocratic Oath: Text, Translation and Interpretation*. Baltimore: the Johns Hopkins Press, p. 56.

¹⁷⁰ Hippocrates of Cos (1923). The Oath. *Loeb Classical Library*, 147: 298–299. In the original text: “ἂ δ’ ἂν ἐνθεραπείῃ ἴδω ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπείης κατὰ βίον ἀνθρώπων, ἂ μὴ χρὴ ποτε ἐκλαλεῖσθαι ἕξω, σιγήσομαι, ἄρρητα ἠγεύμενος εἶναι τὰ τοιαῦτα.”

¹⁷¹ Plato, *De Legibus*, Pl. Leg. 738dn, available on the University of Chicago Perseus database (<http://perseus.uchicago.edu/>): “for where men conceal their ways one from another in darkness rather than light, there no man will ever rightly gain either his due honor or office, or the justice that is befitting. Wherefore every man in every State must above all things endeavor to show himself always true and sincere towards everyone, and no humbug, and also to allow himself to be imposed upon by no such person.”

¹⁷² Barrington Moore, Jr. (2018). *Privacy: Studies in Social and Cultural History*. Routledge.

Aristotle, the most famous of Plato's students, further considered that men were political animals by nature and that their public life was thus far more virtuous than their private life.¹⁷³ Therefore, even if the divide between private and public life can be traced back to Ancient Greece, the idea of granting individuals with a general right to privacy in relation to their intimate or family life was far from being praised in those times.

In contemporary law, the conceptualization of privacy as the right to withdraw from the public eye and to be able to think and act freely, outside of social constraints, from the comfort of one's own head or home, without being restrained, observed or judged by others, can be traced back to the end of the 19th century. In particular, privacy as the "*right to be let alone*"¹⁷⁴ can be attributed to two American scholars; Warren and Brandeis, who published an article titled 'The Right to Privacy' in the December issue of the 1890 Harvard Law Review.¹⁷⁵ In the introduction of that article, Warren and Brandeis refer to several technological developments, such as instantaneous photographs or the printing press, and subsequently highlight the need to grant individuals more protection with respect to their own image and private life.¹⁷⁶ As a second step, they explore how US law already protects individuals' privacy to some extent, by referring to legal protection against defamation (including, for example, the right not to be subject to attacks upon reputation), freedom of expression (including the right *not* to share one's opinions or thoughts), the inviolability of letters and diaries, copyright laws, property rights and the inviolability of the home (including the right to keep intellectual or material property out of the public eye). In the end, Warren & Brandeis conclude on the existence of a right to privacy "*as part of the more general right to the immunity of the person, - the right to one's personality*". One can therefore trace back the origin of a normative right to privacy to the 19th century, at a time where individuals needed to be shielded against the intrusive eyes of an emerging information

¹⁷³ Aristotle. *Politics, Book I*. Penguin Classics (1981). Translated from the Greek by T.A. Sinclair, revised and re-presented by Trevor J. Saunders.

¹⁷⁴ Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5):193-220. Warren & Brandeis actually cite Judge Colley, who is considered at the origin of this expression.

¹⁷⁵ *Ibid.*

¹⁷⁶ *Ibid.*, p. 195.

society.¹⁷⁷ Warren and Brandeis' novel conception of a right to privacy had however not yet gained any *express* recognition in the law, neither in the US nor in Europe.¹⁷⁸

2.1.1.2. Privacy as a human right in international EU treaties

It is only in the second half of the 20th century, that is, in the aftermath of World War II, that privacy was expressly recognized as a human right; first in the Universal Declaration on Human Rights in 1948, and then in the ECHR in 1950. This development has been qualified by legal scholars as "*highly remarkable and unusual*",¹⁷⁹ given the fact that no state in the world had yet recognised privacy as a constitutional or fundamental right at the time. Rather, state constitutions were protecting what could now be considered as facets of the right to privacy, such as the inviolability of the home or the confidentiality of correspondence.¹⁸⁰

The first international instrument to enshrine a general right to privacy was the Universal Declaration of Human Rights (UDHR), which was proclaimed by the United Nations General Assembly in Paris on 10 December 1948.¹⁸¹ The aim of Article 12 of the UDHR was to protect individuals against arbitrary interferences by the states with their right to privacy, including their family life, home, correspondence, honour and reputation.¹⁸² Article 12 of the UDHR therefore makes a distinction between *legitimate* and *arbitrary* interferences, the latter being incompatible with the right to privacy. This distinction indicates that the right to privacy has never been envisaged

¹⁷⁷ As put by Warren & Brandeis, "*the intensity and complexity of life, attendant upon advancing civilization, [had] rendered necessary some retreat from the world (...) so that solitude and privacy [had] become more essential to the individual.*" *Ibid.*, p. 196.

¹⁷⁸ It is only later that the expression 'right to privacy' will become so common that many authors will start looking back at the origin of this expression. See, among others: Carson, B. (2013). Legally Speaking - Warren, Brandeis, and the Creation of the Legal Concept of Privacy. *Against the Grain*, 20(2); Weichert, T. (2012). Anmerkungen zu Warren/Brandeis — Das Recht auf Privatheit. *Datenschutz Und Datensicherheit - DuD*, 36(10):753-754; Powell, C. D. (2011). 'You already have zero privacy. Get over it!' Would Warren and Brandeis argue for privacy for social networking? *Harvard Law Review*, 4:193; Nieves Saldaña, M. (2012). The right to privacy: La génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis. *Revista De Derecho Político*, 0(85):195-239; Bernabe, A. (2012). Giving credit where credit is due: A comment on the historical origin of the tort remedy for invasion of privacy. *The John Marshall Journal of Computer & Information Law*, 29(3):493-512. Kramer, I. R. (1990). The birth of privacy law: A century since Warren and Brandeis. *Catholic University Law Review*, 39(3):703-724.

¹⁷⁹ Diggelmann, O. & Cleis, M. (2014). How the Right to Privacy Became a Human Right. *Human Rights Law Review*, 14(3):442.

¹⁸⁰ *Ibid.*, pp. 441-458.

¹⁸¹ United Nations, *Universal Declaration of Human Rights*, proclaimed by the United Nations General Assembly on 10 December 1948. Source: <https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf>

¹⁸² Although Article 12 refers to all these notions separately, 'privacy' is usually understood today as an umbrella term encompassing the succeeding notions of family, home, correspondence, as well as honour and reputation, i.e., all the aspects to which the US scholars Warren and Brandeis had already referred to in their article published in December 1890 (see Warren, S. D. & Brandeis, L. D. (1890). *op. cit.*).

as an *absolute* right, in the sense that respect for individuals' privacy can be limited for legitimate reasons, for example, when necessary for public safety.¹⁸³

Two years later, in 1950, the Council of Europe decided to adopt its own binding human rights treaty – the ECHR, with a view of reinforcing the protection of essential human rights in Europe.¹⁸⁴ The right to privacy was also enshrined in Article 8 of the ECHR, under the more elaborated name of 'Right to respect for private and family life'. The reason why the drafters of the ECHR chose the name 'right to respect for private and family life' rather than 'right to privacy' also remains uncertain. No explanations were indeed provided by the drafters of the ECHR in that respect, "*as if such decisions were merely editorial details*".¹⁸⁵ Today, Article 8 of the ECHR is still spelled out as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

*2. There shall be no interference by a public authority with the exercise of this right **except** such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The term 'except' in the second paragraph of Article 8 of the ECHR confirms that the right to respect for private and family life is not absolute. In particular, interferences with this right are admissible if (i) they have a legal basis, and if (ii) they are considered necessary in a democratic society for the protection of the public interest or the fundamental rights and freedoms of others. Over the years, the ECtHR has extensively interpreted and given substance to Article 8 of the ECHR, while specifying the elements to be taken into account when assessing the validity of an interference with this right.¹⁸⁶ Within the substance of Article 8 ECHR, the ECtHR has notably recognised that "*the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life*".¹⁸⁷ According to the Court indeed, the right to respect for private and family life

¹⁸³ Determining the limits of the absolute core of privacy becomes however more and more challenging in today's information society. On the topic, see for example: Kleinig, J., Marnett, P., Miller, S., Salane, D., Schwartz, A., & Selgelid, M. (2011). *Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States*. ANU Press; Hildebrandt, M. (2013). Balance or Trade-off? Online Security Technologies and Fundamental Rights. *Philosophy & Technology*, 26(4):357–379.

¹⁸⁴ See Preamble of the ECHR. For a general introduction to the Council of Europe and ECHR, see Schmahl, S. & Breuer, M. (2017). *The Council of Europe: Its Laws and Policies*. Oxford: Oxford University Press.

¹⁸⁵ Diggelmann, O. & Cleis, M. (2014). *op. cit.*, p. 457.

¹⁸⁶ For a comprehensive summary of the case-law on Article 8 ECHR, see: ECtHR (2022, April 31). Guide on Article 8 of the European Convention on Human Rights (as last updated). https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

¹⁸⁷ ECtHR, Judgment of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, para. 133-134

encompasses the right to a form of informational self-determination, in the sense that individuals should be able to exercise a certain degree of control over their personal data. The somewhat complex relation between Article 8 ECHR and Article 7 and 8 of the Charter, and its potential impact on the functionality of EU data protection law, will further be discussed in section 2.2.3.3 and Chapter 5 of this study.

Sixteen years after the Council of Europe drafted and opened the ECHR for signature, the UN adopted the International Covenant on Civil and Political Rights (“ICCPR” - 1966) which, together with the UDHR and the International Covenant on Economic, Social and Cultural Rights (ICESCR), form the International Bills of Human Rights.¹⁸⁸ The ICCPR contains an Article 17 on the right to privacy that is almost identical to Article 12 of the UDHR.¹⁸⁹ Article 12 of the UDHR, Article 17 of the ICCPR, as well as Article 8 of the ECHR all deploy a similar general right to privacy, even if the historical events surrounding the consecration of that right tend to show that “*there was no conscious decision to create an integral guarantee – neither on the global nor on the European level.*”¹⁹⁰ Yet, the right to privacy was not enshrined in those three human rights treaties by mistake. Rather, its aim was clearly to protect individuals from the atrocities committed during WWII,¹⁹¹ and the subsequent pressure exercised by totalitarian governments over the life, freedom of thoughts and personality of individuals.¹⁹² As it is the case for most fundamental rights, the right to privacy was thus born out of necessity. Or, as explained by the philosopher Avishai Margalit, “[i]t is not justice that brings us into normative politics, but injustice. Not equality, but inequality; not happiness, but suffering; not dignity, but humiliation. (...) There is more urgency, if not importance, in fighting evil than in furthering good. Moreover, there is greater clarity and agreement in identifying evil than in recognizing and agreeing on the good. Thus urgency and epistemic priority are good reasons to adopt negative politics over positive politics. And so it is with privacy.”¹⁹³

Keeping those facts in mind, it can be argued that the introduction of the right to privacy in international human rights treaties in the 50s and 60s was both daring and foreseeable; daring, because no European state had explicitly recognised such a general right to privacy beforehand, yet foreseeable, because courts, scholars and legislators, both in the US and in Europe, had agreed on the necessity to better protect individuals’ private life in the face of state abuses and technological

¹⁸⁸ International Covenant on Civil Political Rights (1976). *The International "Bill of Human Rights": A brief history of the International Covenants on Human Rights (and optional protocol)*. New York: Service de l'information des Nation Unies.

¹⁸⁹ Article 17 of the ICCPR provides: “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.”

¹⁹⁰ Diggelmann, O. & Cleis, M. (2014), *op. cit.*, p. 457.

¹⁹¹ Diggelmann, O. & Cleis, M. (2014). *op. cit.*, p. 453.

¹⁹² Council of Europe (1975). *Collected Edition of the "Travaux préparatoires" of the European Convention on Human Rights, Vol. I*. The Hague: Martinus Nijhoff, p. 220.

¹⁹³ Margalit, A. (2001). Privacy in the Decent Society. *Social Research*, 68(1), p. 255.

developments.¹⁹⁴ It should therefore come as no surprise that, in the 70s, the novel risks that computerization was posing on the right to privacy provoked a new outcry. Indeed, as further discussed in the following sections of this study, the first national laws in Europe regulating the computerized processing of personal data were adopted with a view of protecting individuals' private and family life against illegitimate, abusive or intrusive practices by state authorities. Before tracing back the emergence of data protection law in Europe, however, a small historical detour will be made to touch upon the recognition of the right to privacy by the EU.

2.1.1.3. Privacy as a human right in European treaties

At the EU level, the protection of fundamental rights was originally not inscribed as an objective to be achieved by the institutions or its Member States. The 1951 Treaty establishing the European Coal and Steel Community¹⁹⁵ (the 'ECSC', the ancestor of the EU) makes indeed no reference to human rights or fundamental rights. Instead, the aim of the ECSC was to establish an "*economic community*" which would improve the economic relations and standards of living of the peoples living in that community.¹⁹⁶ The European continent was however not deprived from an organisation whose aim was to ensure respect for human rights, since the Council of Europe, which had been founded in 1949 already, had as main objective the "*maintenance and further realisation of human rights and fundamental freedoms*".¹⁹⁷ The reason why the EU did not initially get involved in the protection of human rights would thus at least be two-fold: first, because the role of the EU according to its founding Treaties was to foster economic integration among its members, "*a matter completely unrelated to that of fundamental rights*".¹⁹⁸ And second, because all the EU Member States had already adhered to the ECHR a few years earlier, which seemingly rendered the inscription of human rights protection among the founding Treaties unnecessary.¹⁹⁹

At the outset, the EU and the Council of Europe did not have overlapping agendas: the first was putting emphasis on the creation of an economic community, while the second was focusing on the protection of human rights, democracy and the rule of law. Progressively, however, the agenda of the EU evolved to ultimately include the protection of fundamental rights among its explicit objectives. In 1969, a first milestone was set by the European Court of Justice (for reason of consistency,

¹⁹⁴ Warren & Brandeis had cited, among other, instantaneous photos and the printing press, that enabled the limitless reproduction of one's portrait and the massive publication and distribution of details about one's private life. See Warren, S. D. & Brandeis, L. D. (1890), *op. cit.*, p. 195.

¹⁹⁵ Treaty establishing the European Coal and Steel Community, Paris, 18 April 1951.

¹⁹⁶ *Ibid.*, Preamble.

¹⁹⁷ Article 1 of the Treaty of London creating the Council of Europe, signed on 5 May 1949. The original signatories were Belgium, Denmark, France, Republic of Ireland, Italy, Luxembourg, Netherlands, Norway, Sweden and United Kingdom.

¹⁹⁸ Tizzano, A. (2008). The Role of the European Court of Justice in the Protection of Fundamental Rights. Arnall A., Eckhout P. and Tridimas T. (eds.). *Continuity and Change in EU Law: Essays in Honour of Francis Jacobs*. Oxford Academic.

¹⁹⁹ *Ibid.*

hereafter referred to as the 'CJEU'). In the *Stauder* case, the CJEU rendered a judgment in which it stated that the protection of fundamental rights formed an integral part of the general principles of Community law (for reason of consistency, hereafter referred to as EU law), and therefore ought to be respected and protected within the EU legal order.²⁰⁰ Although unwritten, these general principles apply transversally and generally govern the interpretation to be given to other sources of EU law.²⁰¹ While in *Stauder*, the CJEU had clarified that fundamental rights were implicitly enshrined in the general principles of EU law, it had yet to specify *which* fundamental rights it was referring to. The CJEU partly clarified the matter a year later in the *Internationale Handelsgesellschaft* case, by stating that the protection of fundamental rights at the EU level was “*inspired by the constitutional traditions common to the Member States*”.²⁰² In *Nold II* (1974), the CJEU further declared that, for the purpose of safeguarding fundamental rights, it was bound to “*draw inspiration from the constitutional traditions common to Member States*” and also added that it should take as guidelines “*international treaties for the protection of human rights, on which the Member States have collaborated or of which they are signatories*”.²⁰³ Among these international human rights treaties, the CJEU further recognised that “[t]he European Convention on Human Rights has special significance in that respect”.²⁰⁴

For a long time, the EU was therefore relying on two indirect sources of law to ensure the protection of fundamental rights, including the right to privacy: (1) the constitutional traditions common to the Member States and (2) the international human rights treaties by which the Member States had to abide, including the ECHR which according to the CJEU had “*special significance*”.²⁰⁵ Indirectly, the right to privacy as protected by the constitutional tradition of Member States and as enshrined in Article 8 of the ECHR therefore became part of the EU legal order. Pretending however that the EU had never envisaged to get directly involved in the ‘making’ of its own written catalogue of human rights would be erroneous.²⁰⁶ Discussions over the adoption by the EU of such a catalogue had indeed been

²⁰⁰ CJEU, Judgment of 12 November 1969, *Erich Stauder v City of Ulm – Sozialamt*, Case 29/69. In the 7th paragraph of the Grounds of Judgment, the CJEU states: “*the fundamental human rights [are] enshrined in the general principles of Community law and protected by the Court*”.

²⁰¹ Tridimas, T. (2000). *The general principles of EC Law*. Oxford EC Law Library; Gerkrath, J. (2007). Les principes généraux du droit ont-ils un avenir en tant qu'instrument de protection des droits fondamentaux dans l'Union européenne ? *Revue Des Affaires Européennes*, 2006(1):31-34. Bruxelles : Bruylant.

²⁰² CJEU, Judgment of the Court of 17 December 1970, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, Case 11/70, para. 4.

²⁰³ CJEU, Judgment of the Court of 14 May 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*, Case 4/73, para. 2.

²⁰⁴ CJEU, Judgement of the Court of 18 June 1991, *Elliniki Radiophonia Tileorassi AE v Pliroforissis and Kouvelas (ERT)*, Case C-260/89, para. 41.

²⁰⁵ *Ibid.*

²⁰⁶ de Búrca, G. (2010). The Road Not Taken: The EU as a Global Human Rights Actor. *American Journal of International Law*, 105(4):649-693.

ongoing since the end of the 80s,²⁰⁷ including within the European Parliament²⁰⁸ which eventually adopted in 1989 the Declaration of Fundamental Rights and Freedoms, which enshrined the right to privacy in its Article 6.²⁰⁹ This Declaration did not however have any significant impact within the EU legal order as it lacked any legally binding force.²¹⁰ Debates, discussions and initiatives in relation to the drafting of a (binding) EU human rights catalogue therefore continued throughout the 90s.²¹¹

On the 3d and 4th June 1999, the European Council²¹² met in Cologne.²¹³ During this meeting, following the previous recommendations from various expert groups, the European Council took the view that the fundamental rights applicable at EU level should be consolidated in a Charter.²¹⁴ This decision can be considered as a turning point for the protection of fundamental rights in the EU legal order. The body in charge of drafting such a Charter called itself the 'Convention' and was assisted by a Bureau called the 'Praesidium'.²¹⁵ Their mandate was to make existing EU fundamental rights more clear or evident by listing them in a Charter.²¹⁶ Given that privacy was already enshrined as a human right in the constitution of most Member States, as well as in the European Convention on Human Rights, it came as no surprise that such a right was included within the Charter since its very first draft.

²⁰⁷ Among all the discussions that took place among the EU institutions in the drafting of its own human rights catalogue, see in particular: Committee on Institutional Affairs of the European Parliament (1987, July 16). *Working Document containing the White Paper on the state of fundamental rights in the European Community*. General rapporteur: K. De Gucht. PE 115.274; European Parliament (1983, September 26). *Motion for a Resolution tabled by Mr Luster and Mr Pfennig jointly*, Doc. 1-653/83/rev.; European Parliament (1984, July 26). *Motion for a Resolution tabled by Mr Luster and Mr Pfennig to supplement the draft Treaty establishing the European Union*. Doc. 2-363/84; European Parliament (1989, March 20). *Report on the Declaration of fundamental rights and freedom* (General rapporteur: K. De Gucht)/ Doc. A2-0003/89.

²⁰⁸ *Ibid.*

²⁰⁹ Resolution of the European Parliament adopting the Declaration of Fundamental Rights and Freedoms [1989] OJ C 120/51.

²¹⁰ González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer, p. 187-188.

²¹¹ European Parliament (1005, February 10). Resolution of the European Parliament on the Constitution of the European Union (Herman report). A3-0064/94. OJ C61/155; Private Office of the General Secretariat of the Council of the European Union (1995, October 6). Note for the Reflection Group on the principles and rights included in the constitution of the Member States of the European Union. SN 512/95 (REFLEX 13).

²¹² The European Council is one of the main institutions of the EU; it is composed of the Heads of State or Government of the Member States (Article 15(2) TEU). They meet at least four times a year in order to define the general political directions and priorities of the EU (Article 15(1) and (3) TEU). The European Council may adopt decisions in order to formalize its position and political intentions for the EU. While these decisions are legally binding, they cannot be qualified as legislative acts. In fact, when acting alone, the European Council does not have any legislative function (Article 15(1) and (4) TEU).

²¹³ Cologne European Council of 3 and 4 June 1999. Conclusions of the Presidency. http://www.europarl.europa.eu/summits/kol1_en.htm. The European Council met in Cologne on these days consider major issues for the future following the entry into force of the Amsterdam Treaty.

²¹⁴ *Ibid.*

²¹⁵ The Praesidium had the role of lending impetus to the Convention and providing it with a basis on which to work. It consisted of the Convention Chairman and Vice-Chairmen and nine members drawn from the Convention: the representatives of all the governments holding the Presidency of the Union during the Convention (Spain, Denmark and Greece), two national parliament representatives, two European Parliament representatives and two Commission representatives. For more information, please see the website of the European Convention: <http://european-convention.europa.eu/EN/praesidium/praesidium2352.html?lang=EN>.

²¹⁶ European Council Decision on the Drawing Up of a Charter of Fundamental Rights of the European Union (Annex IV of the Conclusions of the Presidency. Cologne European Council, 3 and 4 June 1999. http://www.europarl.europa.eu/summits/kol1_en.htm).

Today, Article 7 of the Charter, entitled ‘Respect for private and family life’, reads as follows:

“Everyone has the right to respect for his or her private and family life, home and communications.”

Once compared to its equivalent under the ECHR, one may note that the word “correspondence” has been replaced by the word “communications”, as a way to include modern communication media, such as emails, voice messages or telephonic communications.²¹⁷ Also, it can be noted that the Article 7 of the Charter does not explicitly mention the possibility to limit the exercise of the right to privacy, although it has been confirmed by the Convention itself in the Explanations to the Charter that “in accordance with Article 52(3), the meaning and scope of this right are the same as those of the corresponding article of the ECHR. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR”.²¹⁸ The right to privacy is thus not absolute in the EU legal order but may be limited under certain conditions, as confirmed in the case law of the CJEU.²¹⁹ The way in which the ECtHR and the CJEU have interpreted and applied the scope and content of Article 7 of Charter, as well as its relation with the fundamental right to personal data protection inscribed in Article 8 of the Charter, will further be discussed in the following Chapters of this study. It suffices, for the moment, to be aware of the origin and early recognition of that right to privacy in the EU legal order, given its importance in relation to the emergence data protection laws in Europe.

2.1.2. Pioneering European laws regulating the processing of personal data

“In the future, computers may weigh no more than 1.5 tonnes.”
— *Popular mechanics, 1949*

Computers started being installed in commerce and governmental organisations in the 50s and 60s.²²⁰ At that time, these machines were big and costly. As a consequence, only large corporations, universities, or powerful governmental agencies could afford them. Through the 70s however, thanks to the development and normalisation of microprocessors, computers became smaller, more affordable and therefore more common.²²¹ It quickly became obvious that computers were offering many advantages because of their vastly superior storage and processing

²¹⁷ The Explanations to Article 8 of the Charter state in this respect: “To take account of developments in technology the word “correspondence” has been replaced by “communications”.” Source: Draft Charter of Fundamental Rights of the European Union and Explanations of 11 October 2000. CHARTE 4473/00, p. 10. https://www.europarl.europa.eu/charter/pdf/04473_en.pdf.

²¹⁸ *Ibid.*

²¹⁹ Including in the CJEU *Schrems I* and *Schrems II* judgments, discussed below in Section 2.3.2.4.

²²⁰ Campbell-Kelly, M. (2018). *Computer: A history of the information machine, economy edition*. Routledge (3 ed.), p. 143.

²²¹ Weatherford, M. (1996). A quarter century of microprocessors. *Computer*, 29(3):99.

capability, compared to human minds or manual filing. Public authorities and private companies therefore started acquiring computers and creating large databanks with the view of facilitating access to and storage of information on individuals, be it customers, employees, public officers or citizens.

In the mid-60s, the Federal State of Hesse in Germany started collecting and computerising the personal data of its citizens in the framework of a vast modernisation program.²²² Paper files were intended to be gradually turned into computer files, thereby reducing the space needed in archive rooms. This modernisation effort, however, raised concerns over privacy and security in the State of Hesse.²²³ The fact that the data collected included information relating to the health or income of citizens in particular fuelled fears that the State of Hesse could misuse this new technology. In this context, the Government of Hesse was asked to take action to prevent the risks of a permanent surveillance of citizens.²²⁴ On 7 October 1970, after brief parliamentary debates, the Federal State of Hesse became the first territory in the world to adopt a data protection act (the '1970 *Hessische Datenschutzgesetz*').²²⁵ This law had a very limited personal and territorial scope as it only concerned the processing of citizens' personal data by the authorities of the State of Hesse.²²⁶ Yet, it is still recognised today as a landmark piece of legislation given that it is the first law explicitly concerned with 'Datenschutz', i.e., 'data protection'.

Less than three years later, another European state followed the lead of and deepened the path traced by the State of Hesse by adopting a data protection act with a much more general scope. On 11 May 1973 indeed, Sweden adopted the '1973 *Datalag*' which applied to the filing of personal data in any machine-readable form, regardless of whether the files were held by public or private persons.²²⁷ The 1973 *Datalag* can thus be considered as the first nation-wide data protection law in Europe. According to Article 2 of this law, any person falling within the scope of that law needed to obtain a license from the Swedish data inspection board (the '*Datainspektionen*') before starting to process personal data. This system thus established a *de facto* general prohibition to process personal data on a machine, unless a prior permission was obtained from the *Datainspektionen*. Just like the *Hessische Datenschutzgesetz*, the 1973 Swedish *Datalag* was adopted as a result of public concern about computerisation, personal data and abuse of government

²²² Hessische Zentrale für Datenverarbeitung (1970). *Grosser Hessenplan: Entwicklungsprogramm für den Ausbau der Datenverarbeitung in Hessen*. Kassel: Meister.

²²³ Simitis, S. (2010). Privacy—An Endless Debate? *California Law Review*, 98(6):1995.

²²⁴ *Ibid.*

²²⁵ Hessisches Datenschutzgesetz [HDSG] [Hessian Data Protection Act], Hess GVBl. I625 (1970).

²²⁶ For its history, see Simitis, S. (1990). Zwanzig Jahre Datenschutz in Hessen - emekritische Bilanz, in 19 Tätigkeitsbericht Des Hessischen Datenschutzbeauftragten. *Hessischen Datenschutzbeauftragten*, 19:138-153.

²²⁷ *Datalag* (1973:289) <https://rkrattsbaser.gov.se/sfst?bet=1973:289> (Swedish data law of 5 May 1973, repealed on 10 October 1998, Article 1).

power related to mass surveillance.²²⁸ Beginning of the 70s indeed, computers were becoming increasingly small and affordable, revealing both opportunities and general concerns about their use, as illustrated in the below extract from the October 1970 issue of the *Scientific American*.

The page contains several columns of text discussing the impact of computers. The headline reads: **ARE THEY FOR US OR AGAINST US?** The RCA logo is prominently displayed on the right side of the page. The text includes:

In the minds of many, modern technology has created a monster.

The computer. We've all heard the stories about people making, say, a \$30 purchase. And then being billed for \$3,000 by the computer.

Nonsense. The danger is not that the computer makes mistakes, but that human errors remain uncorrected while the machine rolls on, compounding them.

Computers are literal-minded. They must be correctly instructed to help us in the solution of problems. They do exactly what they are told. Not what they ought to have been told.

The computer is man's assistant. Not his replacement. The unaided human mind needs help to cope successfully with the complexity of our society.

Intellectual aids, such as computers, will not only increase the skill of our minds, but leave more time for human creativity by freeing man of burdensome routine tasks.

Do we really believe that our achievements in space could have been accomplished without computer assistance?

Do we really believe that we can function efficiently in our complex modern environment without computer assistance?

The answer, of course, is obvious. In truth, the invention of the computer can be compared with the invention of the printing press.

Engineers engaged in the development of computer systems are convinced that over the next decade it is possible to develop networks of interconnected computer systems capable of offering a wide variety of services to the public.

By necessity, one-way mass communications—radio, television—deal with a common denominator of entertainment. This situation can be changed by developing computer-based systems that offer each individual an almost unlimited range of entertainment and information. Each individual will select what he wants, and to how great a depth he wants to delve into the areas in which he is interested.

At his choice of time. Apply this principle to education.

What it amounts to is individualized instruction. To meet simultaneously the needs of many students.

From a practical standpoint, limits to excellence in education are almost purely economic.

The computer provides a solution by performing high quality instruction for large numbers of students, economically.

Our goal is to make it possible for a teacher to provide individual guidance to many students, instead of few.

Yet, computer-assisted instruction is not a concept which has been enthusiastically embraced by all. There are many who feel that the computer will replace teachers.

Not so. This interpretation implies mechanizing, rather than personalizing, education.

Everywhere in our lives is the effect and promise of the computer.

Its ability to predict demand makes it possible to apply the economies of mass production to a wide variety of customized products.

It will allow for the use of a computer terminal device for greater efficiency in home shopping and much wider diversity in home entertainment.

It can be a safeguard against the boom and bust cycle of our economy.

In short, the computer means accuracy, efficiency, progress.

The computer affords us the way to store knowledge in a directly usable form—in a way that permits people to apply it without having to master it in detail.

And without the concomitant human delays.

The computer is indicative of our present-day technology—a technology which has advanced to such an extent that man now is capable, literally, of changing his world.

We must insure that this technological potential is applied for the benefit of all mankind.

If you're an engineer, scientist or systems programmer, and want to be part of RCA's vision of the future, we invite inquiries.

If you are interested in a comprehensive index of over 1100 technical papers published by RCA, scientists and engineers last year, let us know.

Write to Mr. A. C. Bennett, RCA, Bldg. 2-2, Camden, New Jersey 08102.

Of course, we're an equal opportunity employer.

RCA

© 1970 SCIENTIFIC AMERICAN, INC.

In January 1977, i.e., seven years after the adoption of the 1970 *Hessische Datenschutzgesetz*, Germany ultimately enacted a nation-wide data protection law under the name *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* (the '1977 BDSG').²²⁹ Germany thereby became the first member state of the EU to adopt a binding legislative act to protect individuals against misuse of their personal data.²³⁰ More specifically, the BDSG established a restrictive framework generally prohibiting the processing of personal data by private or public persons, unless such processing was explicitly authorised by German law or the individuals concerned had consented to it.²³¹ The media were however exempted from the scope of the 1077 BDSG when processing personal data for their own journalistic purposes.²³² It is also interesting to note that this law already recognised a set of specific rights to individuals in relation to the processing of their personal data,

²²⁸ In 1972, a report on personal data and integrity was published by a Swedish Parliamentary Commission, which both emphasised the benefits of computer technology in public administration and the lack of trust and confidence of citizens towards the State. For more information, see Gonzáles Fuster, G. (2014). *op. cit.*, pp. 58-59 and Söderlind A. (2009). *Personlig integritet som informationspolitik: Debatt och discussion I samskap/Bibliothekshögskolan. Högskolan I Borås och Göteborg universitete*, p. 272.

²²⁹ *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* (BGBl. I Nr. 7 S. 201) (German law on the misuse of personal data in the context of data processing of 27 January 1977).

²³⁰ In 1977, the European Community was composed of France, Germany, Belgium, Luxembourg, the Netherlands, Denmark, Ireland and the United Kingdom. Sweden only joined the EU in 1995.

²³¹ Gonzáles Fuster, G. (2014), *op. cit.*, p. 60.

²³² Section 1, §1(3) of the 1977 BDSG.

mainly the right to information, correction, blocking or deletion of their personal data (all subject to specific conditions).²³³ Section 6 of the 1977 BDSG further imposed the obligation on parties processing personal data to adopt adequate “*technical and organisational measures*”,²³⁴ some examples of which were listed in an Annex to the law. The BDSG also established a Federal Data Protection Commissioner for Germany²³⁵ in charge of supervising the application of the BDSG. The law further imposed on private persons having five employees or more the obligation to appoint a data protection officer internally.²³⁶ As shown in the following sections of this thesis, the principles, rights and obligations set out in the 1977 BDSG greatly influenced the drafting of ulterior data protection laws, both at the national and supra-national level.

In the 70s, not all countries approached the issues relating to personal data processing from a regulatory stance. Portugal, Austria and Spain, for example, first envisaged data protection as a constitutional right. The first European country to have enshrined a form of right to data protection in its Constitution was Portugal in 1976.²³⁷ Article 35 of the 1976 Portuguese Constitution, entitled ‘*Use of data processing*’, originally consisted of three paragraphs:²³⁸ the first paragraph granted to all citizens a right of information, access and correction of personal data held in data banks; the second paragraph established a general prohibition of the automated processing of sensitive personal data relating to political convictions, religious beliefs or private life; and the third paragraph proscribed the use of national identification number for the interconnection of data. The Portuguese Constitution can therefore be considered as a landmark text in the recognition of the fundamental value of the right to personal data protection, as it was the first constitution to enshrine that right independently from the right to the respect for private life. In 1978, Austria adopted its own data protection law, the *Bundesgesetz über den Schutz personenbezogener Daten* (the ‘1978 Austrian Data Protection Law’).²³⁹ The particularity of this law in comparison to any other data protection laws at the time was that it recognized the fundamental nature of the right to data protection by giving it constitutional force.²⁴⁰ Austria therefore adopted a hybrid approach whereby a national law of constitutional ranking was adopted, both recognizing the fundamental nature of the right to data protection while giving expression to it in specific legislative provisions. For the Austrian legislator, the initial notion of data protection was however intrinsically linked to the notion of private and family life.

²³³ Section 4 of the 1977 BDSG

²³⁴ In German, “*Technische und organisatorische Maßnahmen*”.

²³⁵ In German, “*Bundesbeauftragter für den Datenschutz*” (Section 17 of the 1977 BDSG).

²³⁶ In German, “*Beauftragter für den Datenschutz*” (Section 38 of the 1977 BDSG).

²³⁷ The Portuguese Constitution stands out in comparison to other constitutions due to its degree of details. In particular, human rights are carefully and extensively listed. Beffort, J. (1911, September 6). La constitution portugaise. *L'indépendance luxembourgeoise* (source: newspaper archives eluxemburgensia.lu).

²³⁸ González Fuster, G. (2014), *op. cit.*, p. 66.

²³⁹ *Bundesgesetz vom 18 Oktober 1978 über den Schutz personenbezogener Daten*, BGB1. Nr. 565/1978.

²⁴⁰ Article 1 of the 1978 Austrian Data Protection Law refers to a constitutional right to data protection (“*Grundrecht auf datenschutz*”). It contains multiple sections having constitutional ranking (“*Verfassungbestimmung*”).

Art. 1, §1 (1) of the 1978 Austrian Data Protection Law indeed provided: “Everyone is entitled to secrecy of personal data concerning him, insofar as he has a legitimate interest, especially with regard to **respect for his private and family life**” (emphasis added). Under Austrian law, data protection rights could thus only be activated to the extent that the data subjects had a legitimate interest to protect their private or family life. Also in 1978, the protection of personal data was also included as a fundamental right in the Constitution of the German State of North Rhine-Westphalia. This provision stated that everyone had the right to the protection of their personal data, and that limitations to this right were only allowed when provided by a law pursuing a substantial public interest.²⁴¹ Various other German states have since then also included a provision on the right to data protection in their own constitutional law.²⁴² Shortly after the German State of North Rhine-Westphalia, Spain also recognized a form of right to personal data protection. In particular, Article 18 of the 1978 Spanish Constitution instituted a limit to the use of computerized systems to protect citizens’ honour and their right to private and family life.²⁴³ The expression ‘data protection’ was not used as such; rather, Article 18 of the 1978 Spanish Constitution can be seen as an umbrella article enshrining different rights relating to the broader notion of privacy. Although such wording may be considered as ambiguous and does not amount as such to the recognition of an independent right to personal data protection,²⁴⁴ the 1978 Spanish Constitution did refer to a negative right regarding the processing of personal data in computerized systems, thereby explicitly acknowledging the risks that such computerization posed for the right to privacy.

In France, the *Loi relative à l’informatique, aux fichiers et aux libertés* was adopted on 6 January 1978 (the ‘1978 French Data Protection Law’).²⁴⁵ Like other data protection laws in Europe, the 1978 French Data Protection Law was adopted in response to computerization, and in particular the risk posed by the grouping of different databases detained by various public administrations.²⁴⁶ The main source of such concerns may be traced back to an article published on 21 March 1974 by a French Journalist, Philippe Boucher, in *Le Monde* (see reproduction below).²⁴⁷ This article brought to light the intention of the French authorities to link information about citizens which were held in various registers under a unique identifier. The

²⁴¹ Section 4, para. 2 of the Constitution of the Land of North Rhine-Westphalia.

²⁴² Gonzáles Fuster, G. (2014). *op. cit.*, p. 177.

²⁴³ Article 18 (fourth and last paragraph) of the Constitution passed by the Cortes Generales in plenary meetings of the congress of deputies and the senate held on October 31, 1978 ; ratified by referendum of the Spanish people on December 7, 1978; sanctioned by his majesty the king before the Cortes Generales on December 27, 1978, available at http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingl_es_0.pdf.

²⁴⁴ Gonzáles Fuster, G. (2014). *op. cit.*, p. 69.

²⁴⁵ *Loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés*, published in the *Journal Officiel de la République Française* on 7 January 1978, p. 227.

²⁴⁶ CNIL (2017). Comment Permettre à l’Homme de Garder la Main? Les enjeux éthiques des algorithmes et de l’intelligence artificielle. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf, p. 45.

²⁴⁷ Boucher, P. (1974, March 21). Safari ou la chasse au Français. *Le Monde*, p. 9.

project was called S.A.F.A.R.I., for *Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*. The journalist compared this project to a hunt of French citizens and urged the Parliament to initiate democratic debates in order to establish safeguards against the risk of misuse of such centralized registers.



Philippe Boucher's article caused great public alarm among the French population.²⁴⁸ Because of this national outcry, the project was ultimately abandoned, and the Ministry of Justice established a special commission in order to draw concrete recommendations on how to regulate the processing of large amount of data.²⁴⁹ The report of this commission directly inspired the legislative proposal submitted to the *Assemblée Nationale* in August 1976, which ultimately led to the adoption of the 1978 French Data Protection Law.

The 1978 French Data Protection Law was quite short: only 7 articles long. The first article generally stated that computers should "be at the service of every citizen" and that their use should not jeopardize "human identity, human rights, private life or individual or public freedoms".²⁵⁰ The 1978 French Data Protection Law therefore drew a clear link between regulating the processing of personal data on the one side, and protecting fundamental rights and freedoms on the other side, and in particular

²⁴⁸ Gonzáles Fuster, G. (2014), *op. cit.*, p. 62.
²⁴⁹ Created by the Decree 74-938 of 8 November 1974, this Commission was the Commission Nationale de l'Informatique et Libertés ("CNIL") by the law of 6 January 1978. See Hondius, F. W. (1975). *Emerging data protection in Europe*. Amsterdam : North Holland Publishing Company, p. 34.
²⁵⁰ In French : « Art. 1^{er}. — L'informatique doit être au service de chaque citoyen (...). Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

the right to respect for private and family life. Like Sweden and Germany, the 1978 French Data Protection Law also established a national data protection commission; the *Commission Nationale de l'Informatique et des Libertés* (or 'CNIL'),²⁵¹ in charge of informing data subjects about their rights and of monitoring the application of the law on the French territory. The name of this authority has remained unchanged for the last thirty-five years, although the scope of its competences and powers has been substantially broadened over time.

Denmark is the third member of the European Community (after Germany and France) to have adopted a national legislative framework regulating the processing of personal data. It did so in two separate legislative acts of 8 June 1978 distinguishing the public and private sector: the *Lov om private register*,²⁵² regulating data banks in the private sector, and the *Lov om offentlige myndigheders register*,²⁵³ regulating data banks held by public authorities. Similar legislation was passed in Norway in 1978 (the '1978 Personal Registers Act'),²⁵⁴ also in response to concerns about computerization.²⁵⁵

Finally, in 1979, closing a decade of legislative and constitutional developments in Europe in the field of data protection, Luxembourg adopted its *Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques* (the 1979 Luxembourg Law on the Processing of Nominal Data). The particularity of this law was that it protected both natural and *legal* persons against abusive uses of nominal data. Nominal data was defined as any information relating to an identified or identifiable person, whether natural or legal. The law applied to all databanks located or used on the Luxembourg territory, with some specific exceptions.²⁵⁶ Contrary to other data protection laws, the 1979 Luxembourg Law on the Processing of Nominal Data did not inscribe the protection of fundamental rights or freedoms among its explicit objectives. Rather, the aim of this Law was to prevent "abusive use" of nominal data.²⁵⁷ Although this law did not establish any explicit link between the regulation of nominal data processing and the necessity to protect the fundamental rights and freedoms of individuals, it can be inferred from the overall content and structure of that law, and in particular of its Article 15 prohibiting the

²⁵¹ Articles 6 and 7 of the 1978 French data protection law.

²⁵² Lov nr 293 af 8 Juni 1978 om private registre mv.

²⁵³ Lov nr 294 af 8 juni 1978 om offentlige myndigheders registre.

²⁵⁴ Lov av 9. juni 1978 nr 48 om personregistre mm (Personregisterloven).

²⁵⁵ The Norwegian Government's Council for Computers contracted a group of university researchers to look into the issue of computerization of citizen's personal data.

²⁵⁶ Article 3 of the 1979 Luxembourg Law on the Processing of Nominal Data.

²⁵⁷ Article 1 of the 1979 Luxembourg Law on the Processing of Nominal Data provides: « *Les personnes physiques ou morales sont protégées contre l'utilisation abusive de données nominatives* ».

collection of sensitive data,²⁵⁸ that one the main concern of the Luxembourg legislator was to protect individuals against interference with their right to privacy.

The above brief historical analysis shows how data protection laws in Europe were primarily adopted with the objective to regulate the processing of personal data to protect the right to private life of natural persons. On this basis, it can be argued that the broad objective of data protection law to protect individuals' fundamental rights and freedoms is part of its very 'DNA'. In the following decades, data protection law kept on evolving beyond national borders to find a new expression at the regional or international level. Yet, as seen below, the DNA of data protection law mostly remained unchanged.

²⁵⁸ Article 15 of the 1979 Luxembourg Law on the Processing of Nominal Data established a prohibition to process in databanks sensitive data relating to individuals' political opinions, trade union membership, religious or philosophical convictions or the intimacy of private life. Data relating to health could also not be collected and stored in databanks by non-authorized entities. These categories of data are usually considered as 'sensitive' in the sense that their disclosure could potentially harm the right to respect for private and family life of the individuals.

2.1.3. The internationalisation of data protection law in the 80s as a response to globalisation and digitalisation

“Data knows no borders. Nor should data protection.”

– b.telligent Deutschland

End of the 70s, it became more and more apparent that fragmented national laws on the processing of personal data could not sufficiently protect individuals’ right to privacy in an increasingly globalised world. Indeed, unlike the physical persons to which they belong, personal data can be easily and quickly copied and transferred from one computerized system to another, well-beyond the borders of their original state. More than a domestic issue, the processing of personal data thus became a topic of international interest. Supra-national organisations such as the Organization for Economic Co-operation and Development (‘OECD’), the Council of Europe and later the EU therefore started expressing concern about significant discrepancies among national legislation. These discrepancies were setting different levels of protection for data subjects’ rights and freedoms and were creating undue barriers to the trans-border flows of digital information. In particular, there was a risk that some governments would impose restrictions on data transfers to protect their citizens, and that private organizations operating globally would then be barred from sharing data across various jurisdictions, or experience difficulties in complying with different and sometimes incompatible national rules. This could in turn hinder public cooperation, as well as economic, social or technological developments. There was thus an urgent need for legislative harmonization in the field. Hence, beginning of the 80s, a second wave of regulation in the field of data protection impacted the European continent, this time at the supra-national level.

2.1.3.1. The 1980 OECD Guidelines: reconciling the need to protect privacy with the need to allow the free flow of personal data

The OECD is an international organization that was founded in 1961 to stimulate economic cooperation and development among its members. Today, the OECD counts 36 member countries across Europe, America, Asia and Australia, and other ‘key partners’.²⁵⁹ Policies, standards or recommendations published by the OECD are however not only addressed to its members or key partners but have global reach.²⁶⁰ The OECD was the first international organization to adopt a document relating to the transfer of personal data: the 1980 Guidelines for the Protection of Privacy and Trans-border Flows of Personal Data (the “1980 OECD Privacy Guidelines”).²⁶¹

These Guidelines were developed to fulfil a clear dual objective: on the one side, to secure the informational rights of individuals, and, on the other side, to prevent the

²⁵⁹ Such as Brazil, China, India, Indonesia, and South Africa.

²⁶⁰ OECD (2019, May). Discover the OECD. <http://www.oecd.org/general/Key-information-about-the-OECD.pdf>.

²⁶¹ OECD (1980, September 32). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

negatives consequences that diverging national laws could have on economic development.²⁶² It is interesting to note in this respect that, instead of referring to the laws adopted by Sweden, Germany, France, Norway or Luxembourg as data protection laws, the 1980 OECD Privacy Guidelines refer to “*privacy protection laws*”, “*privacy laws*” or “*national privacy legislation*”.²⁶³ This terminological choice can be explained by the composition of the Expert Group in charge of drafting these Guidelines. Indeed, its members included both EU and US experts and its Chairman was an Australian judge.²⁶⁴ In English-speaking countries such as the US and Australia, the word ‘privacy’ was and is still used today as an umbrella term encompassing the notion of private and family life and the right of individuals “*to determine for themselves when, how and to what extent information about them is communicated to others.*”²⁶⁵ By contrast, in the EU, the expression ‘data protection’ was being used to more specifically target the field of law regulating the processing of personal data on computerized systems. The OECD Expert Group had to accommodate these diverging traditions. This resulted in a terminological compromise where data protection was considered as a sub-set of privacy.²⁶⁶ The Explanatory Memorandum accompanying the Guidelines highlights this choice without however providing for any official explanation as to why the US tradition had ultimately prevailed over the European one.²⁶⁷ One of the main reason was probably that, both in the EU and in the US, the right to privacy had already been recognized as a fundamental right, while the expression ‘data protection’ only existed in the EU but had never been endorsed by the US doctrine, case law or legislation.²⁶⁸ Still today, US scholars usually refer to laws regulating the processing of personal data as ‘privacy laws’. One of key consequences of this terminological choice which seems to still have an impact today is that laws regulating the processing of personal data were further primarily associated with the need to

²⁶² The Explanatory Memorandum accompanying the Guidelines state: “*these [national data protection] laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.*” See also the OECD Privacy Framework (2013), p. 69, available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

²⁶³ See Preface of the 1980 OECD Privacy Guidelines.

²⁶⁴ The Hon. Mr. Justice Michael D. Kirby, Chairman of the Australian Law Reform Commission. See Kirby, M. D. (2010). The history, achievement and future of the 1980 OECD guidelines on privacy. *International Data Privacy Law* February 2011 1(1): 6-14.

²⁶⁵ Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum, p. 7.

²⁶⁶ This was confirmed by the Chair of the Expert Group himself, who wrote in this respect: “*the capacity of [new technologies for auto-mated data processing] to expand and expedite the analysis of personal data and to create connections not otherwise perceived was recognized as presenting new problems for privacy as that notion was to be understood in its wider, modern sense.*” (*Ibid.*, p. 6).

²⁶⁷ Paragraph 4 of the of the Explanatory Memorandum to the 1980 OECD Privacy Guidelines states: “*it is common practice in continental Europe to talk about “data laws” or “data protection laws” (lois sur la protection des données), whereas in English speaking countries they are usually known as “privacy protection laws.”*”

²⁶⁸ Gonzáles Fuster, G. (2014), *op. cit.*, p. 79.

protect the right to privacy, and only secondarily with the need to prevent the violation of other human rights.²⁶⁹

Aside from this terminological development, the 1980 OECD Privacy Guidelines also broadened the objectives of data protection rules. The aim of these Guidelines was indeed to reconcile two *prima facie* opposing interests: (i) guaranteeing the protection of individuals' right to privacy on the one hand, and (ii) ensuring the free flows of personal data between member countries on the other hand.²⁷⁰ Through their internationalisation, data protection and privacy rules were thus ascribed a new function: ensuring that personal data could be freely shared and transferred among countries that were respecting minimum standards of data protection. The 1980 OECD Guideless furthermore established important legal notions that have been passed on to future legislative texts, such as the notion of personal data²⁷¹ or the notion of data controller.²⁷² Most importantly, these Guidelines established eight basic principles that members of the OECD were encouraged to adopt into their domestic legislation: (i) the collection limitation principle; (ii) the data quality principle; (iii) the purpose specification principle; (iv) the use limitation principle; (v) the security safeguards principle; (vi) the openness principle; (vii) the individual participation principle; and (viii) the accountability principle. These basic principles are similar to the key-principles of data processing that would later be enshrined in EU law, first in Article 6 of the 1995 Data Protection Directive and then in Article 5 of the GDPR.²⁷³

Despite their non-binding nature, the 1980 OECD Privacy Guidelines, including their 2013 revised version,²⁷⁴ have succeeded in influencing the development of national data protection legislation and model codes within the OECD member countries.²⁷⁵ Regrettably, they have also contributed to the terminological and legal confusion that still exist today around the notions of privacy and data protection. While the historical impact of the OECD Privacy Guidelines is undeniable,²⁷⁶ they were soon shadowed on the European continent by a similar instrument that was adopted by the Council of Europe: Convention 108 on the protection of Individuals with regard to the Automatic Processing of Personal Data ('Convention 108').²⁷⁷ A key feature of

²⁶⁹ See Chapter 2, Section 2.3.4, below on the existence of a perceived 'deficit' in the fulfilment of the FRO of EU data protection law.

²⁷⁰ Expert Group on Drafting Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data.

²⁷¹ Any information relating to an identified or identifiable individual, i.e., the data subject.

²⁷² The party who is competent to decide about the contents and use of personal data regardless of whether or not such data are processed by that party or by an agent on its behalf.

²⁷³ Article 6 of the 1995 Data Protection Directive and Article 5 of the GDPR.

²⁷⁴ The 2013 OECD Privacy Framework, available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

²⁷⁵ *Ibid.*, p. 65-66.

²⁷⁶ The 2013 OECD Privacy Framework notes in this respect: "*The [1980 OECD] Guidelines have been a remarkable success. They represent an international consensus on personal data protection in the public and private sectors. They have influenced the development of national legislation and model codes within OECD member countries, and beyond.*" (p. 69).

²⁷⁷ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, opened for signature on 28 January 1981, entered into force on 1 October 1985.

Convention 108 is that, unlike the 1980 OECD Privacy Guidelines, this instrument is binding upon its signatories.

2.1.3.2. Convention 108 of the Council of Europe: confirmation of the need to ensure the protection of privacy of individuals in the context of data processing

The Council of Europe is a supra-national organisation founded in 1949. Its mission is to promote human rights, democracy and the rule of law on the European continent and achieve greater unity among its members.²⁷⁸ All Council of Europe's members have to be party to the ECHR, which entered into force on 3 September 1953. Today, 46 states are High Contracting Parties to the ECHR, including all 27 EU Member States. Among the institutions of the Council of Europe, the ECtHR is of paramount importance to ensure that all High Contracting Parties apply and respect human rights as enshrined in the ECHR and its Protocols.²⁷⁹

The ECHR does not contain any provision on the right to data protection as such. As a matter of facts, when this instrument was first drafted, modern computers were barely emerging,²⁸⁰ and the notion of personal data protection itself did not yet exist.²⁸¹ Therefore, towards the end of the 60s, when the Council of Europe started to look into human rights issues relating to the use of computers, it did so from the perspective of the right to respect for private and family life, as enshrined in article 8 of the ECHR.²⁸² One of the question that had arisen was whether Article 8 of the ECHR offered sufficient safeguards against abusive data processing practices, especially since Article 8 of ECHR was only applicable to interferences by public authorities and not by private entities.²⁸³ In 1972, it was therefore suggested that a Convention be drafted to bridge this gap and enhance the protection of fundamental

²⁷⁸ Preface and Article 1 of the Statute of the Council of Europe, ETS No. 1, opened for signature on 5 May 1949, entered into force on 3 August 1949.

²⁷⁹ Article 19 of the ECHR.

²⁸⁰ See Turing, A. M. (1937). On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*. 2. 42 (1): 230–265. The idea of a universal computing machine was first developed in 1936 by Alan Turing. However, the first modern computers using microprocessors only emerged beginning of the 70s.

²⁸¹ As a reminder, the first law having endorsed the legal terms “data protection” was the 1970 *Hessische Datenschutzgesetz*. See section 2.1.2 of Part I above.

²⁸² Prior to the drafting of Convention 108, the Council of Europe had already issued multiple Recommendation and Resolutions relating to the protection of human rights, and in particular the right to private and family life (Article 8 of the ECHR), in relation to technological developments: Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments; Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Minister's Deputies, and ; Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

²⁸³ Explanatory report accompanying Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Minister's Deputies

rights in the context of modern issues relating to the processing of personal data.²⁸⁴ A comparative study carried out by the Secretariat of the Council of Europe in 1975 highlighted that national data protection laws in Europe were not all granting the same level of protection to individuals with respect to the processing of their personal data, and that these disparities could hinder the protection of fundamental rights, as well as the free flows of personal data between member states.²⁸⁵ Following this study, a group of experts was set up in 1976²⁸⁶ and was given the mission to draw up an international treaty, working in close cooperation with the OECD.²⁸⁷ This ultimately led to the drafting of the *Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* (hereafter, “Convention 108”).²⁸⁸ Today, all 46 members of the Council of Europe have ratified this instrument, as well as nine non-members of the Council of Europe.²⁸⁹

On paper, Convention 108 has only *one* explicit objective: “*to protect every individual (...) with regard to the processing of [their] personal data, thereby contributing to respect for human rights and fundamental freedoms, and in particular the right to privacy*”.²⁹⁰ Implicitly, the aim of the Convention is also to facilitate the free flows of personal data among its signatories by encouraging them to harmonise their national rules.²⁹¹ The 1980 OECD Guidelines and the Convention 108 are thus very similar with respect to their objective. By contrast, a substantial difference between these two instruments is that Convention 108 is legally binding for its signatories. Another difference resides in the terminology: rather than referring to the protection of privacy, Convention 108 makes it clear that its object is to strengthen “*data protection*”.²⁹² Yet, like most pre-existing national data protection laws, Convention 108 still draws a clear link between data protection rules on the one side, and the protection of the fundamental right to privacy on the other side, by stating that data protection is meant to secure respect for individuals’ rights and fundamental freedoms, and “*in particular the right to privacy*”.²⁹³ In other words, while clearly distinguishing both notions, the Convention puts data protection rules at the service of the right to privacy.

²⁸⁴ Hondius wrote in this respect: “*Only an international treaty can give a satisfactory reply to the complex set of problems posed by the international nature of data flow and data protection. The committee of experts which prepared the Council of Europe Resolutions on data protection first suggested such a treaty in 1972, and the European Conference of Ministers of Justice, which met in Basle in the same year, endorsed the proposal.*” Hondius, F. W. (1980). *Data Law in Europe*. *Stanford Journal of International Law*, 16:87-112, p. 104.

²⁸⁵ Hondius, F. W. (1978). *Council of Europe and Round Table on the Use of Data Processing for Parliamentary Work. The Council of Europe's Work in the Area of Computers and Privacy: Discussion Paper*. Strasbourg: Council of Europe.

²⁸⁶ The Committee of Experts on Data protection, renamed in 1978 the Project Group on data protection (CJ-PD).

²⁸⁷ Hondius, F. W. (1980), *op. cit.*, p. 104.

²⁸⁸ Council of Europe (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No. 108. Strasbourg. Open for signature on 28 January 1981.

²⁸⁹ Argentina, Burkina Faso, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay. Source: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=SVJZxx2k.

²⁹⁰ Article 1 of Convention 8 on the object and purpose of the Convention.

²⁹¹ The third Chapter of the Convention 108 is indeed entirely dedicated to rules with respect to data transfers.

²⁹² Article 1 of Convention 108 and Paragraph 1 of the Explanatory report to the Convention.

²⁹³ Article 1 of Convention 108.

Regarding its substance, Convention 108 of the Council of Europe established various basic principles for the protection for personal data such as the duty to ensure data quality and security,²⁹⁴ or the general prohibition to process sensitive personal data, unless provided by law.²⁹⁵ All the signatories to the Convention were committing to apply these principles by amending or adopting new legislation where necessary.²⁹⁶ Next to those principles, the Convention also granted data subjects individuals rights, such as the right to be informed, the right to obtain the erasure of their personal data or the right *not* to be subject to a decision with significant effects based solely on an automated processing of their data.²⁹⁷ Convention 108 furthermore imposed obligations on data controllers and processors, such as the obligation to ensure the transparency and security of data processing activities, as well as the obligation to document the measures adopted to ensure compliance with those rules and standards.²⁹⁸ An entire Chapter of the Convention was also dedicated to the role and powers that should be given to national supervisory authorities in the field of data protection. Raising awareness about data protection issues, controlling compliance and enforcing the applicable rules were part of the tasks that had to be conferred upon those authorities.

As further shown below, Convention 108 established the foundations of what will later become the structural pillars of EU data protection law and of its functionality: (1) a broad scope – based mainly on the definition given to the notion of ‘personal data’ and ‘processing’; (2) a set of general principles, individual rights and specific obligations and; (3) supervision mechanisms aimed at ensuring the respect of these rules by the concerned actors. In the opinion of the author, these three pillars became the structure on which the functionality of EU data protection law would later grow (see Chapter 3, below).

In the 80s, many European states that had not yet enacted a national data protection law did so in consideration of the OECD Guidelines and Convention 108.²⁹⁹ The Netherlands, for example, signed Convention 108 on 21 January 1988 and adopted its first data protection law by the end of that same year.³⁰⁰ As far as

²⁹⁴ This notion encompassed multiple sub-principle according to which persona data should: (a) be obtained fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, keptup-to-date; and (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

²⁹⁵ Convention 108 identifies different types of sensitive data: personal data revealing racial origin, political opinions or religious or other beliefs, personal data concerning health or sexual life, as well as personal data relating to criminal convictions.

²⁹⁶ Article 3(1) of Convention 108.

²⁹⁷ Article 9(1) of Convention 108.

²⁹⁸ Article 5, 6 7 8 and 10 of Convention 108.

²⁹⁹ González Fuster, G. (2014), *op. cit.*, p. 71 and 92-94.

³⁰⁰ Wet van 28 december 1988, houdende regels ter bescherming van het persoonlijke levensfeer in verband met persoonregistraties (Wet persoonregistraties), Staatsblad van het Koninkrijk der Nederlanden, 1988, no. 662-693, 01-01-1988.

Belgium is concerned, it took the national legislator several attempts³⁰¹ and an extra 10 years after the signing Convention 108 to adopt its first data protection law in 1992.³⁰² Like most of their European predecessors, both the Belgian and the Dutch data protection laws were drawing a clear link between the processing of personal data on the one side, and the need to ensure the respect of the right to privacy, on the other side.



Magazine advertising the VIC-20 computer 1982, starring William Shatner (1982).

2.1.4. Emergence of EU data protection law at the EU level: the 1995 Data Protection Directive

“Computing is not about computers anymore. It is about living.”
 – Nicholas Negroponte (1995), *Being Digital*

Although the first EU legal act regulating the processing of personal data was only adopted in 1995, the EU had not remained oblivious to the technological developments taking place in the field of computer sciences. In the mid-70s, as several Member States were adopting legislation in the field of data protection, the European Parliament started having concerns about the obstacles that conflicting national laws could unwillingly create within the internal market. In 1975, 1976 and 1979 respectively, the European Parliament therefore issued three Resolutions on the protection of the rights of individuals in the face of technical developments in

³⁰¹ Boulanger, M-H., Moreau, D., Léonard, T., Louveaux, S., Poulet, Y., & de Terwangne, C. (1997). La protection des données à caractère personnel en droit communautaire: troisième partie. *Journal des Tribunaux - Droit Européen*, 42:173-179; Dumortier, J. & Robben, F. (1995). *Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer*. Brugge: Die Keure.

³⁰² Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B. 18/03/1993.

the field of the automatic processing of personal data.³⁰³ Each time, it suggested that the Commission should draft an EU-wide legislation establishing common rules and principles for the processing of personal data.³⁰⁴ Then, on 28 January 1981, the Council of Europe opened Convention 108 for signature. Taking the view that this instrument could produce a sufficient level of harmonisation in the field of data protection, the Commission invited all Member States (at that time, 10)³⁰⁵ to ratify it.³⁰⁶ In spite of this official invitation, the ratification process proved to be a challenge for some Member States. Hence, in 1990, several Member States, including the Belgium and the Netherlands, still had not ratified Convention 108. Ultimately, the Commission admitted that Convention 108 had failed at preventing discrepancies between national data protection laws within the EU, and thus submitted a proposal for a directive concerning the protection of individuals in relation to the processing of personal data.³⁰⁷ After five years of negotiations (including a fully revised proposal submitted by the Commission in October 1992),³⁰⁸ the EU adopted a final text in October 1995. The below section will briefly look into the DNA and core objective of this 1995 Data Protection Directive.

2.1.4.1. The Fundamental Rights Objective of the 1995 Data Protection Directive

At the time the 1995 Data Protection Directive was being drafted, the EU institutions could rely on two decades of legislative developments in the field of data protection law both at the national and international level. The influence of these preceding instruments is reflected in the wording, structure and substance of the Directive, as well as in the duality of its objectives. As clearly stated in Article 1 of the Directive, its object was indeed: (1) to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data (the ‘Fundamental rights objective’ or ‘FRO’); and (2) to ensure the free flows of personal data between EU Member States (the ‘Internal market objective’ or ‘IMO’).³⁰⁹

³⁰³ Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developing progress in the field of automatic data processing [1975] OJ C60/48 ; Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developing progress in the field of automatic data processing [1976] OJ C100/27 and; Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing [1979] OJ C140/34.

³⁰⁴ At the time, the EU was still called the European Community. For the sake of harmony, the author will exclusively refer to the EU regardless of the period concerned.

³⁰⁵ Greece joined the EU in 1981, bringing the total number of Member States to 10, next to France, Germany, Belgium, the Netherlands, Luxembourg, Italy, Denmark, Ireland, and the United Kingdom.

³⁰⁶ Commission recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data [1981] OJ L246/31.

³⁰⁷ COM(90) 314 final, Brussels, 13 September 1990.

³⁰⁸ Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (92/C 311/04) COM (92) 422 final — syn 287, 16 October 1992 [1992] OJ C 311, 27.11.1992, p. 30–61.

³⁰⁹ Article 1 of the 1995 Data Protection Directive.

At the time the 1995 Data Protection Directive was adopted, the use of computers was becoming more and more common and the impact of the internet on the collection and sharing of personal data was expected to become substantial. Over the last decades, data processing activities had progressively integrated more and more aspects of humans' life, with the potential to interfere with an array of different fundamental rights and freedoms, from privacy, to the right to an effective remedy, to non-discrimination or freedom of expression (see point B of the Introduction of this study). Hence, the inclusion of such a broad FRO, although appearing as ambitious, was in line with the past and foreseen evolution of digitalization. Furthermore, once seen through the prism of History, the ambitious FRO of the 1995 Data Protection Directive appears both consistent and coherent. Since its origin indeed, data protection law had always been envisaged as a tool to mitigate the risks that computerization was posing to individuals' rights and freedoms, and in particular their right to privacy. The 1995 Data Protection Directive more specifically refers to the right to privacy as "*recognized in Article 8 of the European Convention for the Protection of Human Rights and in the general principles of Community law (...)*". This reference to the ECHR and the general principles of EU law are not innocuous. In 1995, the Charter did not exist yet,³¹⁰ while the ECHR had already acquired a "*special significance*"³¹¹ in the EU legal order. Hence, references to the ECHR in EU legal acts were not rare at the time. It is interesting to note that the 1995 Data Protection Directive refers to the right to privacy as enshrined in Article 8 ECHR, while in the official text of the ECHR, Article 8 is *not* named 'right to privacy' but 'right to respect for private and family life'. The 1995 Data Protection Directive thus seems to consider that both terms are synonymic and interchangeable. This choice may as well reflect the influence of preceding laws, treaty or guidelines in the field of data protection, and in particular of the OECD Privacy Guidelines and Convention 108, which both refer to the right to privacy rather than the right to private and family life.

Next to this FRO, the Directive also stressed the importance to ensure the free flows of personal data among Member States in order to allow public authorities as well as private undertakings to collect and share personal data among them. As already highlighted by the 1980 OECD Guidelines and Convention 108, cross-border transfers of personal data had indeed become increasingly important for a wide range of public, economic and social activities, including collaboration between Member States' authorities, or commercial partnerships between undertakings located in different Member States.³¹² Although the FRO and the IMO of the 1995 Data Protection Directive are presented as equally important, the competence of the EU to draft and adopt the 1995 Data Protection Directive actually rested on the IMO alone. At the time indeed, the EU had not been recognized any exclusive or shared

³¹⁰ The EU Charter of Fundamental Rights and Freedoms was proclaimed five years later, in 2000, and only came into force in 2010.

³¹¹ CJEU, Judgement of the Court of 18 June 1991, *ERT*, Case C-260/89, para. 41.

³¹² Recitals 4 to 6 of the 1995 Data Protection Directive.

competence in the field of fundamental rights protection and could therefore not legislate on this basis alone. By contrast, Article 100a of the Treaty establishing the European Community (now Article 115 TFEU)³¹³ granted to the European Parliament and the Council the task to adopt measures in order to harmonize Member States laws for the establishment and functioning of the internal market. With this mind, the competence of the EU to adopt the 1995 Data Protection Directive exclusively rested on grounds relating to the functioning of the internal market, and not on grounds of fundamental rights protection.³¹⁴ This is clearly reflected Recitals 6th to 8th of the Directive, which provide that the difference in levels of protection of the rights and freedoms of individuals with regard to the processing of personal data could prevent the transmission of such data from the territory of one Member State to another, and consequently create obstacles to the pursuit of a number of economic activities, distort competition and impede cooperation between public authorities. Establishing a level playing field for controllers, processors and data subjects across the EU by adopting an EU-wide data protection directive had thus been described as “*vital to the internal market*”.³¹⁵ To fulfil those dual objectives (FRO/IMO), the 1995 Data Protection Directive compiled state-of-the-art definitions,³¹⁶ an ambitious material and territorial scope,³¹⁷ the set of principles, rights and obligations already consecrated in Convention 108, as well as more refined supervision mechanisms, as further discussed below.

2.1.4.2. The transposition of the 1995 Data Protection Directive by Member States and its lack of enforcement

The 1995 Data Protection Directive was built around the three structural pillars already established by Convention 108 (the three ‘S’). In a nutshell:

³¹³ TFEU stands for Treaty on the Functioning of the European Union. Together with the TEU, the TFEU forms the current constitutional basis of the EU.

³¹⁴ Some scholars have argued that the 1995 Data Protection Directive was primarily focused on establishing principles of good governance and imposing obligations on controllers and processors in relation to the processing of personal data, rather than on protecting the fundamental rights of the individuals (see, for example, van der Sloot, B. (2014). Do data protection rules protect the individual and should they? An assessment of the proposed General data Protection Regulation. *International Privacy Law* 4(4):307-325, cited by McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1):2-7). Although it is correct that the GDPR extended or introduced new rights for the data subjects, it would be erroneous to argue that the 1995 Data Protection Directive was exclusively focused on the obligations of controllers and processors. Several rights had already been enshrined, such as the right to information, access or rectification. Furthermore, the dual objective of the Directive expressly included the protection of data subjects’ fundamental rights and freedoms.

³¹⁵ Recital 8 of the 1995 Data Protection Directive.

³¹⁶ As an example, the 1970 Hessische Datenschutzgesetz already defined personal data as follows; “*Personal data are details about the personal and factual circumstances of an identified or identifiable natural person*” (in the original text: “*Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).*”) The 1995 Data Protection Directive defines personal data as follows: “*personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*”.

³¹⁷ See, for example, Moerel, L. (2011). The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? *International Data Privacy Law*, 1(1):23-41; and Post, D. (2014). The long arm of the EU Data Protection directive. *Computing*, 24.

- The **Scope** of the Directive was relatively broad, taking into account in particular the definition given to the notion of ‘personal data’ and ‘processing’. Like in most preceding legislation, the Directive defined personal data as information relating to an identified or identifiable natural person, thereby excluding legal entities. As far as its material scope was concerned, the Directive was applicable to “*processing of personal data wholly or partly by automatic means*” and to “*processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*”. For example, for the storage of medical data such as patient files, the Directive would apply regardless of whether these files would be stored on a server managed by a public hospital or in the paper filing system of general practitioner;
- The Directive also reaffirmed the **Substance** of data protection law, with general principles governing the processing of personal data, individual rights for data subjects, and specific obligations for controllers and processors.
- The Directive also reinforced the **supervision and sanction mechanisms** applicable to the processing of personal data. In particular, each Member State was given the task to establish a national independent authority for supervising the application of data protection law (if not existing yet) and to grant special competences and powers to this DPA.³¹⁸ With respect to sanctions, the Directive required Member States to “*adopt suitable measures to ensure the full implementation of [the Directive]*”, and to “*lay down the sanctions to be imposed in case of infringement*”.³¹⁹ The amount and nature of these sanctions was however left to the discretion of each Member State.

Member States were given “*a period of three years from the date of its adoption*”³²⁰ to transpose the 1995 Data Protection Directive. EU directives are indeed legislative acts which are addressed to Member States and which need to be transposed by each Member State into national law to become enforceable. If a Member State would fail to fulfil this obligation, a person could invoke the provisions of the 1995 Data Protection Directive against that Member State³²¹ but would not be able to invoke these provisions against another person directly, such as a controller.³²² The effectiveness of EU Data Protection Law was thus to a great extent dependent on the action of the Member States. Furthermore, it must be noted that directives are a

³¹⁸ Article 28 of the 1995 Data Protection Directive.

³¹⁹ Article 24 of the 1995 Data Protection Directive.

³²⁰ Article 32(1) of the 1995 Data Protection Directive.

³²¹ The direct *vertical* effect of directives has been recognized for the first time in 1974 in the case *Van Duyn* (CJEU, Judgment of the Court of 4 December 1974, *Yvonne van Duyn v Home Office*, Case 41/74). For the provisions of a directive to have a direct vertical effect, these provisions must be unconditional and sufficiently clear and precise.

³²² The absence of direct *horizontal* effect has been confirmed in multiple case-law, and originally in the *Marshall* case (CJEU, Judgment of the Court of 26 February 1986, *Marshall v Southampton and South West Hampshire Area Health Authority*, Case 152/84).

type of EU legal acts that set goals which must be achieved while leaving a certain margin of manoeuvre to Member States regarding the means of implementation. As a consequence, national legislation transposing the 1995 Data Protection Directive slightly differed from one Member State to another. For example, Article 9 of the 1995 Data Protection Directive stated that, when necessary to reconcile the right to privacy with the rules governing freedom of expression, Member States had to provide for “*exemptions or derogations*” to data protection rules to facilitate the processing of personal data carried out “*for journalistic purposes or the purpose of artistic or literary expression*”. The Directive did not indicate however the nature or extent of such exemptions or derogations.

Although the 1995 Data Protection Directive was not conceptually innovative, it had nonetheless a substantial impact in the EU in terms of legislative reforms, even if some Member States failed to transpose it within the given deadline.³²³ This was the case of the Netherlands, Luxembourg, France, Germany and Ireland.³²⁴ As a consequence, the Commission initiated proceedings against those countries before the CJEU in December 2001.³²⁵ Eventually, each of these Member States amended or adopted a new law on data protection in compliance with the Directive’s goals and requirements. A major flaw of many of these national laws was, however, the absence of deterrent sanctions in case of an infringement. This, in turn, contributed to the partial ineffectiveness of data protection law in the EU. As the years went by, it gradually appeared that EU data protection law was slowly turning into a ‘dead letter, and that its objective to adequately protect data subjects against intrusive or unlawful processing practices was not fully met.³²⁶ This, in turn, prompted the Commission to initiate a legislative reform which led to the adoption of the GDPR,³²⁷ as further discussed below (see Chapter 3, below).

2.1.5. Concluding remark: since its origin, EU data protection law has been conceived as a tool to protect data subjects’ fundamental rights, and in particular their right to privacy

The above Chapter has given an overview of the origin of the broad FRO of EU data protection law. As seen above, the 70s were marked by a first wave of national legislation regulating the processing of personal data on the European continent in response to concerns over computerization. In particular, the fact that states or private organisations could increasingly rely on the computing power of machines to process vast amount of data about individuals raised a number of concerns over

³²³ Robinson N., Graux H., Botterman M., & Valeri L. (2009). Review of the European Data Protection Directive. RAND Technical report. California: RAND Corporation. https://www.rand.org/pubs/technical_reports/TR710.html, p. 8.

³²⁴ Those Member States failed to notify the Commission in time about the measures that they had taken in order to implement the Directive within the 3-years period that was granted to them after its adoption.

³²⁵ European Commission (2003). First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final, p. 1, footnote 1.

³²⁶ Koops, B.-J. (2014). *op. cit.*, p. 250.

³²⁷ Kosta, E. (2014). *op. cit.*

confidentiality and privacy. Those concerns included, *inter alia*, the possibility of linking different databases, the creation of individual profiles and the mass surveillance of citizens by public authorities. Or, as summarized by Jacques Desabie³²⁸ in an interview for the national French television on 17 September 1975, computerization had raised the question of “*who has the right to know what about who*”.³²⁹ In addressing this question, various governments initiated legislative debates across the European continent. While most states (such as Germany, Sweden, France or Luxembourg) had decided to approach this issue from a regulatory stance by subjecting data protection activities to a prior authorisation, other states (such as Portugal or Spain) approached it from the perspective of fundamental rights protection by giving constitutional value to an embryonic form of the right to personal data protection. Regardless of the approach taken, most of these provisions were already drawing a clear link between the regulation of data processing on the one side, and the need to protect the right to privacy of individuals on the other side.

Prior to the adoption of data protection rules by various states, the right to privacy had already gained international recognition as a human right in the UDHR, the ECHR and the ICCPR. This right was then mainly understood as protecting individuals against arbitrary interferences by the state with their ‘private life’ (i.e., the privacy of their home, of their family, of their personal communications, etc.) by opposition to their ‘public life’ (i.e., activities in the public sphere, realisation of civic duties, professional activities, etc.). Yet, no clear definition of the concept of ‘privacy’ or ‘private life’ had been provided in any human rights treaty, thereby leaving the door open for interpretation. It should therefore not come as a surprise that that the scope of the right to privacy was extended through the years and started covering aspects that were probably not initially envisaged at the time where the UDHR, the ECHR or the ICCPR were being codified.³³⁰ Keeping this in mind, the evolution of data protection legislation as a tool to guarantee the respect of the right to privacy should be appreciated in parallel with the “*career of the right to privacy*” itself.³³¹

In the 80s, because of globalization and continuous technological advances, and in particular the facilitation of data transfers from one country to another, national data protection laws became increasingly easy to circumvent. Prohibiting all cross-border data transfers for the sake of individuals’ privacy was however neither a practical solution, nor a beneficial measure for economic or social developments. Aware of this duality, the OECD and the Council of Europe both adopted an

³²⁸ Jacques Desabie was the former director of the National Institutes for Statistics and Economic Studies in France (INSEE). This Institute had created the first digital national identification registry in France based on a unique identifier: the social security number of each citizen or residents.

³²⁹ « *Il y a un problème moral dans ces questions; c’est de savoir qui a le droit de savoir quoi sur qui.* » (Source : interview with Jacques Desabie on 17 September 1975. Le Journal A2 20H. Informatique : un risque pour les libertés individuelles?, archive available at <https://sites.ina.fr/cnil-40-ans/focus/chapitre/2/medias/CAB7501179101>)

³³⁰ Diggelmann, O. & Cleis, M. (2014). *op. cit.*, p. 457.

³³¹ Diggelmann, O. & Cleis, M. (2014). *op. cit.*, p. 457.

instrument whose aim was to set common data protection standards among all concerned states. By establishing a level-playing field for the protection of fundamental rights with respect to data processing, it was expected that states would be less likely to impose restrictions on cross-border data transfers. With this vision in mind, the 1980 OECD Guidelines and Convention 108 were adopted in order to pursue two dual and yet complementary objectives: the protection of the fundamental rights of individuals on the one side, and the free flows of personal data on the other side. With respect to the first objective, particular emphasis was put on the need to ensure the respect of the right to privacy. This was a logic arrangement at the time, since national legislation regulating the processing of personal data was already putting emphasis on the right to privacy, and since personal data protection had not yet been recognized as a fundamental right on its own. Despite some promising elements, the overall effectiveness of the OECD Guidelines and of Convention 108 proved limited. Among the negative factors which restrained the overall effectiveness of these instruments, one may point, in particular, the fact that the OECD Guidelines were not (and are still not) binding, and that the ratification process of Convention 108 turned out to be slow and inconclusive in terms of national reforms. This does not mean, however, that these instruments did not contribute to the growth of the functionality of EU data protection law. Indeed, the three structural pillars that these conventions established were passed on, from one legislative text to another, to eventually find their way in the 1995 Data Protection Directive. In the opinion of the author, and as further argued in this study (see Chapter 3 below), these three structural pillars constitute the foundational factors of the functionality of EU data protection law as it stands today.

The 1995 Data Protection Directive was the first EU legislative act to comprehensively regulate the processing of personal data at the EU level. Its content was the logic result of two decades of legislative developments at the national and international level. Due to its ambitious scope, substance, and supervisory mechanisms, one could have expected the 1995 Data Protection Directive to become an effective instrument for the protection of individuals' fundamental rights against harmful data-driven practices. This expectation partly materialised in the following years, especially through the generous interpretation and active stance taken by the CJEU in the field of data protection law (see Section 2.3, below). Among factors of effectiveness and functionality, one may point out the consecration of the three structural pillars of data protection law, or the existence of provisions facilitating access to justice by data subjects.³³² Those positive factors were however partly cancelled out by some internal flaws. As pointed out in the literature, one major internal factor which hindered the overall effectiveness and functionality of the Directive was the absence of provision establishing harmonized administrative and criminal sanctions. Compliance with the law – and this is particularly true for imperative rules – is indeed largely dependent on the existence of deterrent

³³² In Luxembourg, for example, a cease-and-desist action had been made available to data subjects and the data protection authorities against infringers.

sanctions.³³³ With respect to the 1995 Data Protection Directive in particular, it could have increased preventive compliance actions from controllers and processors, but also encouraged governments to seriously finance data protection authorities. Those authorities would then have been able to better perform their tasks and directly impose administrative sanctions when needed. Instead, the workforce of those authorities was largely buried under administrative tasks, such as maintaining a register of notifications which proved completely cumbersome.³³⁴

Next to the lack of harmonized sanctions and the administrative burden of the prior notification system, one may also point negative *external* factors which have hindered the overall effectiveness of the 1995 Data Protection Directive, and in particular the sudden surge in the use and capabilities of computers and other data-processing machines in the years following the adoption of the Directive. It must indeed be acknowledged that, end of the 90s, only medium to big enterprises could afford and rely on IT systems. For most people, computers were still a luxury or an important investment, as illustrated by the ad for computer loans below. In parallel, the scope of data processing activities was still quite rudimentary given the limited storage and processing capacity of computers, and the fact that the internet itself was still in its infancy.³³⁵ The situation however quickly evolved, with most EU families being able to afford a computer in less than a decade after the adoption of the Directive. In the years 2000s, especially, the boom of the internet and of connected devices caused the overall scale of collection and use of personal data to surge. In parallel, the 1995 Data Protection Directive progressively lost its relevance and thus effectiveness.³³⁶ Overall, it can therefore be concluded that the 1995 Data Protection Directive established the foundations of the functional nature of EU data protection law. Yet, as further argued below, such a framework still needed to grow and adapt to the changing technological environment to reach its full maturity and become truly multi-functional with respect to fundamental rights protection.

This brief historical review of the birth and growth of EU data protection law was meant to shed light on the origin of the FRO of EU data protection law, and on the construction of its main pillars of functionality. In particular, it can be concluded that the objective of protecting fundamental rights, and in particular the right to privacy, was inscribed in the DNA of EU data protection law.

³³³ Friedland, M. (1989). *Sanctions and Rewards in the Legal System: A Multidisciplinary Approach*. University of Toronto Press; Van Gerven, W. & Zuleeg, M. (1996). *Sanktionen Als Mittel Zur Durchsetzung Des Gemeinschaftsrechts*. Köln : Bundesanzeiger ; Foucault, M. (1989). *op. cit.*

³³⁴ Article 18(1) of the 1995 Data Protection Directive provided that controllers had to notify their national supervisory authority before carrying out any wholly or partly automatic processing operation. It had probably not been foreseen by the EU legislator that the processing of personal data within private or public organisations would become the rule rather than the exception. As a consequence, data protection authorities were submerged with notifications that they could not all properly review.

³³⁵ In 1995, only 1% of the EU population was using the Internet.

³³⁶ On this topic, see the speech of Viviane Reding, Vice-President of the European Commission. Redding, V. (2012, June 18). Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world. *Digital Enlightenment Forum*. Luxembourg. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_464.



This ad from the college newspapers of California State University of 22 February 1995,³³⁷ presents students with the possibility to apply for a 2-year loan to get a computer.

2.2. EU DATA PROTECTION LAW IN THE 21ST CENTURY: A FRAMEWORK AT THE SERVICE OF THE FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION

In December 2000, i.e., five years after the adoption of the 1995 Data Protection Directive, the EU enshrined the right to personal data protection in the EU Charter of Fundamental Rights, thereby placing it at equal footing with the right to privacy. Those developments have significantly impacted the FRO of EU data protection law. From a tool at the service of the fundamental right to privacy, EU data protection law gradually became a tool at the service of the fundamental right to personal data protection itself. This section will precisely aim at briefly retracing the steps which have led to this shift. Beyond exploring the origin, meaning and substance of the fundamental right to personal data protection, this Chapter will also analyse the impact that it had on the functionality of EU secondary law in the field of data protection with respect to its FRO.

2.2.1. The ‘unveiling’ of the fundamental nature of the right to personal data protection

Section 2.1.1 above has already briefly retraced the historical steps which have led the EU to adopt its own catalogue of human rights, from the 70s up to the year 2000. It is important to keep in mind that, in parallel to this process which has led to the adoption of the Charter, data protection law was finding new forms of expression at the national and international level. Looking back at various documentation covering that period, one can notice some early interactions between the growing body of EU fundamental rights on the one side, and the emerging body of EU data protection law on the other side. Ultimately, these interactions led to the inclusion of the right

³³⁷ Source: CSU Chicago Digital Collection, available via <https://library.csuchico.edu/special-collections/license>.

to personal data protection as a self-standing fundamental right within the Charter, as retraced below.

The first preliminary steps in that direction took place in 1975, 1976 and 1979 respectively, when the European Parliament adopted three Resolutions, whose aim was to ensure the protection of individuals rights in the context of data processing.³³⁸ The next important step took place in 1989, when the European Parliament adopted a Resolution establishing the Declaration of Fundamental Rights and Freedoms.³³⁹ From the perspective of EU data protection law, it is interesting to note that this Declaration already contained a provision entitled ‘Right to information’, which recognised a right of access and correction to personal data, i.e., a somewhat embryonic form of the fundamental right to personal data protection as we know it today.³⁴⁰ This Declaration, however, did not have any significant impact within the EU legal order since it lacked any legally binding force.³⁴¹

In 1996, i.e., the year following the adoption of the 1995 Data Protection Directive, a *Comité des Sages* appointed by the Commission published a report recommending that a bill of fundamental rights be included in the Treaties.³⁴² This report highlighted in particular that modern technologies were triggering novel issues in terms of fundamental rights protection³⁴³ and further suggested that a new generation of rights be recognised taking into account these technological changes.³⁴⁴ A right to personal data protection could have supposedly been part of this new generation of EU fundamental rights. When the Amsterdam Treaty was adopted in 1997 however, the EU missed its chance to amend the founding Treaties so as to include a bill of innovative fundamental rights, as recommended by the *Comité des Sages*.³⁴⁵

In 1999, the Commission appointed a Group of Experts in order to carry forward the debate initiated by the *Comité des Sages* on the opportunity for the EU to adopt its own catalogue of fundamental rights.³⁴⁶ This Expert Group was composed of eight

³³⁸ Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developing progress in the field of automatic data processing [1975] OJ C60/48 ; Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developing progress in the field of automatic data processing [1976] OJ C100/27 and; Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing [1979] OJ C140/34.

³³⁹ Resolution of the European Parliament adopting the Declaration of Fundamental Rights and Freedoms [1989] OJ C 120/51.

³⁴⁰ Article 18: “Everyone shall be guaranteed the right of access and the right to corrections to administrative documents and **data concerning them.**” [emphasis added]

³⁴¹ González Fuster, G. (2014). *op. cit.*, p. 187-188.

³⁴² *For a Europe of Civic and Social Rights*, report by the Comité des Sages, 27 July 1996, p. 41.

³⁴³ *Ibid.*, p. 41.

³⁴⁴ *Ibid.*, p. 9.

³⁴⁵ Instead, the following simple reference to human rights was included in the TEU: “The Union is founded on the principles of liberty, democracy, **respect for human rights and fundamental freedoms**, and the rule of law, principles which are common to the Member States” [emphasis added] (Article 1(8) of the Treaty of Amsterdam (1997), amending Article F, paragraph 1 of the TEU).

³⁴⁶ European Commission (1999). Directorate-General for Employment, Social Affairs and Inclusion, *Affirming fundamental rights in the European Union: Time to act: Report of the Expert Group on Fundamental Rights*, Publications Office.

experts. Its President, Spiros Simitis, was Director of the Research Centre for Data Protection at the University of Frankfurt at the time and had previously been Chief Data Protection Commissioner for the state of Hessen; he was thus well acquainted with EU developments in the field of data protection law. It is therefore not a coincidence if the Final Report issued by the Expert Group on Human Rights in June 1999 contained multiple references to data protection law.³⁴⁷ Most importantly, in its final recommendations, the Expert Group stated that the EU catalogue of fundamental rights should contain rights already recognised in the ECHR, but also additional rights “*detailing or complementing the ECHR*”, among which “*the right to determine the use of personal data*”.³⁴⁸ One may wonder why the Expert Group on Human Rights had chosen the expression ‘right to determine the use of personal data’ over ‘right to personal data protection’, which would have been more in line with the wording of the 1995 Data Protection Directive. The fact that Spiros Simitis was a German scholar seems to provide part of the answer. Since the early 80s indeed, the Constitutional Court of Germany³⁴⁹ had started to recognise and to articulate a “*right to informational self-determination*”³⁵⁰ based on Article 1 (human dignity) and Article 2 (personality right) of the *Grundgesetz*.³⁵¹ Such a right included the capacity for individuals to determine the disclosure and use of their personal information. It may be considered ironic that the Constitutional Court of Germany – the country in which the expression ‘data protection’ was invented (cf. the 1970 *Hessische Datenschutzgesetz*) – ultimately opted for a different wording, while the EU itself had adopted the expression ‘data protection’ in most legislative acts and would later enshrine a fundamental right to personal data protection. From a purely terminological point of view, it is true that the terms ‘data protection’ appears misleading since it puts emphasis on the data rather than the individuals behind

³⁴⁷ *Ibid.*, p. 13: in the third Chapter of the Final Report, the Expert Group highlighted the deficit and inconsistencies of fundamental rights protection across the three pillars of the EU. As an illustration of this deficit, the report referred to the “*quest for improvement of the protection of personal data*”. The report also pointed out the inconsistency in the EU’s approach which, on the one hand, had already drawn a clear link between data protection and fundamental rights in the 1995 Data Protection Directive, while it had, on the other hand, completely failed to take into consideration respect for fundamental rights in the framework of multiple EU agreements involving the processing of personal data by the EU institutions and/or the Member States, such as the Europol Treaty: “*While Parliament, Council and Commission, in connection with the adoption of the 1995 data protection directive, unanimously pointed to the direct link between data protection and fundamental rights, the Member States followed a restrictive policy in the two other pillars. The very principles and measures that had been accepted in the case of the directive in order to respect fundamental rights were thus questioned and to a large extent abandoned in agreements such as the Europol Treaty.*” In the final Chapter of the Report (“*Recommendations*”), the Expert Group also made critical comments about the separation traditionally made in the doctrine between civil rights and social rights, and positioned itself in favour of the theory of the indivisibility of fundamental rights. The Expert Group therefore argued that any attempt to explicitly recognize fundamental rights at the EU level should include both civil and social rights, without differentiating their status or importance. To illustrate its point, the Expert Group referred once again to the right to data protection, arguing that the right to privacy of employees, for example, could be accurately formulated “*only in connection with an explicit recognition of individuals’ right to determine the processing of their data*”.

³⁴⁸ *Ibid.*, p. 24.

³⁴⁹ The first German judgment referring to a right to informational self-determination was rendered by the Constitutional Court in 1983: BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf diemündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden (the “*Population Census Decision*”).

³⁵⁰ In German, “*Recht auf informationelle Selbstbestimmung*”.

³⁵¹ *Grundgesetz für die Bundesrepublik Deutschland* (The Basic Law for the Federal Republic of Germany, i.e., the German Constitution).

those data. Burkert in particular considers the expression ‘Datenschutz’ or ‘data protection’ to be a misnomer since the law does not primarily intend to protect the data, as it might suggest, but rather the rights of the individuals to whom these data relate.³⁵² In that sense, it is true that the German expression ‘right to informational self-determination’ can be considered more accurate with respect to the actual content of that right.³⁵³

Following the 1999 Cologne Council and the final recommendations of the Group of Experts, the European Council appointed a special body – the Convention – in charge of drafting the Charter of Fundamental Rights of the EU. At that time, the European Council had taken the view that “**the fundamental rights applicable at [the EU] level should be consolidated in a Charter and thereby made more evident**” (emphasis added).³⁵⁴ The European Council adopted a binding decision in this respect (“the Decision”).³⁵⁵ This Decision confirmed that there was “*a need, (...), to establish a Charter of fundamental rights in order to make their overriding importance and relevance more visible to the Union's citizens*” (emphasis added). On paper, the mandate of the Convention was thus limited to identifying and inscribing within a Charter already existing fundamental rights in order to make them “*more evident*”.³⁵⁶ The sources in which the Convention could find such rights were specified in the Decision itself: as far as civil or political rights were concerned, reference was made to the general principles of EU law;³⁵⁷ and as far as social rights were concerned, reference was made to two treaties protecting the rights of workers in the Internal Market.³⁵⁸

Behind this apparently limited mandate, however, two elements of the European Council’s Decision gave some margin of manoeuvre to the Convention for uncovering innovative fundamental rights: first, the Decision was based on the assumption that some fundamental rights were not visible enough since the very purpose of the Charter was to “*make their overriding importance and relevance more visible to the Union's citizens*” (emphasis added).³⁵⁹ This wording thus implied

³⁵² Burkert H. (1999), Privacy-Data Protection: A German/European Perspective, in Proc. 2nd Symposium of the Max Planck Project Group on the Law of Common Goods, 62, p. 46; see also Adam Warren & James Dearnley (2005), Data protection legislation in the United Kingdom, *Information, Community & Society*, 8:2, p. 239.

³⁵³ See below for a further analysis of the right to informational self-determination as construed by the German courts.

³⁵⁴ Cologne European Council of 3 and 4 June 1999. Para. 44 of the Conclusions of the Presidency.. http://www.europarl.europa.eu/summits/kol1_en.htm.

³⁵⁵ European Council Decision on the Drawing Up of a Charter of Fundamental Rights of the European Union (Annex IV of the Conclusions of the Presidency. Cologne European Council, 3 and 4 June 1999. http://www.europarl.europa.eu/summits/kol1_en.htm).

³⁵⁶ Cologne European Council of 3 and 4 June 1999. Para. 44 of the Conclusions of the Presidency.. http://www.europarl.europa.eu/summits/kol1_en.htm.

³⁵⁷ i.e., drawing inspiration from international treaties to which the Member States are signatories, such as the ECHR, and their common constitutional traditions.

³⁵⁸ i.e., the European Social Charter and the Community Charter of the Fundamental Social Rights of Workers. Although no other source is mentioned, the Decision does not seem to envisage these sources as being exclusive.

³⁵⁹ First paragraph of the European Council Decision on the Drawing Up of a Charter of Fundamental Rights of the European Union (Annex IV of the Conclusions of the Presidency. Cologne European Council, 3 and 4 June 1999. http://www.europarl.europa.eu/summits/kol1_en.htm).

that the Convention did not have to merely copy fundamental rights that had already been explicitly recognised at the EU level, but could also uncover other fundamental rights whose existence was less “*visible*”.³⁶⁰ Such other rights could include, for example, rights buried in the case law of the CJEU, or rights in need of being remodelled in light of “*social progress and scientific and technological developments*”.³⁶¹ Second, while it is true that the European Council’s Decision explicitly mentioned different sources for uncovering EU fundamental rights,³⁶² it did not present such sources as being exhaustive.³⁶³ Furthermore, even if these sources had been exhaustive, one must admit that the protection of fundamental rights as guaranteed in the general principles of EU law (one of the explicitly mentioned sources) is a rather elastic concept, especially since these general principles are based on two further external sources for the protection of human rights: international treaties of which Member States are signatories (and in particular the ECHR), as well as the constitutional traditions common to the Member States.

At the end of the day, the Convention *did* include data protection as a stand-alone right³⁶⁴ in the final version of the EU Charter of Fundamental Rights (Article 8 – *Protection of Personal Data*).³⁶⁵ Such an inclusion seems to be justified by both official and unofficial reasons, as briefly discussed below.

2.2.2. The reasons behind the inclusion of Article 8 in the Charter

2.2.2.1. Official reasons behind the inclusion of Article 8 in the Charter

In 2007, i.e., seven years after the Charter was proclaimed, the EU published the final version of a document explaining the content of the Charter of Fundamental Rights, article per article (the ‘Explanation(s)’).³⁶⁶ The Explanations were originally prepared under the authority of the Praesidium and were updated before their publication in the Official Journal in 2007 because of some drafting adjustments

³⁶⁰ *Ibid.*

³⁶¹ This has been confirmed *a posteriori* in the Preamble of the Charter of Fundamental Rights of the EU which provides in its 4th paragraph that “(...) *it is necessary to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter*”.

³⁶² Second paragraph of the European Council Decision on the Drawing Up of a Charter of Fundamental Rights of the European Union (Annex IV of the Conclusions of the Presidency. Cologne European Council, 3 and 4 June 1999. http://www.europarl.europa.eu/summits/kol1_en.htm).

³⁶³ The exact sentence being: “*The European Council believes that this Charter should contain the fundamental rights and freedoms as well as basic procedural rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and derived from the constitutional traditions common to the Member States, as general principles of Community law.*” [emphasis added]

³⁶⁴ The expression “*stand-alone fundamental right to data protection*” is often used to stress that data protection was recognised as an independent right and was given its very own Article in the Charter, independently from the right to respect for private and family life. See for example, McDermott, Y. (2017). *op. cit.* pp. 2-7.

³⁶⁵ Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.

³⁶⁶ Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, p. 17–35.

made to the Charter³⁶⁷ as well as further developments of Union law.³⁶⁸ Although having no clear legal value, these Explanations presumably offer some insight into the official sources behind the inclusion of each fundamental right in the Charter.

The Explanation on Article 8 of the Charter (*Protection of personal data*) refers in particular to the following sources:

- Article 286 TEC³⁶⁹ (according to which EU legislation in matters of data protection should apply to the EU institutions and bodies);
- The 1995 Data Protection Directive (which had established a clear link between the protection of personal data and the protection of individuals' fundamental rights, in particular the right to privacy);
- Article 8 of the ECHR on the right to respect for private and family life (aka the right to privacy);
- Convention 108 of the Council of Europe (a treaty that all Member States had adhered to, and which also recognised the link between the protection of personal data and the protection of fundamental rights, in particular the right to privacy);
- Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.³⁷⁰

It is worth noting that none of the above-mentioned sources contain any explicit or implicit reference to the fundamental nature of the right to data protection.³⁷¹ Rather, a majority of these sources present data protection as a set of legal rules *at the service* of fundamental rights, and in particular at the service of the right to

³⁶⁷ Most notably amendments made to Articles 51 and 52 on the scope of the Charter.

³⁶⁸ *Ibid.* (see introductory comment).

³⁶⁹ Introduced by the Treaty of Amsterdam in 1999 and later modified by the Lisbon Treaty in 2009 (now article 16 of the TFEU).

³⁷⁰ Regarding this last source, it must be noted that Regulation (EC) No 45/2001 was adopted *after* the Charter was proclaimed. The Convention could have therefore not possibly been able to rely on this Regulation in the year 2000 with a view of uncovering the fundamental nature of the right to data protection. The reference was thus probably added later, at the time the Explanations were updated before their publication in 2007 (Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1).

³⁷¹ González Fuster, G. (2014). *op. cit.*, p. 206. González Fuster and Gutwirth also note in this respect that none of these sources listed in the Explanation on Article 8 "*ever mentioned any right to the protection of personal data or advanced 'data protection' in an autonomous fashion*". See González Fuster, G. & Gutwirth, S. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 29(5), p. 535.

privacy.³⁷² Article 8 of the ECHR, which is also mentioned as a relevant source in the Explanations, embodies the right to privacy.

One may wonder why the right to privacy as enshrined in Article 8 of the ECHR was mentioned among the relevant sources for the recognition of an EU fundamental right to personal data protection. One could even argue that invoking the right to privacy in this context could lead to more confusion, as it could imply that data protection would be a mere sub-set of the right to privacy.³⁷³ This reference is however not as far-fetched as it might first appear. Two possible justifications may be spelled out in this respect. First, most legislative texts adopted since the 80s had always singled out the special connection between privacy and data protection, usually presenting the right to privacy as benefitting from legislation in matters of data protection.³⁷⁴ This special connection could entail that the data protection-related rights had gained a similar (or even identical) value than the right to privacy. This could in turn be used as an argument in favour of the recognition of the fundamental nature of data protection-related rights. Second, the case-law of the ECtHR interpreting Article 8 ECHR had been broadened over time to ultimately encompass elements that were primarily attached to the field of data protection law.³⁷⁵ For example, Article 8 ECHR had already been interpreted as providing the right for individuals to request access to a personal file held by the police.³⁷⁶ This echoed the right to access one's personal data commonly granted to individuals under data protection law. In other words, the fact that the ECtHR had broadly interpreted the right to privacy and had already recognised the fundamental nature of some data protection-related rights might have thus been regarded as an element in support of the recognition of an EU fundamental right to personal data protection.

As already mentioned above, however, invoking Article 8 of the ECHR as a way to legitimate the fundamental nature of the right to data protection can be seen as a double-edged sword, supporting the Praesidium's decision on the one side, while bringing about more confusion on the other side. In particular, the following question probably arose out of this confusion: if the right to privacy has been interpreted by the ECtHR as encompassing data protection-related rights, such as the right to access one's personal data, should these data protection-related rights be considered as a *subset* of the right to privacy? The persons involved in the drafting of the Charter undoubtedly engaged into long discussions on this subject. Indeed, the different drafts of the Charter reveal that the Convention was hesitating

³⁷² See section 2.1.5, above.

³⁷³ A structural vision in line with the US notion of privacy which had already shaped the OECD Privacy Guidelines.

³⁷⁴ See section 2.1 of this Chapter, which has retraced the different legislative texts linking data protection to the right to privacy.

³⁷⁵ De Hert, P. & Gutwirth, S. (2009). *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. Reinventing data protection?* eds. Serge Gutwirth, Yves Pouillet, Paul de Hert, Cécile de Terwangne and Sjaak Nouwt eds. Berlin: Springer; Nardell, G. (2010). *Levelling up: Data Privacy and the European Court of Human Rights. Data Protection in a Profiled World*, eds. Serge Gutwirth, Yves Pouillet and Paul de Hert. Dordrecht: Springer, pp. 43-52.

³⁷⁶ ECtHR, Judgment of 26 March 1987, *Leander v. Sweden*, 9 EHRR 433.

to add personal data protection as a stand-alone right (cf. Article 8 of the Charter), or to include it within the Article on the right to privacy (Article 7 of the Charter).³⁷⁷ At the end of the day, however, the right to personal data protection was enshrined in a separate article. The author of this study believes that this choice was the most appropriate one, since, as further demonstrated below, the scope of the right to data protection sometimes goes beyond the scope of privacy, and conversely.³⁷⁸ In other words, even if the scope of these two rights sometimes overlap, none of them may be considered as fully *encompassing* the other. Treating data protection as being part of the broader right to privacy would have thus raised substantive issues from the perspective of the material scope of each right, which will be discussed in the following Chapter of this study.

One could argue that other sources might have been more relevant for justifying the inclusion of the right to personal data protection in the Charter, and in particular the constitutional tradition of the Member States. In 2007, indeed, some Member States had already enshrined rights in relation to the processing of personal data in their constitution.³⁷⁹ The Convention however failed to make use of this source (or at least, it was decided not to officially refer to it in the Explanation on Article 8). A possible reason is that only a few Member States had recognised the fundamental nature of data protection-related rights in their constitutions;³⁸⁰ the Convention might thus have feared to trigger a controversy on the applicable threshold for a right to be considered as being part of “*constitutional traditions common to the Member States*”.³⁸¹ Some questions were indeed difficult to answer. For example,

³⁷⁷ In January 2000, a first discussion draft of the Charter was submitted which presented data protection as an independent right. In February 2000, a second draft also included a separate article on data protection. In May 2000, a third draft also included a separate article on data protection but the comment accompanying the draft article provided that “*data protection is an aspect of privacy*”. In a fourth draft submitted end of May 2000, some Convention’s members suggested to delete the article on data protection and to incorporate a reference to data protection-related rights under the article on the right to privacy. In July 2000, an almost final draft was submitted which established a right to data protection under a separate article, i.e., Article 8 of the Charter. Source: Cover Note, Subject: Draft Charter of Fundamental Rights of the European Union, CHARTE 43/70/00 CONTRIB 233, Brussels, 15 June 2000; Note from the Praesidium, Subject: Draft Charter of Fundamental Rights of the European Union – Proposed Articles (Articles 10-19), CHARTE 4137/00 CONVENT 8 (OR.fr), Brussels, 24 February 2000; Draft Charter of Fundamental Rights of the European Union – New proposal for articles 1- 30, CHARTE 4284/00 CONCENT 28 (OR.fr), Brussels, 5 May 2000; Praesidium Note, Subject: Draft Charter of Fundamental Rights of the European Union – Amendments submitted by the members of the Convention regarding civil and political rights and citizens’ rights, CHARTE 4332/00 CONVENT 35, Brussels, 25 May 2000.

³⁷⁸ See next Chapter, Section 3.1 on the scope of the GDPR.

³⁷⁹ Besides Portugal, Austria and Spain, other Member States had recognised the constitutional significance of data protection-related rights, such as Germany (under the name ‘right to informational self-determination’ (*informationelle Selbstbestimmung*), the Netherlands (although as an aspect of the right to privacy), Finland (although under a constitutional section titled ‘the right to privacy’), Greece, Hungary, Slovakia, the Czech Republic, Lithuania, Poland and Estonia. See in this respect, González Fuster, G. (2014). *op. cit.*, pp. 174-183.

³⁸⁰ González Fuster, G. (2014). *op. cit.* ; McDermott, Y. (2017). *op cit*, p. 2.

³⁸¹ In the Explanations, the constitutional tradition of the Member States was only invoked as a source for the following EU fundamental rights: Article 10 (Freedom of thought, conscience and religion); Article 14 (Right to education); Article 17 (Right to property); Article 20 (Equality before the law); Article 37 (Environmental protection); Article 49 (Principles of legality and proportionality of criminal offences and penalties). Except for the right to environmental protection, all these other rights could be found in the vast majority or in all Member States’ constitution, and were therefore unlikely to trigger any controversy. As far as Article 37 is concerned (environmental protection), the Explanations carefully state that “*it also draws on the provisions of some national constitutions.*” [emphasis added].

how many Member States must have enshrined data protection in their constitution for the tradition to be considered as being “common”? When comparing data protection-related rights in various constitutions, what degree of similarity should these rights have in order to be considered as being part of the same constitutional tradition? Besides those questions, another reason which may explain the silence of the Convention in this respect is that, by referring to the general principles of EU law, the Convention had already indirectly included the constitutional traditions of Member States as a source. Hence, the Convention might have considered it unnecessary to directly and explicitly list the constitutional tradition of Member States as one of the sources justifying the recognition of the fundamental nature of the right to personal data protection.

Finally, it is worth stressing that, unlike most fundamental rights, the right to personal data protection had been given expression in EU secondary law *before* being elevated to the rank of primary law.³⁸² Traditionally, it is the prior recognition of a fundamental right in a higher treaty that triggers the development of secondary legislation aiming at ensuring the effective respect of that right.³⁸³ In the case of data protection, however, this process was reversed. Indeed, the 1995 Data protection Directive, which is also mentioned in the relevant sources in the Explanation on Article 8, had been adopted five years before the fundamental right to personal data protection was included in the Charter. Because of this Directive, many data protection-related rights had already been established, implemented and enforced at the national level, paving the way for a higher recognition. There is no doubt that the prior adoption of the 1995 Data Protection Directive partly contributed to the unveiling of the fundamental nature of the right to personal data protection.

All in all, the main criticism that can be levelled regarding the Explanation on Article 8 of the Charter is that none of the mentioned sources explicitly ascertain the fundamental nature of the right to data protection.³⁸⁴ The poorness of the Explanation on Article 8 calls for the conclusion that the EU has “*neither adequately justified the introduction of the right to data protection in the EU legal order nor explained its content*”.³⁸⁵ But the controversy around the sources of the fundamental right to data protection did not affect its recognition *per se*, nor the additional layer of functionality that it would confer to EU data protection law as a whole for the protection of EU fundamental rights, as further discussed in the following chapters of this study.

³⁸² Bonnici, J. (2014). Exploring the non-absolute nature of the right to data protection. *International Review of Law, Computers & Technology*, 28(2), p. 131.

³⁸³ *Ibid.*

³⁸⁴ McDermott, Y. (2017). *op. cit.*, p. 2.

³⁸⁵ Lynskey, O. (2014). Deconstructing Data Protection: The ‘Added-Value’ of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly*, 63(3):569-597. See also McDermott, Y. (2017). *op. cit.*, p. 2.

2.2.2.2. Unofficial reasons behind the inclusion of Article 8 in the Charter

To compensate for the poorness of the official explanations, scholars have elaborated different theories regarding the reason behind the recognition of a fundamental right to personal data protection by the EU. McDermott, for example, analyses data protection from the perspective of its underpinning values and argues that the inclusion of this right in the Charter was made possible because it already reflected some key values inherent in the European legal order, namely privacy, transparency, autonomy and non-discrimination,³⁸⁶ i.e., four values that were becoming increasingly important in a changing global order.³⁸⁷

Other scholars have approached the question from the perspective of EU institutional law and have found other potential reasons for the inclusion of the right to personal data protection in the Charter. One of them could be the inconsistencies in the level of protection of personal data across the three pillars of the EU. Prior to the adoption of the Charter, the Expert Group on Fundamental Rights had already pointed out that the 1995 Data Protection Directive applied to the first pillar of the EU (the European Communities, including the functioning of the internal market), but not to the other two pillars (the Common Foreign and Security Policy, and the Police and Judicial Cooperation in Criminal Matters).³⁸⁸ This created an imbalance that was difficult to justify given that fundamental rights ought to be equally protected among the three pillars, including in the context of the processing of personal data.

Another theory which may justify the inclusion of Article 8 in the Charter in the one of legitimacy, as developed by Paul De Hert and Serge Gutwirth; these authors have suggested that one of the main purposes behind this inclusion was to boost the legitimacy of EU secondary law in the field of data protection, and in particular the fundamental rights dimension of the 1995 Data Protection Directive.³⁸⁹ As previously stated indeed, this Directive had a double objective; one linked to the EU market (the IMO) and the other linked to the protection of fundamental rights (the FRO). In legal terms however, the adoption of the Directive rested on Article 100a of the TEC (now Article 115 TFEU), i.e., the functioning of the internal market.³⁹⁰ As a result, the EU lacked any express competence to regulate the processing of personal data for protecting fundamental rights. In 2000, the recognition of a fundamental right to personal data protection could have thus been envisaged as a mean to remedy the lack of legitimacy of the fundamental right dimension of the 1995 Data Protection

³⁸⁶ McDermott (2017), p. 5.

³⁸⁷ *Ibid.*, p. 5.

³⁸⁸ See above, Chapter 2.

³⁸⁹ De Hert, P. & Gutwirth, S. (2009). *op. cit.*, pp. 8-9.

³⁹⁰ Art 115 TFEU: “Without prejudice to Article 114, the Council shall, acting unanimously in accordance with a special legislative procedure and after consulting the European Parliament and the Economic and Social Committee, issue directives for the approximation of such laws, regulations or administrative provisions of the Member States as directly affect the establishment or functioning of the internal market.”

Directive.³⁹¹ This reasoning, however, is undermined by the fact that the 1995 Data Protection Directive did not aim at protecting the fundamental right to personal data protection, but aimed at protecting fundamental rights *in general*, and the right to privacy *in particular*. The protection of fundamental rights in general, and the right to privacy in particular, had already been recognised as forming an integral part of the general principles of EU law. The alleged lack of legitimacy of the Directive in this respect is thus questionable. Furthermore, from an institutional law perspective, the legal basis used for adopting a directive does not restrict per se the scope its objectives. In other words, the fact that Article 100a of the TEC had been chosen as the legal basis for the 1995 Data Protection Directive did not mean that the objectives of this Directive should have been limited and directed towards the functioning of the internal market. Although the author of this study here argues that the recognition of a fundamental right to personal data protection was not strictly necessary from an institutional law perspective, there is however no doubt that it has helped consolidating the legitimacy of the EU's actions in the field of data protection law. This alone may have played in favour of the recognition of such a fundamental right at the EU level.

From the perspective of effective protection, other scholars have suggested that the right to personal data protection might have been included because it was necessary to protect individuals against unlawful or abusive processing practices that neither fell within the scope of the fundamental right to privacy, nor within the scope of the 1995 Data Protection Directive. Indeed, both the right to privacy and the Directive suffered from limitations; the 1995 Data Protective Directive did not apply, for instance, to processing operation relating to Member States' security matters or to the activities of Member States in areas of criminal law.³⁹² The right to privacy, for its part, did not apply to all types of processing of personal data, but only to processing activities that would interfere with the private life of the individuals concerned. These limitations thus created legislative gaps, which could leave some data subjects helpless against abusive data processing practices. The inclusion of a fundamental right to personal data protection in the Charter might as well have been seen as a way to bridge those gaps. In particular, it could give individuals more control over their personal data, regardless of whether their right privacy had been violated, or whether the processing activity at stake was falling outside the scope of the 1995 Data Protection Directive. In other words, the *opportunity* and *necessity* to fill these legislative gaps might have been a driving force in the decision to include a right to personal data protection in the Charter.

Similarly, Lynskey explains the inclusion of Article 8 from the perspective of the added value of the right to data protection compared to the right to privacy, both in scope and content.³⁹³ Data protection-related rights, such as the right to information,

³⁹¹ De Hert, P. & Gutwirth, S. (2009), *op. cit.*, pp. 8-9.

³⁹² Article 3(2) of the 1995 Data Protection Directive.

³⁹³ Lynskey, O. (2014). *op. cit.*

the right to access or the right to erasure of personal data, were already enshrined in the 1995 Data Protection Directive, and provided individuals with different prerogatives than the right to privacy. Overall, data protection gave individuals “*more rights over more types of data than the right to privacy*”.³⁹⁴ The added value of personal data protection could thus be one of the reasons for its inclusion in the Charter as a self-standing fundamental right. It is also relevant to note in this respect that various members of the Convention or Praesidium were important figures who had been previously involved in the drafting of data protection legislative texts at the national, international and EU level, and who were therefore well acquainted with the similarities but also the divergences between the right to privacy and the right to data protection.³⁹⁵ In line with Lynskey’s theory, the author of this study thus agrees that the differing material scope of the right to privacy and of the right to personal data protection is probably one of the key elements having led the Convention to decide to split them in two different articles.

Finally, in the opinion of the author, another potential reason for the inclusion of data protection as a self-standing fundamental right could lie in the desire of the EU to shine and gain more normative power in the field of fundamental rights. Since its creation, the EU has built a strong narrative around fundamental rights protection, which allowed it to gain global influence³⁹⁶ and further enhance its own mandate in that field.³⁹⁷ Since the proclamation of the Charter, the EU has proven particularly active in the defence and promotion of fundamental rights, both at home and abroad,³⁹⁸ thereby exercising and expanding its normative power in the field.³⁹⁹ The drafters of the Charter were certainly aware that enshrining innovative rights, such as the right to personal data protection, would send a clear message to the world, according to which the EU was not only committed to promoting *traditional* fundamental rights but also *innovative* fundamental rights.

2.2.3. Wording, content and scope of the fundamental right to personal data protection

³⁹⁴ *Ibid.*

³⁹⁵ González Fuster, G. (2014). *op. cit.*, pp. 194-195. González Fuster cites in particular (i) the Chair of the Convention, Roman Herzog, former President of the Federal Republic of Germany and of the Federal Constitutional Court of Germany; (ii) Guy Braibant, who had indirect influence on the 1978 French law on *informatique et libertés*, and who had prepared a report for the French government on the draft 1995 Data Protection Directive; (iii) Jordi Solé Tura, who had participated in the discussions over the data protection provision of the 1978 Spanish Constitution; (iv) Stefano Rodotà who had been a member of the Expert Group to draft the OECD Privacy Guidelines and who was at the time Chairman of the Italian data protection authority and member of the Article 29 Working Party.

³⁹⁶ Nicolaidis, K. & Howse, R. (2002). 'This is my EUtopia ...': Narrative as power. *Journal of Common Market Studies*. 40(4): 767-792.

³⁹⁷ Muir, E. (2014). Fundamental Rights: An Unsettling EU Competence. *Human Rights Review*, 15(1):25-37.

³⁹⁸ Wetzel, J. R. (2003). Improving fundamental rights protection in the European union: Resolving the conflict and confusion between the Luxembourg and Strasbourg courts. *Fordham Law Review*, 71(6):2823-2862; European Union Agency for Fundamental Rights (2014). *An EU internal strategic framework for fundamental rights: Joining forces to achieve better results*. Luxembourg: Publications Office.

³⁹⁹ Manners, I. (2000). *Normative Power Europe: A Contradiction in Terms?* Copenhagen Peace Research Institute, p. 44.

Still today, the EU is the only supra-national organization where personal data protection is considered as a stand-alone fundamental right in a binding treaty. This section will therefore be dedicated to understanding what this right actually entails by looking at its wording, scope and content.

2.2.3.1. Analysis of the Wording of Article 8 of the Charter

Article 8 of the Charter, conspicuously titled “*Protection of personal data*”, is composed of three paragraphs that read as follows:

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

Article 8 of the Charter may be read as a *binary* or as a *unitary* provision.⁴⁰⁰ According to the binary reading theory, the first paragraph would establish a general rule according to which it would be prohibited to process personal data, whereas the second and third paragraphs would provide for derogations under specific conditions.⁴⁰¹ By contrast, according to the unitary reading theory, the first paragraph of Article 8 of the Charter would not proscribe the processing of personal data *per se*, but would allow it as long as the individuals concerned enjoy a certain level of protection in this respect. The second and third paragraphs would then simply provide details with respect to the applicable level of protection. This unitary reading, rather than introducing a restrictive conception of the right to personal data, reflects a *permissive* conception (i.e., “*processing of personal data is allowed, as long as ...*”).⁴⁰² Taking into account the wording and structure of Article 8 of the Charter, as well as EU secondary legislation in the field of data protection, the author believes that this unitary reading (or permissive conception) is the most accurate. Indeed, Article 8 of the Charter does not prohibit the processing of personal data but rather indicates that individuals ought to be protected in this respect. Similarly, secondary legislation in the field of data protection does not prohibit data processing activities but rather establishes a set of rules that controllers and processors are supposed to respect when processing personal data. What remains unclear, however, is the extent of such a protection. Indeed, the Explanations to the Charter

⁴⁰⁰ González Fuster, G. & Gutwirth, S. (2013). *op. cit.*, p. 533.

⁴⁰¹ *Ibid.*, p. 532.

⁴⁰² *Ibid.* p. 533.

do not provide any clear indications with respect to the actual scope or specific content of the fundamental right to personal data protection. The below sub-section will attempt at clarifying such scope and content on the basis of a textual and functional approach.

2.2.3.2. Analysis of the content of Article 8 of the Charter

Regarding the actual content of Article 8 of the Charter, the expression ‘protection of personal data’ in the first paragraph is unspecified and can thus be understood in its literal or broader sense. A literal approach suggests that the *data* themselves ought to be protected. The term ‘protection’ would then relate to the measures that ought to be implemented to ensure the security of the personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.⁴⁰³ Data protection in the sense of data security would thus mainly be concerned with the integrity and confidentiality of the personal data. Such integrity and confidentiality obligation would require controllers and processors to keep personal data safe, for example by making sure that the servers on which they are stored are password-protected, by encrypting sensitive data, by having a back-up of all data, by limiting the number of persons who can read the data in clear, and so on.

In its broader sense, however, the expression ‘protection of personal data’ can be understood as conferring on individuals the right to exercise control over the processing of their personal data. The expression ‘data protection’ would then refer to the entire set of principles, rights and obligations that protect individuals against unlawful or intrusive practices involving the processing of their personal data. This would include, for example, the right for data subject to be informed about the existence and purposes of any processing activity involving their personal data, or to right to object to the processing of their personal data.⁴⁰⁴ The right to be informed and the right to object are not concerned with the security of personal data *per se*, but rather participate to the overall empowerment of data subjects, and thus to the protection of the natural persons to whom these data relate. Because of the aim of EU data protection law as reflected in both EU primary and secondary law, the author of this study believes that this first paragraph should be understood in its broader sense. In other words, the statement that “[e]veryone has the right to the protection of personal data concerning him or her” would refer to the set of rights, principles and obligations laid down in EU secondary law which participate to the protection of the individuals whose personal data are being processed. This would also indirectly include the obligation to guarantee the security of the personal data, as laid down in Article 5(1)(f) and 32 GDPR.

⁴⁰³ The security of personal data is guaranteed by Article 32-34 of the GDPR. The obligation to protect personal data against data breaches can be found in article 32(2) of the GDPR on the security of processing.

⁴⁰⁴ The right to information regarding the processing of personal data is now detailed in articles 12 to 14 of the GDPR.

The second paragraph of Article 8 of the Charter is more specific, as it details what appears to be three important (sub-)principles and two important (sub-)rights of the fundamental right to personal data protection.⁴⁰⁵ The three principles detailed in the second paragraph of Article 8 can be identified as (i) the fairness principle, (ii) the purpose limitation principle and (iii) the lawfulness principle. More specifically, it is stated that personal data may only be processed “fairly” and “for specified purposes”. The expression “specified purposes” entails that controllers or processors cannot process personal data at random but must be able to identify one or several determined purposes that they aim to achieve by processing the personal data. The third principle is that personal data may only be processed on a “legitimate basis laid down by law”. Today, this obligation for controllers and processors to have a legitimate legal basis for processing personal data is further detailed in Article 6, 9 and 10 of the GDPR (depending on whether the personal data are sensitive or not). Two important (sub-)rights in relation to data protection are further detailed in the second paragraph of Article 8: (i) the right to have access to one’s own personal data, and (ii) the right to request rectification of the personal data. These rights can also be found in Article 15 and 16 GDPR.

Finally, the third paragraph of Article 8 touches upon *enforcement*. It provides that compliance with data protection rules must be subject to control by an independent authority. At the EU level, the independent authority in charge of ensuring that EU institutions and bodies comply with EU data protection law is the European Data Protection Supervisor (‘EDPS’). At the Member States’ level, the 1995 Data Protection Directive already requested each Member State to establish and give specific competences and powers to a national DPA.⁴⁰⁶ The third paragraph of Article 8 of the Charter thus refers to the independence of these authorities.

Content-wise, Article 8 of the Charter therefore includes a small selection of data protection principles, rights and obligations that had already been laid down in the 1995 Data Protection Directive. Because of this correlation, Article 8 of the Charter can be considered as establishing a clear link between EU primary and secondary law in the field of data protection. Yet, the succinctness of Article 8 of the Charter also triggered debates as to the reason why these particular principles, rights and obligations had been selected. Indeed, next to the rights and principles explicitly mentioned in Article 8 of the Charter, other specific data protection principles, rights and obligations – which appear equally important – can be found in EU secondary law, such as the principle of data minimisation,⁴⁰⁷ the right to information of data

⁴⁰⁵ Secondary law reveals that the fundamental right to personal data protection is actually composed of a multitude of rights provided to individuals with respect to the processing of personal data (right to information, right to access the personal data, right to object to the processing, right to erasure, right to data portability, etc). The fundamental right to data protection is thus composed of a patchwork of ‘sub-rights’. The expression ‘sub-right’ does not mean such rights are less important. Rather, it is intended by the author to reflect the structural composition of the fundamental right to personal data protection.

⁴⁰⁶ Article 28 of the 1995 Data Protection Directive.

⁴⁰⁷ Article 6(1)(c) of the 1995 Data protection Directive and Article 5(1)(c) of the GDPR.

subjects,⁴⁰⁸ or the obligation for controllers to ensure an adequate level of protection in case of data transfers outside of the EU.⁴⁰⁹ For some reasons, these other principles rights and obligations have been left out from the wording of Article 8 of the Charter. Unfortunately, the Explanations relating to the Charter⁴¹⁰ do not shed any light on this particular point.⁴¹¹

In view of this selection, one may wonder whether the intention of the drafters of the Charter was to operate a distinction between the fundamental substance and essence of data protection, and its peripheral (less fundamental) substance. In other words, one may wonder if the rights, principles or obligations that were omitted from the wording of Article 8 of the Charter are 'less fundamental' than those which have been expressly enshrined in it. From a functional point of view, however, a closer analysis of the substance of EU data protection law reveals that each of these principles, rights and obligations are interdependent.⁴¹² The right to information, for example, is a prerequisite for data subjects to be aware that their personal data are being processed, and to be able to request access to or receive a copy of such data. Because of this interdependence, it would be odd to claim that the right to access is part of the fundamental substance of EU data protection law, but that the right to information is not, solely based on the wording of Article 8 of the Charter. Furthermore, the case-law of the CJEU shows that Article 8 of the Charter has been invoked in order to justify the existence and/or guarantee the respect of data-related rights that are not explicitly mentioned within that Article, such as the right to be forgotten⁴¹³ or the right not to be subject to a transfer of personal data towards a territory where the level of data protection is not equivalent.⁴¹⁴ Moreover, the CJEU has (quite controversially)⁴¹⁵ already declared that a law allowing public authorities to generally gain knowledge of the *content* of electronic communications,⁴¹⁶ or a law that would fail to put providers of electronic communications services or networks under the obligation to ensure the security of personal data through organizational and technical measures,⁴¹⁷ would violate the essential core of Article 8 of the Charter. By saying so, and regardless of the criticism expressed towards this case-law, the CJEU has thus included the principle of data

⁴⁰⁸ Article 14 of the 1995 Data protection Directive and Article 21 of the GDPR.

⁴⁰⁹ Articles 25-26 of the 1995 Data protection Directive and Articles 45-49 of the GDPR.

⁴¹⁰ Explanations relating to the Charter of Fundamental Rights, *OJ C 303, 14.12.2007, p. 17–35*. *Prior versions of the Explanations have been published on the website of the Convention. However, these preceding versions do not provide any additional element of explanation with respect to Article 8, in comparison to the final Explanations. This is the reason why only the final published Explanation on Article 8 will be analysed in this study.*

⁴¹¹ See Explanation on Article 8. Explanations relating to the Charter of Fundamental Rights, *OJ C 303, 14.12.2007, p. 17–35*.

⁴¹² See Section 3.2.4, below.

⁴¹³ *Google Spain*.

⁴¹⁴ CJEU, Judgment of 6 October 2015, *Schrems I*, Case C-362/14 ; and Judgment of 16 July 2020, *Schrems II*, C-311/218

⁴¹⁵ Brkan, M. (2019b). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 20(6):864-883, p. 878; Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford University Press, p. 172.

⁴¹⁶ *Digital Rights Ireland*, pt. 39.

⁴¹⁷ CJEU, *Digital Rights Ireland*, para. 40.

security within the ‘essential core’ of Article 8 of the Charter, although the latter does not expressly mention such a principle. This tends to confirm that a literal reading of Article 8 of the Charter does not suffice to determine its content. In the opinion of the author, each data protection-related right that has been enshrined in secondary legislation should thus be considered as forming a piece of the content of Article 8 of the Charter. In the end, the reason why some pieces may have been left out from the wording of this Article could simply be a matter of layout. Like in any other important human rights treaty, each Article of the Charter is indeed concise (on average one or two paragraphs).⁴¹⁸ If Article 8 of the Charter had explicitly mentioned all the existing data protection-related principles, rights or obligations already recognised in EU secondary law, it would have been inconveniently lengthy.

In conclusion, the content of the fundamental right to personal data protection (both in terms of substance and essential core) is in any case not limited by the wording of Article 8 of the Charter but must be interpreted in light of the case-law of the CJEU as well as EU secondary law in the field of data protection. This important finding will serve as a basis for making recommendations on how to potentially enhance the multi-functionality of EU data protection law by relying on Article 8 of the Charter.

2.2.3.3. Analysis of the scope of Article 8 of the Charter and of its overlap with the right to privacy

It seems impossible to discuss the scope of Article 8 of the Charter without considering at the same time the scope of Article 7 of the Charter, given the strong historical, legal and jurisprudential connection that they share, as well as the many academic debates – and sometimes confusion – that their respective scope have induced. In the decade following the proclamation of the Charter indeed, the CJEU has often referred to Article 7 and Article 8 of the Charter as guaranteeing a “*right to respect for private life with regard to the processing of personal data*”.⁴¹⁹ By adopting this peculiar wording, the CJEU seems to have crossbred Article 7 and Article 8 of the Charter into a sort of “*hybrid species*”.⁴²⁰ As a matter of facts, the first time that the CJEU *exclusively* considered the fundamental right to personal data protection without melding it with the right to privacy was in its judgment of 5 May 2011 in the *Deutsche Telekom* case.⁴²¹ This ‘trend’ of the CJEU to almost always ‘couple’ Article 7 and Article 8 of the Charter to interpret EU data protection rules has quite logically led many scholars to question whether the right to personal data protection should

⁴¹⁸ Article 41 of the Charter on the Right to good administration is the longest Article with four paragraphs.

⁴¹⁹ See, among others, CJEU judgments *Volker und Markus Schecke and Eifert*, para. 52; *ASNEF and FECEMD*, para. 42; *Schwarz*, para. 26.

⁴²⁰ Lynskey O. (2014). *op. cit.*, p. 580.

⁴²¹ CJEU, Judgment of 5 May 2011, *Deutsche Telekom AG v Bundesrepublik Deutschland*, Case C-543/09.

really be considered as a self-standing fundamental right, or rather as an offspring or subset of the right to privacy.⁴²²

In order to be able to understand this jurisprudential trend, it is however first necessary to recall three important elements pertaining to the pre- and peri-Lisbon era, as well as to the pre- and peri-GDPR eras, which have without any doubt participated to the merging or conflating of Article 7 and of 8 of the Charter by the CJEU:

- First, with respect to the pre-Lisbon era, it must be recalled that the Charter had neither a clear legal status nor any binding force. For almost nine consecutive years (7 December 2000 – 1 December 2009), the text of the Charter had been proclaimed, but no constitutional reform had allowed to clarify its legal status. During that period, the Charter was thus stuck “*in a sort of legal limbo*”.⁴²³ Of course, saying that the Charter did not have any influence during that period would be exaggerated.⁴²⁴ As a matter of facts, as from 2001, newly adopted EU legislative acts started referring to the Charter and to the rights that it contained in anticipation of its application.⁴²⁵ Also during that period, the CJEU started referring to the Charter in its judgments. However, since the Charter had no legally binding force, the CJEU could not exclusively articulate its reasoning or base its decisions on the rights that the Charter contained. As a consequence, the CJEU had no other choice than to continue relying on other sources of human rights law for interpreting EU law in light of these rights, and in particular on the ECHR. As already mentioned above however, the ECHR, while explicitly consecrating the right to privacy, did not (and still does not) contain any explicit reference to a right to personal data protection. This logically explains why, in the pre-Lisbon era, the CJEU was reluctant to rely on the right to personal data protection alone when interpreting EU data protection law. Hence, in the decade following the adoption of the Charter, the CJEU often relied on the right to privacy *in lieu of* the right to personal data protection, or sometimes *combined* both rights as if they were forming an inseparable pair.

⁴²² González Fuster, G. (2014). *op. cit.*, p. 214 ; Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), p. 222 ; Hondius, F. W. (1980), *op. cit.*; Benyekhlef, K. (1993). *La protection de la vie privée dans les échanges internationaux d'informations*. Montréal, Thémis; Balz, S. D. & Hance, O. (1996). Privacy and the internet: Intrusion, surveillance and personal data. *International Review of Law, Computers & Technology*, 10(2):219-234.

⁴²³ González Fuster, G. & Gellert, R. (2012). The fundamental right of data protection in the European Union: In search of an uncharted right. *International Review of Law, Computers & Technology*, 26(1):74.

⁴²⁴ Nicolaou, G. (2013). The Strasbourg View on the Charter of Fundamental Rights. *Research papers in law 3/2013. College of Europe*. https://www.coleurope.eu/sites/default/files/research-paper/researchpaper_3_2013_nicolaou_lawpol_final_0.pdf

⁴²⁵ In the field of data protection, for example, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) directly referred to Articles 7 and 8 of the Charter (Recital 2). González Fuster observes that “*the mention of the Charter of its Article 8 represented a key innovation of the fundamental rights framing of the instrument, compared to its predecessors (Directive 97/56/EC) (...)*.” See González Fuster (2014), *op. cit.*, p. 217.

- Second, with respect to the Lisbon era (i.e., the period after the adoption of the Lisbon Treaty), it must be recalled that, even after the Charter had acquired its binding force in December 2009, a certain ‘legal dichotomy’ persisted between EU *primary* and *secondary* law in the field of data protection until the adoption of the GDPR in May 2016. Indeed, while EU secondary law (notably, the 1995 Data Protection Directive) had as an explicit objective to ensure the respect of the right to privacy of natural persons and did not mention the existence of a fundamental right to personal data protection, the Charter had enshrined both rights separately. Hence, in the period from December 2009 to May 2018, most of the preliminary references which were submitted to the CJEU on the interpretation to be given to EU secondary law in the field of data protection were still ‘privacy-oriented’, in the sense that they either explicitly referred to the right to privacy or were articulated around the idea that the objective of these rules was to ensure the respect of the right to privacy. Keeping this legal dichotomy in mind, one can better understand why the CJEU continued answering these questions in light of Article 7 of the Charter, or in light of a combination of Article 7 and 8 of the Charter. In other words, the lack of recognition of a fundamental right to personal data protection in EU secondary law until 2018 can explain the persistence of the jurisprudential trend of the CJEU to merge Article 7 and Article 8 of the Charter in the pre-GDPR era.
- As from 2018, one may have expected this curious jurisprudential trend to stop or at least to slowly disappear since the adoption of the GDPR spelled the end of the legal dichotomy between EU primary and secondary law in the field of data protection. The 1995 Data Protection Directive was indeed repealed and replaced by the GDPR in May 2018,⁴²⁶ and the fundamental rights objective of EU secondary law was thereby updated. In particular, instead of referring to the need of ensuring the respect of the right to *privacy* of the data subject, the GDPR explicitly referred – and still refers today – to the need of ensuring the respect of the fundamental right to personal data protection.⁴²⁷ Despite this change however, an analysis of the first ten judgments rendered by the CJEU after May 2018 reveal that Article 8 of the Charter is still often envisaged together with Article 7, as if data protection was a mere subset of privacy.⁴²⁸ This persistent trend can once again be explained by the fact that, in all these cases, the questions referred to the CJEU still concerned the interpretation to be given to the 1995 Data Protection Directive (and not the GDPR) because the facts of these cases had

⁴²⁶ Article 94(1) of the GDPR.

⁴²⁷ Article 2(2) of the GDPR is worded as follows: “*This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*” (emphasis added).

⁴²⁸ See Table under Section 2.3.4.1, below.

taken place before 2018. Furthermore, in accordance with its established jurisprudential practice, the CJEU formulated each decision by referring to its own prior case-law. In the 2019 cases *Google* and *GC and Others* for example (on the right to de-referencing in search engines), the CJEU repeated almost word for word its findings in the 2014 *Google Spain* judgment,⁴²⁹ where it had systematically coupled Articles 7 and 8 of the Charter together.

- Finally, it must also be acknowledged that a majority of the cases that are brought before the CJEU are based on a dispute where both the right to privacy *and* of personal data protection are suspected to have been violated; it is thus quite logical that referring courts sometimes formulate their preliminary questions to the CJEU in light of both rights. Taking these elements into account, the tendency of the CJEU to couple Article 7 and Article 8 of the Charter when interpreting EU data protection legislation is likely to continue way beyond May 2018.

As already mentioned above, the “*coupling*”⁴³⁰ or “*conflating*”⁴³¹ of Articles 7 and 8 of the Charter has been extensively discussed and has caused a lot of ink to flow in the academia and among practitioners with respect to the scope and content of each right.⁴³² Today, a vast majority of scholars advocate for a distinction between the scope of the fundamental right to privacy on the one side, and the scope of the fundamental right to personal data protection on the other side, as two autonomous rights.⁴³³ Yet, a vast majority of scholars also recognize that both rights are closely related, and that they partly overlap.⁴³⁴ Stating that the CJEU *systematically* conflates Article 7 and Article 8 of the Charter in the context of the interpretation or application of EU data protection law would however be false. In several cases indeed, the CJEU has also participated to the emancipation of Article 8 of the Charter by interpreting EU data protection law in light of that Article, either *exclusively*, or at least *separately* from Article 7 (for an overview, see below, section 2.3.4.1).

On the basis of a literal approach, it can no longer be debated that the right to privacy and the right to personal data protection are formally recognised as two separate fundamental rights under the Charter, since they each have their own Article.⁴³⁵ On the basis of a functional approach, however, it cannot be denied that they are closely related, mainly because they are both rooted in the notion of human

⁴²⁹ CJEU, Judgment of 13 May 2014, *Google Spain*, Case C-131/12.

⁴³⁰ González Fuster (2014). *op. cit.*, pp. 258.

⁴³¹ Lynskey, O. (2014). *op. cit.*, p. 580.

⁴³² See, among others: Docksey, C. (2016). *Four fundamental rights: finding the balance. International Data Privacy Law*, 6(3):195–209; González Fuster, G. & Gellert, R. (2012). *op. cit.*; Kokott, J., & Sobotta, C. (2013). *op. cit.*; Lynskey, O. (2014). *op. cit.*; Bonnici, J. (2014). *op. cit.*; González Fuster (2014), *op. cit.*, pp. 213–248; González Fuster, G. & Gutwirth, S. (2013). *op. cit.*, p. 533.

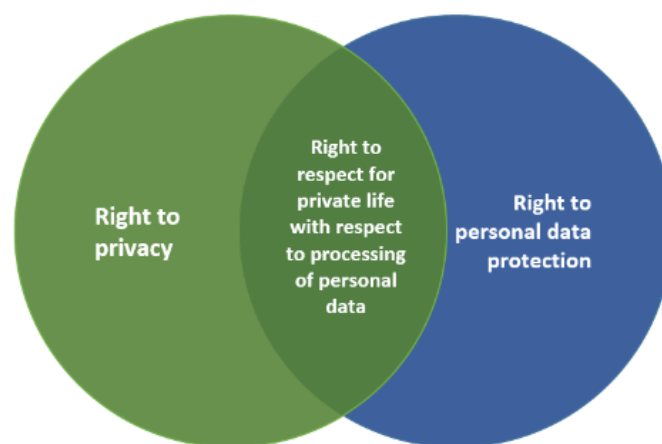
⁴³³ *Ibid.*

⁴³⁴ *Ibid.*

⁴³⁵ In the sense that they have formally been enshrined in two separate articles. Depending on the approach taken (formal, functional or comparative (Charter/ECHR)), some may still argue that they are not separate rights.

dignity and informational freedom.⁴³⁶ In the opinion of the author, the fact that these rights are closely related and that their scopes sometimes overlap do not annihilate their autonomy. As a matter of facts, all fundamental rights are somehow connected to the notion of human dignity and may thus overlap.⁴³⁷ Hence, the author of this study considers that it would be incorrect to state that the CJEU has created a new hybrid fundamental right out of two existing rights.⁴³⁸ Rather, the references to Article 7 and Article 8 as a '*right to privacy with respect to personal data processing*' should be understood as references to situations where both rights have been infringed by the same act or omission and can therefore be invoked together.

THE RIGHT TO PRIVACY AND THE RIGHT TO PERSONAL DATA PROTECTION
UNDER THE EU CHARTER



Taking the above reflections into account, and with a view of further shedding light on the respective scope of Article 7 and 8 of the Charter, a distinction can thus be drawn between three potential types of limitation or interference with the right to privacy and/or personal data protection:

- 1) Interference with Article 7 of the Charter alone: for the fundamental right to privacy to be invoked solely, the infringement at stake must impede the right to private and family life of an individual without involving the processing of personal data.

E.g., adoption of a law by a Member State depriving a parent from equally establishing a close relation with his/her child, thereby impeding his/her right

⁴³⁶ It can be argued indeed that the 'right to be alone', the 'right to create relations with others', and the 'right to informational self-determination' share the same essence: the possibility for human beings to develop, determine and disclose (or decide not to disclose) who they are vis-à-vis the external world.

⁴³⁷ Gonzalez Fuster, G. & Hijmans, H. (2019). The EU Rights to Privacy and Data Protection: 20 years in 10 questions. *Privacy Hub Working Papers*. Web version.

⁴³⁸ The wording employed by the CJEU echoes the expression enshrined in Article 1(1) of the 1995 Data Protection Directive itself, whose object is the protection of "*the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*" (emphasis added).

to a private and family life;⁴³⁹ adoption of a law by a Member State allowing surveillance and use of intimidation by police force on the basis of infiltration and shadowing processes, but without involving any type of personal data processing.⁴⁴⁰

- 2) Interference with Article 7 *and* 8 of the Charter: for both rights to be invoked, the infringement at stake must involve the unlawful or illegitimate processing of personal data by the infringer, while impeding the right to private and family life of the individual concerned.

E.g., a dispute relating to the transfer of personal data from a company located in the EU to a company located in the US, the latter being subject to intrusive US surveillance laws;⁴⁴¹ the collection of (sensitive) personal data, without the knowledge of the data subjects, by a religious association over existing or potential new members;⁴⁴² etc.

- 3) Interference with Article 8 of the Charter alone: this would imply a case where the fundamental right to personal data protection would have suffered from an infringement, without causing any interference with the right to privacy. In other words, the infringement would not affect the right to respect for private or family life, but solely the right to personal data protection. It would then be enough for the judges to analyse the facts of the case and the applicable law in light of Article 8 of the Charter, without relying in parallel on Article 7 of the Charter.⁴⁴³

E.g., a dispute arising from the fact that a Member State relies on algorithmic decision-making for fraud detection in the field of taxation, without having conducted a data protection impact assessment beforehand; a dispute arising from the lack of independence of the data protection authority of a given Member State in light of Article 8(3) of the Charter.⁴⁴⁴

In the opinion of the author of this study, the partial overlap between the scope of Article 7 and Article 8 of the Charter should not annihilate their autonomy and should not prevent the CJEU from fully interpreting and exploiting the scope of each fundamental right individually. As further discussed in the third Chapter of this study, however, one risk exists in this respect: the *dilution* of the scope of the right to personal data protection within the scope of the right to privacy. If such a dilution would take place, Article 8 of the Charter would no longer be a stand-alone right but

⁴³⁹ See, for example, ECtHR, Judgment of 13 June 1979, *Marckx v. Belgium*.

⁴⁴⁰ By analogy to ECtHR, *Ilaşcu and Others v. Moldova and Russia* [GC], para. 481.

⁴⁴¹ See, for example, CJEU, Judgment of 6 October 2015, *Schrems I*, Case C-362/14.

⁴⁴² See, for example, CJEU, Judgment of 10 July 2018, *Jehovan todistajat*, Case C-25/17.

⁴⁴³ See, for example, CJEU, Judgment of 5 May 2011, *Deutsche Telekom*, and Judgment of 5 June 2018, *Wirtschaftsakademie*, where the reasoning of the Court is based solely on Article 8 of the Charter.

⁴⁴⁴ This question was for example debated in *Wirtschaftsakademie* (see paras. 68 and 74) and in *Schrems II* (see paras. 106-121).

could only be applied in combination with the right to privacy. This, in turn, would limit the circumstances in which data subjects could rely on Article 8 of the Charter to seek the respect of their right to personal data protection. In the opinion of the author, preserving the respective scope of Article 7 and Article 8 of the Charter is therefore important to preserve the multi-functional nature of EU data protection law with respect to its FRO, as further outlined in the third Chapter of this study.

2.2.4. Preliminary conclusion: the recognition of a fundamental right to personal data protection triggered a shift within the FRO of EU data protection law

The above sections have shown that the unveiling of the fundamental nature of the right to personal data protection is the result of interactions between the growing body of EU fundamental rights on the one side, and of the body of EU data protection law on the other side. In particular, the above sections have explored both the official and unofficial reasons that may explain the inclusion of personal data protection as a fundamental right in the Charter.

When the Charter was proclaimed in 2000, the significance and impact of the fundamental right to personal data protection did not immediately materialize for Member States, controllers, processors or data subjects, mainly because the Charter itself did not have any clear legal value.⁴⁴⁵ In the end, it took an extra nine years for the Charter to become legally binding and for Article 8 to start having direct effect.⁴⁴⁶ Yet, it cannot be denied that the inclusion of a right to personal data protection in the Charter triggered a shift. Progressively, EU secondary law in the field of data protection was repositioned from being a set of rules primarily at the service of the right to privacy, to a set of rules at the service of the fundamental rights of natural persons, and of their right to personal data protection in particular.⁴⁴⁷ Today, Article 1(2) of the GDPR expressly states that “[t]his Regulation protects fundamental rights and freedoms of natural persons **and in particular their right to the protection of personal data**” (emphasis added).

In the context of this study, the most relevant outcome of the recognition of a fundamental right to personal data protection in the Charter is the shift it triggered for the FRO of EU data protection law itself. The below section will more specifically show how this shift was progressively reflected and materialised within the case-law of the CJEU, before being textualized in 2016, when the GDPR repealed and replaced the 1995 Data Protection Directive.

⁴⁴⁵ The Charter was first proclaimed during the European Council meeting in Nice on 7 December 2000. However, it only became binding with the entry into force of the Lisbon Treaty in 2009. On this topic, see the background note of the European Parliament. *EU Charter of Fundamental Rights – Proclamation at Parliament in Strasbourg 12 December 2007*. REF.: 20071127BKG13869.

⁴⁴⁶ Article 6(1) TEU, as amended by the Lisbon Treaty, gives legally binding force to the Charter.

⁴⁴⁷ This shift was however officially textualized only 16 years later, with the adoption of the GDPR.



This December 2002 advertising for the new iMac shows how computers started being branded not only as professional tools, but also as tools for leisure and personal activities, such as photographing.

2.3. OVERVIEW ON THE FULFILMENT OF THE FUNDAMENTAL RIGHTS OBJECTIVE OF EU DATA PROTECTION LAW

In the below section, the author will review and analyse the case-law of the CJEU in the field of data protection with a view of determining whether EU data protection law has been interpreted to the benefit of the right to privacy and/or personal data protection (cf. primary functionality), as well as to the benefit of any other fundamental right or freedom enshrined in the Charter (cf. secondary functionality). For the sake of clarity and with a view of better understanding some jurisprudential trends, a distinction will be operated between the case law of the CJEU in the pre-Lisbon era (Section 2.3.1), in the Lisbon era (Section 2.3.2), and in the GDPR era, respectively (Section 2.3.3). Through this review of the relevant EU case-law, the author will generally assess the overall fulfilment of the FRO of EU data protection law. In a closing section, the author will then discuss whether the FRO of EU data protection law would not be currently facing a shortfall and discuss the potential causes behind that phenomenon (Section 2.3.4).

2.3.1. Pre-Lisbon era: interpretation of EU data protection law mainly for the benefit of the right to privacy

When personal data protection was enshrined in Article 8 of the Charter, one could have expected it to become a focal point of the interpretation and application of EU data protection law by the CJEU. For almost an extra decade, however, the fundamental right to personal data protection lingered in the shadow of the right to privacy. This is reflected in particular in the early case-law of the CJEU since, as further detailed below, the EU judges either disregarded Article 8 of the Charter

(*Rundfunk*⁴⁴⁸, *Lindqvist*⁴⁴⁹ and *Satamedia*⁴⁵⁰) or just mentioned it in a cosmetic way (*Bavarian Lager*,⁴⁵¹ *Promusicae*⁴⁵²).

From the outset, it must be noted that the lack of explicit reference to Article 8 of the Charter can be easily explained by two elements pertaining to the legislative landscape of that period (i.e., 2000 – 2009). As already mentioned above indeed, during that period, the preliminary questions submitted by national courts to the CJEU concerned the interpretation to be given to legislation that was adopted *prior* to the inclusion of the fundamental right to personal data protection in the Charter (such as the 1995 Data protection Directive or the e-Privacy Directive). As we already know, such legislation did not include any reference to the fundamental right to personal data protection but was instead putting emphasis on the importance to protect the fundamental right to privacy in the context of data processing.⁴⁵³ When interpreting these directives, the CJEU was therefore bound by this conception. Moreover, until December 2009, the Charter did not have any certain legal value. As a consequence, from the perspective of legal legitimacy, the CJEU could hardly rely on the fundamental right to personal data protection as enshrined in Article 8 of the Charter. Instead, it was safer to invoke the well-established right to privacy which had been enshrined in the ECHR since 1950 already, and whose protection was also guaranteed as part of the general principles of EU law. In other words, the fundamental right to privacy offered a more solid legal ground for the CJEU to articulate its decisions than the fundamental right to personal data protection.⁴⁵⁴

2.3.1.1. Rundfunk (2003) – a missed opportunity to exploit the functionality of EU data protection law

*Rundfunk*⁴⁵⁵ is the first case where the CJEU was asked to interpret the 1995 Data Protection Directive. The facts of the case related to the application of an Austrian law according to which bodies subject to control by the Austrian Court of Audit had to transmit the salaries and pensions of (ex) public servants exceeding a certain threshold. Disclosure of the names of the individuals concerned was not expressly mentioned in the Austrian legislation but followed from the doctrine adopted by the Court of Audit. The data were compiled in an annual report which was transmitted to both the Austrian Parliament and the provincial parliaments before being made available to the public. After the transposition of the 1995 Data Protection Directive into national law, some public undertakings decided not to communicate the data of their (ex) employees, or to communicate the data without the names of the

⁴⁴⁸ CJEU, Judgment of 20 May 2003, *Österreichischer Rundfunk e.a.*, Case C-465/00

⁴⁴⁹ CJEU, Judgment of 6 November 2003, *Lindqvist*, Case C-101/01.

⁴⁵⁰ CJEU, Judgment of 16 December 2008, *Satamedia*, Case C-73/07.

⁴⁵¹ CJEU, Judgment of 8 November 2007, *Bavarian Lager*, Case T-194/04.

⁴⁵² CJEU, Judgment of 29 January 2008, *Promusicae*, Case C-275/06.

⁴⁵³ See in particular Article 1(1) of the 1995 Data Protection Directive, Article 1(1) of Regulation (EC) No 45/2001 and Article 4(1)(b) of Regulation (EC) No 1049/2001.

⁴⁵⁴ Lynskey, O. (2014). *op. cit.*, p. 574.

⁴⁵⁵ CJEU, *Österreichischer Rundfunk e.a.*

individuals concerned,⁴⁵⁶ arguably for complying with the applicable data protection law. Other public undertakings, however, continued to communicate the full names of the individuals concerned. Such was the case of the public broadcasting organization *Österreichischer Rundfunk*. In this context, Ms Neukomm and Mr Lauer mann – two employees of *Österreichischer Rundfunk* – argued before the Austrian Court that the transmission and publication of their personal data was contrary to the 1995 Data Protection Directive. The Austrian courts decided to stay the proceedings and ask the CJEU for clarification in this respect.

In its judgment of 20 May 2003, instead of interpreting the relevant provisions of the 1995 Data Protection Directive,⁴⁵⁷ the CJEU decided to examine whether the transmission of the data would be compatible with the right to respect for private and family life as enshrined in Article 8 of the ECHR. Relying on the three-step process usually applied by the ECtHR, the CJEU therefore first assessed whether there had been an interference with the right to privacy of the individuals concerned, before analysing whether such an interference could be justified because it was “*in accordance with the law*” and “*necessary in a democratic society*”. In the end, the CJEU found that the processing practice at stake constituted an interference with the right to privacy of the individuals concerned, but that this interference was made in accordance with Austrian law. It further stated that it was for the national court to ascertain whether the domestic law was meeting the requirement of foreseeability. Regarding necessity, the CJEU observed that the object of the interference was to ensure the thrifty and appropriate use of public funds by the authorities, which constituted a legitimate aim within the meaning of Article 8 of the ECHR. In this respect, the CJEU further considered that it was for the national court to examine whether it was necessary to make both the names and the financial data available to the general public, or whether it would be sufficient to inform the general public about the salaries or pensions paid by the public undertakings, without identifying the persons concerned.

In the *Rundfunk* case, the CJEU did not mention the EU Charter of Fundamental Rights and did not interpret the relevant provisions of the 1995 Data Protection Directive. Instead, it relied on an external source of EU law, the ECHR, and in particular on its Article 8 (right to respect for private and family life). Some scholars

⁴⁵⁶ Cf. personal data are data relating to an identified or identifiable living person. If the names of the individuals were not communicated with the list of salaries and pensions paid, the individuals concerned could (normally) no longer be identified and the data would have then fallen outside of the scope of the 1995 Data Protection Directive.

⁴⁵⁷ It is interesting to note in this respect that the CJEU did quote the relevant provisions of the 1995 Data Protection Directive in its judgment, although it failed to interpret them in the light of the circumstances at hand (paras. 7-16 of the judgment). This is even more surprising given the fact that some of the Member States who joined the proceedings submitted written observations which interpreted these provisions. The Austrian, Italian, Netherlands, Finnish and Swedish Governments and the Commission considered in particular that the national provisions at issue were compatible with the 1995 Data Protection Directive because the processing was necessary in order to achieve a task in the public interest, in accordance with Articles 6(b) and (c) and 7(c) or (e) of the Directive. The public interests at stake were the respect of the principle of transparency, of the proper management of public funds and the prevention of abuses (see para. 50 of the judgment).

have therefore expressed a critical opinion on this judgment.⁴⁵⁸ Lynskey, for example, states that “the Court entirely overlooked the specific rules set out in the Data Protection Directive” and instead “simply substituted privacy rules for data protection rules”.⁴⁵⁹ Instead of using EU data protection law as a functional tool for ensuring the respect Ms Neukomm and Mr Lauerermann’s right to privacy, the CJEU exclusively articulated its preliminary ruling on the basis of Article 8 of the ECHR. This decision can therefore be criticized for its lack of consideration of data protection rules, and its over-emphasis on the right to privacy as enshrined in the ECHR.

In the context of this study, the main remark that can be made with respect to *Rundfunk* is that the CJEU completely overlooked and thus missed the opportunity to use EU data protection rules as a functional framework for the defence of fundamental rights. Although this ruling ignored the potential functional nature of EU data protection law, it did indirectly contribute to achieving its FRO by reminding that the right to privacy as enshrined in the ECHR could not be unduly interfered with through the publication of personal data.

2.3.1.2. Lindqvist (2003) – the right to privacy of individuals in the context of blogging

The same year as *Rundfunk*, the CJEU rendered another preliminary ruling with respect to several questions on the interpretation to be given to the 1995 Data Protection Directive in the *Lindqvist* case.⁴⁶⁰ This time, the CJEU meticulously interpreted the wording of the 1995 Data Protection Directive and delivered a ruling which reinforced the scope of EU data protection law, while putting emphasis on the importance to respect data subjects’ right to privacy in the context of online blogging.

The facts concerned Mrs Lindqvist, an active member of the parish of Alseda in Sweden who was involved in preparing people for Communion, among others. At the end of 1998, she took the initiative to set up internet pages providing practical information on the activities of the parish. Those pages also contained personal information on 18 of Mrs Lindqvist’ colleagues, including their names, parish work, hobbies and in several cases their family circumstances or telephone number. She also mentioned that one of her colleagues had injured her foot and was working part-time on medical grounds. Following a complaint from those colleagues, Mrs Lindqvist was fined SEK 4000 (approximately EUR 450) by the Swedish data protection authority (the Datainspektionen) for infringing data protection law. In

⁴⁵⁸ Classen, C. (2004). Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk*, Judgment of 20 May 2003, Full Court, [2003] ECR I-4989. *Common Market Law Review*, 41(5), pp. 1380-1385; Docksey, C. (2016). *op. cit.*, p. 201; Irion, K. (2016). A special regard: The Court of Justice and the fundamental rights to privacy and data protection. *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte*, p. 880; Lynskey, O. (2014), *op. cit.*, p. 575.

⁴⁵⁹ Lynskey, O. (2014), *op. cit.*, p. 575.

⁴⁶⁰ CJEU, Judgment of 6 November 2003, *Lindqvist*, Case C-101/01.

particular, it had been found that Mrs Lindqvist had unlawfully processed sensitive personal data (i.e., health data) and had failed to make a prior written notification to the Datainspektionen with respect to the intended processing activity (an obligation which does not exist anymore, but which was mandatory under the regime of the 1995 Data Protection Directive).⁴⁶¹ Mrs Lindqvist appealed against that decision invoking, *inter alia*, her freedom of expression. In this context, the Court of Appeal of Göta asked the CJEU whether the activities conducted by Mrs Lindqvist were contrary to the provisions of the 1995 Data Protection Directive.

Among the preliminary questions referred to the CJEU, three of them concerned the scope of the 1995 Data Protection Directive. Each time, the CJEU answered these questions in a manner which confirmed the broad scope of application of the Directive – thereby making it effective and functional for the data subjects concerned. With respect to the material scope of the Directive, the CJEU recalled that personal or domestic processing activities, such as keeping a private diary, engaging into correspondence or the holding of a private record of addresses, normally fall outside of EU data protection law.⁴⁶² The CJEU however considered that the publication of the data subjects’ personal data by Mrs Lindqvist on her blog could not benefit from this exception, since the blog was public. In particular, the Court pointed that when personal data are published on the internet and thereby “*made accessible to an indefinite number of people*”, such an activity cannot be considered as “*exclusively personal or domestic*”.⁴⁶³ As a consequence, most processing activities undertaken by private individuals on publicly accessible website or social media accounts now fall under the scope of EU data protection law, given they are directed *outwards* from the private setting of these individuals. Personal data published on a public TikTok or Twitter account, for example, would arguably be covered by the GDPR since they are made available to an indefinite amount of internet users and non-users.

With regard to the FRO of EU data protection law, the ruling of the CJEU was overall beneficial to the right to privacy of the concerned data subjects (i.e., the colleagues of Mrs Lindqvist). The CJEU however made no reference to the right to personal data protection as protected by Article 8 of the Charter.⁴⁶⁴ Another interesting point concerns the clash between the right to privacy of the data subjects and the freedom of expression of Mrs Lindqvist. It is important to note in this respect that the FRO of the 1995 Data Protection Directive aims at ensuring the respect of the fundamental rights and freedoms of the *data subjects*. By contrast, the fundamental rights and freedoms of *other* individuals are not expressly mentioned in the objective of the Directive. In this case, the data subjects were the colleagues of Mrs Lindqvist, who had arguably suffered from an invasion of their right to privacy. Mrs Lindqvist herself

⁴⁶¹ Article 18(1) of the 1995 Data Protection Directive. See also *Lindqvist*, para. 15.

⁴⁶² Article 3(2) of 1995 Data Protection Directive 95/46 (today Article 2(2) of the GDPR).

⁴⁶³ CJEU, *Lindqvist*, para. 47.

⁴⁶⁴ *Ibid.*, paras. 10, 72, 76, 78 and 90. Only the right to privacy enshrined in Article 8 of the ECHR is mentioned.

was the person responsible for processing the personal data – the so-called ‘controller’, and was invoking her freedom of expression to justify the publication of information relating to her colleagues on her blog. Keeping this important distinction in mind, it must therefore be acknowledged that EU data protection law is primarily concerned with the protection of the fundamental rights of the data subjects (in this case, the right to privacy of the colleagues of Mrs Lindqvist), even if such protection would entail a limitation of the rights of other persons (such as the freedom of expression of Mrs Lindqvist). In its ruling, the Court however observed that the 1995 Data Protection Directive contains several provisions allowing Member States to weigh conflicting fundamental rights.⁴⁶⁵ The Court observed in particular that “*Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site.*”⁴⁶⁶ It then recalled that it is for the national court to ensure that the 1995 Data Protection Directive is not interpreted in a way that would be in conflict with the fundamental rights or general principles of EU law.⁴⁶⁷

In the context of this study, it can be concluded that *Lindqvist* is the first case where the CJEU contributed to the blooming of the FRO of EU data protection law by interpreting the Directive in a manner which confirmed its broad material scope, for the benefit of the right to privacy of the data subjects concerned. The CJEU further recalled that when the fundamental right to privacy of a data subject conflicts with the fundamental right(s) of a third party, the Member States are responsible for applying EU data protection rules in a way that respect the principle of proportionality, in an attempt to reconcile the exercise of those conflicting rights. On the downside, it can be noted that the questions referred to the CJEU were exclusively articulated around the right to *privacy* of the data subjects, and that no mention was made of their right to personal data protection as enshrined in Article 8 of the Charter. This is representative of the reluctance of the CJEU to refer, in the pre-Lisbon era, to the Charter as a self-standing source of law because of its lack of legal status in the EU legal system. Yet, it can still be argued that this ruling contributed to the realisation of the FRO of EU data protection law since the provisions of the 1995 Data Protection Directive were interpreted generously in favour of the data subjects’ right to privacy.

Lindqvist also shows that the regulation of processing activities may give rise to situations where the fundamental rights and freedoms of data subjects may sometimes clash with the fundamental rights and freedoms of controllers or third parties. In this respect, it is undeniable that EU data protection law can be interpreted or applied in a manner which may restrict the exercise of important

⁴⁶⁵ *Ibid.*, para. 83.

⁴⁶⁶ *Ibid.*, para. 86.

⁴⁶⁷ *Ibid.*, para. 87.

rights and freedoms or the defence of public interests, such as freedom of expression, right to a good administration, access to documents, etc. As pointed out in the Introduction and first Chapter of this study, however (see point D and section 1.3.2 above), the issue relating to the potential ‘weaponization’ of EU data protection law in a way that could be harmful to controllers or third parties falls outside of the scope of this study, as it does not directly relate to the functionality of EU data protection law for the defence of the rights and freedoms of data subjects. Therefore, even if it is important to acknowledge the existence of this tension and the need to establish a balance between conflicting rights and interests, as exemplified in the Lindqvist case, readers should be aware that this topic will not be explored in detail in this study.

2.3.1.3. *Promusicae* (2008) – Article 8 of the Charter as a mere cosmetic source

In *Promusicae*,⁴⁶⁸ the CJEU interpreted the compatibility of intellectual property rights enforcement with the provisions of the 1995 Data Protection Directive on. The proceedings were brought by *Promusicae*, a Spanish non-profit-making organization defending the interests of the music industry. *Promusicae* was seeking the disclosure of the identities and physical addresses of certain individuals who were suspected to illegally share music content through a peer-to-peer file exchange program. *Promusicae* needed this information in order to be able initiate civil proceedings against the individuals concerned for copyright infringements. The internet service provider, which could have provided that information to *Promusicae*, refused to do so, arguing that such a disclosure would be contrary to Spanish law, including data protection law. *Promusicae*, on the other hand, referred to several Directives requiring Member States to ensure the effective protection of copyright. In this context, the Spanish court asked the CJEU whether EU law required the Member States to lay down an obligation to communicate personal data of potential infringers in the context of civil proceedings for the enforcement of copyrights. In its reasoning, the CJEU refers to both Article 7 (right to respect for private and family life) and Article 8 (right to personal data protection) of the Charter.⁴⁶⁹ However, in the rest of the judgment, the CJEU only focuses on the right to privacy in particular, and stresses “*the need to reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other*”.⁴⁷⁰ The CJEU remains silent with respect to the right to personal data protection, as if it had been integrated *into* the right to privacy.⁴⁷¹ At the end of its ruling, the CJEU concludes that it is the duty of the Member States, when transposing the directives on intellectual property and the protection of personal data, to rely on an

⁴⁶⁸ CJEU, Judgment of 29 January 2008, *Promusicae*, Case C-275/06.

⁴⁶⁹ *Ibid.*, para. 64.

⁴⁷⁰ *Ibid.*, para. 65.

⁴⁷¹ *Ibid.*, p. 576. Lynskey, O. (2014) argues in this respect that “*to the Court data protection is synonymous with privacy*”.

interpretation of those directives which allows a fair balance to be struck between the fundamental rights to privacy, the protection of property and the right to an effective remedy. Furthermore, when implementing national measures, the authorities and courts of the Member States should make sure that they do not rely on an interpretation of EU law which would be in conflict with EU fundamental rights or with the other general principles of EU law, such as the principle of proportionality.

The fact that the CJEU referred to Article 8 of the Charter “*offered some initial promise*”,⁴⁷² including the possibility that the CJEU would interpret the relevant EU law in light of the fundamental right to personal data protection. But in the rest of the judgment, the CJEU exclusively put emphasis on the right to privacy, relegating data protection in the shadows. All in all, the *Promusicae* judgment can thus be considered as yet another illustration of the tendency of the EU to disregard the fundamental right to data protection and to rely on the right to privacy instead.

2.3.1.4. Satamedia (2008) – the limits of journalistic freedom in light of the right to privacy

The same year, the CJEU rendered another ruling in the *Satamedia* case.⁴⁷³ This case concerned the interpretation to be given to the 1995 Data Protection Directive in order to reconcile data protection rules, privacy and journalistic freedom.

For several years, *Markkinapörssi* (a Finish company) collected public data from the national tax authorities with a view of publishing these data in the regional editions of the newspaper *Veropörssi*. The information contained in those publications comprised the name and financial data of approximately 1.2 million persons. In 2003, *Markkinapörssi* and its associated company, *Satamedia*, signed an agreement with a mobile telephony company, in order to put in place a text-messaging service, on behalf of *Satamedia*, allowing mobile telephone users to receive information published in the newspapers on their telephone for a charge of approximately two euros. On request, the personal data of the individuals could be removed from that service. Following complaints from individuals alleging infringement of their right to privacy, the Data Protection Ombudsman applied for an order prohibiting *Markkinapörssi* and *Satamedia* from carrying on the personal data processing activities at issue. This decision was contested by *Markkinapörssi* and *Satamedia*, who relied, *inter alia*, on freedom of expression for journalistic purposes. In the course of the proceedings, the Supreme Administrative Court of Finland referred several questions to the CJEU regarding the interpretation to be given to the 1995 Data Protection Directive. In particular, the CJEU was asked whether the directive should be interpreted as meaning that the processing activities of *Markkinapörssi*

⁴⁷² Lynskey, O. (2014). *op. cit.*, p. 576.

⁴⁷³ CJEU, Judgment of 16 December 2008, *Satamedia*, Case C-73/07.

and *Satamedia* (and in particular the text message service) must be considered as carried out solely for journalistic purposes.

At this stage, it is important to note that the 1995 Data Protection Directive contains a special provision aiming at reconciling the right to privacy of data subjects on the one side, and freedom of expression for the purpose of journalism, or artistic or literary expression:

Article 9 – Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations (...) for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

In its ruling, the CJEU first confirmed that the processing activities of *Markkinapörssi* and *Satamedia* had to be considered as processing of personal data in the sense of the Directive, thereby reaffirming its broad scope. The CJEU then pointed out that the obligation to reconcile privacy and freedom of expression under Article 9 of the Directive lies on the Member States.⁴⁷⁴ In this respect, the CJEU first recalled the cardinal importance of freedom of expression in every democratic society. Hence, according to the CJEU it is necessary “to interpret notions relating to that freedom, such as journalism, broadly”.⁴⁷⁵ Looking into the activities of *Markkinapörssi* and *Satamedia*, the CJEU acknowledged that these companies are not officially “media undertakings”,⁴⁷⁶ that they generate a profit through the proposed service,⁴⁷⁷ or that they do not use classic medium of communication.⁴⁷⁸ Yet, according to the EU judges, those three criteria are *not* determinative as to whether an activity is undertaken ‘solely for journalistic purposes’. The CJEU considers *a contrario* that *Markkinapörssi* and *Satamedia*’s activities may be classified as ‘journalistic activities’ if their object is the disclosure – to the public – of information, opinions or ideas, irrespective of the medium used. It is however for the national court to determine whether the text messaging service developed on behalf of *Satamedia* fulfils these criteria.⁴⁷⁹ Most importantly, the CJEU highlighted that, in order for the national court to achieve a balance between freedom of expression and the right to privacy, the protection of the fundamental right to privacy requires that the derogations and limitations provided by national law must apply only in so far as is strictly necessary.⁴⁸⁰ In other

⁴⁷⁴ *Ibid.*, para. 54.

⁴⁷⁵ *Ibid.*, para. 56.

⁴⁷⁶ *Ibid.*, para. 58.

⁴⁷⁷ *Ibid.*, para. 59. The CJEU even notes in this respect that “a degree of commercial success may even be essential to professional journalistic activity.”

⁴⁷⁸ *Ibid.*, para. 60.

⁴⁷⁹ *Ibid.*, para. 62.

⁴⁸⁰ *Ibid.*, para. 56.

words, while it is true that Article 9 of the 1995 Data Protection Directive introduces some derogations for the sake of journalistic freedom, such derogations must be interpreted restrictively, otherwise the object of the 1995 Data Protection Directive itself would be undermined.⁴⁸¹

In the context of this study, it can be concluded that the ruling in *Satamedia* partially contributed to the realisation of the FRO of EU data protection law, since the interpretation given to the 1995 Data Protection Directive was centred around the need to ensure the respect of the right to privacy of the data subjects concerned. In particular, the CJEU expressly admitted that Member States could limit journalistic freedom on the basis of the 1995 Data Protection Directive where such a limitation would be proportionate and necessary for protecting the privacy of data subjects. Contrary to the judgment in the preceding case *Promusicae*, however, the CJEU did not mention the fundamental right to personal data protection. In the opinion of the author, this reluctance to rely on Article 8 of the Charter to assess the situation is understandable for the reasons explained in Section **Error! Reference source not found.**(2.2.3.3), above. Yet, it remains regrettable, since Article 8 of the Charter would have enabled to assess the legitimacy of the concerned processing activities not only in relation to an interference with private life but also in relation to an interference with data protection-related rights, such as the right to request the access, rectification or erasure of personal data – a set of data protection rights which were arguably substantially compromised by the means of dissemination chosen by *Markkinapörssi* and *Satamedia*.

2.3.1.5. Huber (2008) – early evidence of the secondary functionality of EU data protection law

The same day as the judgment in *Satamedia*, the CJEU rendered another decision in the case *Huber*, where a data subject was objecting to the processing of his personal data by the federal government of Germany.⁴⁸² This decision is particularly important with respect to the realisation of the FRO of EU data protection law, since the data subject in that case (Mr Hanz Huber) was not arguing that the processing of his personal data was contrary to his *right to privacy*, but was instead claiming that it infringed his right to *equal treatment* and *non-discrimination*.

The facts of the case were as follows: Mr Hanz Huber, an Austrian national, moved to Germany in 1996 as a self-employed insurance agent. At that time, a centralized register (the “AZR”) containing personal data on foreign nationals residing in Germany was kept by the Federal government. This register contained information

⁴⁸¹ i.e., the protection of “the fundamental rights and freedoms of natural persons, and in particular their **right to privacy** with respect to the processing of personal data”. See Article 1(1) of the 1995 Data Protection Directive (“Object of the Directive”).

⁴⁸² CJEU, Judgment of 16 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, Case C-524/06.

on both EU and non-EU foreign nationals that had moved to Germany. By contrast, the AZR did not exist in respect of German nationals. On 22 July 2000, Mr Huber requested the deletion of his personal data from the AZR by relying on the relevant provisions of the German data protection legislation as well as the principle of non-discrimination. That request was rejected on 29 September 2000 by the administrative authority which was responsible for maintaining the AZR at the time. Mr Huber contested such a decision before the competent courts. In the course of the proceedings, Germany notably argued that the processing of such personal data was lawful because it was “*necessary for the performance of a task carried out in the public interest (...)*”, i.e., one of the specific grounds listed in Article 7 of the 1995 Data Protection Directive for the purpose of processing personal data. In this context, three questions were referred to the CJEU. The principal question concerned the compatibility of the AZR with the prohibition of discrimination on grounds of nationality against EU citizens who exercise their right to move and reside freely within the territory of the Member States.

After interpreting the relevant EU law in light of the facts of the case, the CJEU found that the use of a register such as the AZR could, in principle, be legitimate and compatible with the prohibition of discrimination on grounds of nationality if the purpose was to provide support to the authorities responsible for the application of the legislation relating to the right of residence. In other words, if the purpose of such a register was indeed to help the authorities to fulfil a legitimate administrative purpose, it could be allowed (i.e., application of a ‘legitimacy’ criteria). The Court stressed however that such a register should not contain any information other than what is necessary for that specific purpose. Furthermore, the Court added that centralizing this information at the State level could only be considered as “*necessary*” in the sense of the law, if it allowed the legislation on the right to residence to be more effectively applied (the ‘necessity’ criteria). The CJEU then recalled that it was for the national court to ascertain whether those two criteria were satisfied in the case at hand.

In the context of this study, this case can be considered as a milestone since it is the first time that the CJEU rendered a ruling on the lawfulness of a data processing practice in light of a fundamental right *other* than the right privacy or personal data protection – i.e., the right to equal treatment. This case therefore shows that EU data protection law can indeed be deployed as (multi-)functional tool for protecting various fundamental rights or freedom, beyond privacy. As further shown below, however, *Huber* stands as an exception in the data protection case-law of the CJEU, whose multi-functional nature therefore appears to largely remain unexploited.

2.3.2. Lisbon era: EU data protection law at the service of Article 7 and 8 of the Charter

As just seen in the previous section, between December 2000 and December 2009, most of the case-law of the CJEU in the field of data protection primarily served the fundamental right to privacy of the data subjects. In a large majority of cases indeed, the CJEU generously interpreted EU data protection law for the benefit of the right to privacy of individuals confronted to intrusive data processing practices. It remained however silent on the actual substance of the fundamental right to personal data protection, as enshrined in Article 8 of the Charter, and rarely interpreted EU data protection law in light of, or for the benefit of other fundamental rights or freedoms (with the notable exception of *Huber*). This tendency to focus on the right to privacy appears logical when one takes into consideration the origin of the FRO of EU data protection law whose DNA is arguably rooted in the right to privacy, as well as the fact that the Charter of Fundamental Rights of the EU (including its Article 8) was not yet binding at that time.

In December 2009 however, a major change occurred in the EU legislative landscape when the Lisbon Treaty entered into force.⁴⁸³ Article 6 of the TEU was thereby amended to be composed of three paragraphs which elevated the Charter to the rank of EU primary law, reaffirmed in parallel the willingness of the EU to accede to the ECHR, and further aimed at accommodating these two different sources of law that still form today the main *corpus* of EU fundamental rights law.⁴⁸⁴ As from that day, the binding force of the Charter was unleashed, and the CJEU started to increasingly rely on the provisions of the Charter in its judgments, not merely as a mean to vaguely support or justify its reasoning,⁴⁸⁵ but as a mean to concretely interpret and assess the validity of EU law, including EU data protection law.⁴⁸⁶ In parallel, the Lisbon Treaty integrated a new “*key provision*”⁴⁸⁷ on the protection of personal data : Article 16 of the TFEU, which provides a clear legal basis to the European Parliament and the Council to lay down rules in matters of data protection.⁴⁸⁸ Shortly afterwards, the Commission relied on Article 16 of the TFEU to initiate a reform and introduce a new data protection package, which would later lead to the adoption of the GDPR.⁴⁸⁹ Among the foreseen changes, this updated version of EU data protection law was articulated around the premise that

⁴⁸³ Article 6(1) TEU, as amended by the Lisbon Treaty.

⁴⁸⁴ Pech, L. & Groussot, X. (2010). Fundamental Rights Protection in the European Union post Lisbon Treaty. *European Issues* 173.

⁴⁸⁵ Pech, L. & Groussot, X. (2010), *op. cit.*, p. 2.

⁴⁸⁶ Lock, T. & Layden, P. (2011). Protection of Fundamental Rights Post-Lisbon: The Interaction between the EU Charter of Fundamental Rights, the European Convention on Human Rights (ECHR) and National Constitutions. *FIDE National Report for the United Kingdom*.

⁴⁸⁷ González Fuster (2014). *op. cit.*, p. 232.

⁴⁸⁸ *Ibid.*, p. 233.

⁴⁸⁹ The reform was initiated in January 2012, when the EU Commission proposed a legislative package in order to update EU legislation in matters of data protection. For a comprehensive summary, please refer to COM MEMO/12/41 of 25 January 2012, available at https://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=fr.

individuals enjoyed a fundamental right to personal data protection, and that such a right ought to be protected (in lieu of the right to privacy). From a legal point of view, everything was falling into places for the career of the fundamental right to personal data protection to 'take off' as from 2009. In the end however, it took several years for these new instruments to be adopted and replace the old ones.⁴⁹⁰

As from December 2009, when national courts started referring questions to the CJEU in matters relating to the processing of personal data, the CJEU was thus caught between (1) a newly legally binding Charter which enshrined a fundamental right to personal data protection, whose specific scope, substance and essence still needed to be clarified, and (2) a pre-existing set of legislation in matters of data protection which did not refer to Article 8 of the Charter but put emphasis on the right to privacy instead. As further analysed below, the case-law of the CJEU in the Lisbon era reflects this legal dichotomy. Sometimes indeed, the CJEU simply disregarded Article 8 of the Charter when interpreting EU data protection law, while in other cases, it relied on it to interpret EU secondary law in the field of data protection, thereby participating to its emancipation. Finally, in several cases, the CJEU interpreted EU data protection law for the benefit of *two other* fundamental rights: freedom of expression (Article 11 of the Charter) and the right to judicial remedy and a fair trial (Article 49 of the Charter).

To illustrate these trends, the following sub-section will discuss five landmark judgments that the CJEU rendered in the early Lisbon era.

2.3.2.1. Volker und Markus Schecke and Eifert (2010) – the coupling of Article 7 and 8 of the Charter

On 9 November 2010, i.e., one year after the entry into force of the Lisbon Treaty, the CJEU rendered a preliminary ruling concerning the interpretation of data protection legislation in the joined cases C-92/09 (Volker und Markus Schecke GbR) and C-93/09 (Hartmut Eifert).⁴⁹¹ Quite notably, this preliminary ruling is the first one in which the CJEU attempted to interpret the relevant EU legislation in light of the fundamental right to personal data protection as enshrined in Article 8 of the Charter.

This case concerned the processing of personal data by the German government in the context of the attribution of agricultural aid. Volker und Markus Schecke GbR, an agricultural firm, as well as Hartmut Eifert, a full-time farmer, were both granted EU

⁴⁹⁰ As an illustration, the GDPR – which has replaced the 1995 data Protection Directive – was first submitted as a proposal by the Commission in 2012, was adopted by the European Parliament and the Council in 2016, and only became effectively applicable in May 2018. During this 'in-between' period, the 1995 Data Protection Directive, as well as other pre-existing legislative texts putting emphasis on the right to privacy, remained the applicable law.

⁴⁹¹ CJEU, Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, Joined Cases C-92/09 and C-93/09.

agricultural aid for the financial year 2008 after having applied for it. In each case, the application form contained the following statement: “*I am aware that [EU law] requires publication of information on the beneficiaries of [funds from] the EAGF and the EAFRD and the amounts received per beneficiary.*”⁴⁹² Under the applicable EU law indeed,⁴⁹³ Member States had to publish the names of beneficiaries of EU agricultural funds, the amounts received by each beneficiary, as well as the place in which those beneficiaries were established or resided.⁴⁹⁴ In Germany, it was the German Federal Office for Agriculture and Food which made this information available to the public through a website. The website included a search tool that facilitated the retrieval of information concerning beneficiaries of these funds. In their respective actions, Volker und Markus Schecke GbR and Hartmut Eifert (the ‘Beneficiaries’) were seeking an order requiring the Land of Hesse not to publish these data on the website, as they considered that this would amount to an unjustified interference with their fundamental right to privacy and their right to personal data protection, as recognized in Article 7 and 8 of the Charter. In this context, the Administrative Court of Wiesbaden stayed the proceedings and referred several questions to the CJEU on the interpretation to be given to EU secondary law in the field of data protection (including the 1995 Data Protection Directive), in light of Article 7 and 8 of the Charter.

In the judgment of the CJEU, under the section “*Legal context*”, the applicable legislation is quoted, starting with the fundamental right to privacy. However, instead of quoting Article 7 of the Charter, the CJEU refers instead to Article 8 of the ECHR – and this, despite the fact that the Administrative Court of Wiesbaden had expressly mentioned the Charter in its reference for a preliminary ruling. This seems to indicate that, in the mind of the CJEU, the ECHR was still a more relevant or solid source of fundamental rights law than the Charter. In the core of the judgment, however, when analysing the first question submitted by the referring court, the CJEU suddenly refers to Article 6(1) of the TEU (as modified by the Lisbon Treaty one year earlier), according to which the Charter had gained “*the same legal value as the Treaties*”. It goes on by stating that the validity of EU law must be assessed in the light of the provisions of the Charter, and in particular Article 8(1) of the Charter, which provides: “[e]veryone has the right to the protection of personal data concerning him or her” – an Article which is “*closely connected with the right to respect of private life expressed in Article 7 of the Charter*”.⁴⁹⁵ One may agree that the statement of the CJEU according to which Article 7 and 8 of the Charter are

⁴⁹² *Ibid.*, para. 26.

⁴⁹³ And in particular Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, *OJ L 209, 11.8.2005, p. 1–25* (no longer in force) and Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Council Regulation (EC) No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EDFRD), *OJ L 76, 19.3.2008, p. 28–30* (no longer in force).

⁴⁹⁴ In particular, the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EDFRD).

⁴⁹⁵ CJEU, *Volker und Markus Schecke and Eifert*, para. 47.

“*closely connected*” is neither surprising nor incorrect. After all, in the Explanations of the Charter, the right to privacy is expressly mentioned in the sources of the fundamental right to personal data protection. Yet, in one of the following paragraphs of the Judgment, the CJEU goes one step further by conflating both rights into a sort of “*hybrid species*”⁴⁹⁶, by referring to “*the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter (...)*”. This wording echoes the expression enshrined in the 1995 Data Protection Directive itself, whose object was the protection of “*the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*” (emphasis added).⁴⁹⁷ A major difference however is that the 1995 Data Protection Directive did not link or refer to Articles 7 and 8 of the Charter to justify such a wording, for an obvious reason: at the time of the adoption of the 1995 Data Protection Directive, the Charter had not yet been proclaimed. The initiative of the CJEU to recycle the expression used in the 1995 Data Protection Directive and to match it with two provisions of the Charter can either be considered as logical or, on the contrary, criticized for the questionable hierarchy that it seems to establish between Article 7 and 8 of the Charter. On the one side indeed, it could be argued that the CJEU simply intended to highlight the areas in which the right to privacy and the right to personal data protection are overlapping – the product of this overlap creating a “*right to privacy with respect to the processing of personal data*”. On the other side however, it appears that this wording gives prevalence to the right to privacy, since it refers to the mere context of ‘data processing’ rather than the right to data protection itself. The rest of the paragraph brings even more confusion since the CJEU suddenly refers to the ECHR (instead of the Charter) to conclude that “*limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the [ECHR]*.”⁴⁹⁸ In other words, the CJEU seems to be of the opinion that the scope of the fundamental right to personal data protection is limited to the scope of the right to privacy under the ECHR, and can thus be analysed in the light of the case-law of the ECtHR on the right to privacy. In the rest of the judgment, the CJEU exclusively refers to the right to personal data protection in combination with the right to privacy (the expression “*Articles 7 and 8 of the Charter*” is used 16 times throughout the judgment), without ever considering Article 8 independently. As a consequence, when interpreting whether the publication of the names of the Beneficiaries could constitute an interference with their “*right for private life with regard to the processing of personal data*,” and whether such an interference could be justified under Article 52(1) of the Charter, the CJEU did not conduct two separate analyses, but treated Articles 7 and 8 of the Charter as one.⁴⁹⁹

⁴⁹⁶ Lynskey, O. (2014). *op. cit.*, p. 580.

⁴⁹⁷ Article 1(1) of the 1995 Data Protection Directive.

⁴⁹⁸ CJEU, *Volker und Markus Schecke and Eifert*, para. 52.

⁴⁹⁹ *Ibid.*, paras. 56-89.

While, in previous cases, the CJEU mainly ignored the existence of the fundamental right to data protection, or simply mentioned it without further consideration, *Schecke and Eifert* is the first case where the CJEU acknowledged the role and existence of Article 8 of the Charter. Confusingly, however, the CJEU never relied on Article 8 of the Charter alone but systematically coupled it with Article 7, while seemingly giving precedence to the latter. In that sense, it can be argued that the judgment in *Schecke and Eifert* participated to the coupling⁵⁰⁰ of the right to privacy with the right to data protection, rather than to its emancipation or clarification.

2.3.2.2. Deutsche Telekom (2011) – the start of the emancipation of Article 8 of the Charter

In May 2011, the CJEU rendered judgment on the interpretation of the e-Privacy directive in the field of telecommunications in which, for the very first time, the fundamental right to personal data protection as enshrined in Article 8 of the Charter was envisaged independently from the right to privacy, thereby breaking the habit that the CJEU had always had to conflate both rights together. The case *Deutsche Telekom*⁵⁰¹ concerned a reference for a preliminary ruling regarding the obligations of telephone service providers (TSPs) under EU law to share data on their subscribers and other TSPs' subscribers with companies providing publicly available directories ('directory holders'). The questions referred to the CJEU focused in particular on the extent of these obligations as far as 'external data' are concerned (data relating to subscribers of *other* TSPs). By its first question, the referring court asked in essence whether the obligation of TSPs under EU law⁵⁰² to share data with directory holders was extending to 'external data', or if it was limited to the data of their own subscribers. The CJEU answered this question by stating that the obligation of TSPs to share information about subscribers with directory holders could include internal and external data.⁵⁰³

By its second question, the referring court then asked whether Article 12 of the e-Privacy Directive made the transfer of such external data conditional on the consent, or lack of objection, of the subscribers concerned. The CJEU started to answer that second question by recalling that "*Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') states that '[e]veryone has the right to the protection of personal data concerning him or her'*"⁵⁰⁴ – a right which is "*not absolute but must be considered in relation to its function in society'*".⁵⁰⁵ Referring to the second paragraph of Article 8 of the Charter, the CJEU then noted that the passing of

⁵⁰⁰ Following the expression used by Gonzáles Fuster, G. (2014). In the same vein, Lynskey refers to the "conflating" of both rights (see Lynskey, O. (2014). *op. cit.*, p. 573).

⁵⁰¹ CJEU, Judgment of 5 May 2011, *Deutsche Telekom*, Case C-543/09.

⁵⁰² And in particular, Article 25(2) of the Universal Service Directive (Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services, *OJ L 108*, 24.4.2002, p. 51–77).

⁵⁰³ CJEU, Judgment of 5 May 2011, *Deutsche Telekom*, Case C-543/09, para. 47.

⁵⁰⁴ *Ibid.*, para. 49.

⁵⁰⁵ *Ibid.*, para. 51.

subscribers' personal data to a third-party undertaking constitutes processing of personal data, which may therefore be undertaken only “*on the basis of the consent of the person concerned or some other legitimate basis laid down by law*”. After analysing the relevant provisions of EU secondary law, the CJEU applied those provisions to the facts at hand in the light of Article 8 of the Charter and concluded in this respect that “*where a subscriber has consented to the passing of his personal data to a [directory holder], the passing of the same data to another [directory holder] without renewed consent having been obtained from that subscriber is not capable of substantively impairing the right to protection of personal data, as recognised in Article 8 of the Charter*”.⁵⁰⁶

By doing so, the CJEU interpreted both the scope and content of the fundamental right to personal data protection independently from the right to privacy. As a matter of fact, the CJEU did not even mention the right to privacy in its findings but interpreted the relevant EU secondary law exclusively in the light of Article 8 of the Charter. *Deutsche Telekom* can thus be considered as the first case where the CJEU interpreted and applied the right to personal data protection independently from the right to privacy, thereby participating to its emancipation and to the clarification of its actual content.⁵⁰⁷

2.3.2.3. Digital Rights Ireland (2014)⁵⁰⁸ – evidence of the independent yet connected nature of Article 7 and 8 of the Charter

In 2006, the EU adopted the Data Retention Directive,⁵⁰⁹ whose purpose was to harmonize the obligations of providers of (electronic) communication services ('PECS') regarding the retention of traffic and location data, in order to ensure that these data were available for the purpose of the investigation, detection and prosecution of serious crime.⁵¹⁰ This Data Retention Directive was adopted in the aftermath of the terrorist attacks of Madrid in 2004 and of London in 2005. Following these attacks, it had been found that terrorists and other criminals were increasingly relying on ICTs to plan and commit serious crimes. In this context, most Member States had reported that the data collected by PECS played a central role in their criminal investigations. In particular, the retained data provided valuable leads and evidence that could help to convict criminals or, *a contrario*, acquit innocent suspects.⁵¹¹ The Data Retention Directive aimed at harmonizing the obligations of PECS in this respect; it required PECS to retain certain communications data for a period between six months and two years and to make them available, on request,

⁵⁰⁶ *Ibid.*, para. 66.

⁵⁰⁷ González Fuster (2014). *op. cit.*, p. 239.

⁵⁰⁸ CJEU, Judgment of 8 April 2014, *Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12.

⁵⁰⁹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L105, p. 54 (no longer in force – Date of end of validity: 03/05/2006).

⁵¹⁰ Article 1 of the Data Retention Directive (Date of end of validity: 03/05/2006).

⁵¹¹ Commission evaluation report on the Data Retention Directive, COM(2011) 225 final, 18 April 2011, pp. 1-4.

to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism.⁵¹² This obligation only concerned traffic and location data; it did not apply to the content of the communications. Traffic and location data can however help trace and identify the source of a communication, as well as its destination, date, time, duration, or the equipment used. It can also help identifying the name and address of the user, the telephone number of the sender/caller of the recipient/callee, or an IP address for Internet services. Those data therefore make it possible to know the identity of the person with whom a user has communicated, as well as the frequency of their communications over a given period.⁵¹³ Given the facts that personal data could be processed, kept and transferred to the authorities without the knowledge of the individuals concerned, the Data Retention Directive posed clear limitations to the fundamental right to privacy and to the fundamental right to personal data protection.⁵¹⁴ The EU legislator expressly acknowledged the existence of this tension in the preamble of the Directive by affirming that the Directive had been drafted in a manner guaranteeing compliance with the right to privacy and the right data protection.⁵¹⁵

Despite the Data Retention Directive's self-proclaimed compliance with Article 7 and 8 of the Charter however, the CJEU declared that Directive invalid in April 2014 on the basis that it did not meet the principle of proportionality and should have provided more safeguards to protect the fundamental right to privacy and the fundamental right to personal data protection.⁵¹⁶ The validity of the Data Retention Directive was thus analysed in the light of both Article 7 and 8 of the Charter. From the perspective of the emancipation of the right to data protection, it is particularly relevant to note that, in the *Digital Rights Ireland* case, the CJEU did not merge Article 7 and 8 of the Charter in a form of hybrid "*right to privacy with respect to the processing of personal data*",⁵¹⁷ but decided to look into each right distinctly at the different stages of the conducted analysis.

In a first stage, the CJEU analysed whether Article 7 and 8 of the Charter were relevant to rule on the validity of the Data Retention Directive. In this respect, the CJEU stated in particular that "*the retention of data for the purpose of possible access to them by the competent national authorities (...) directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that*

⁵¹² Article 3 and 6 of the Data Retention Directive (Date of end of validity: 03/05/2006).

⁵¹³ CJEU, *Digital Rights Ireland*, para. 26

⁵¹⁴ Kosta, E. (2018). The retention of communications data in Europe and the UK. L. Edwards (Ed.). *Law, policy and the internet*. Hart Publishing, pp. 193-212.

⁵¹⁵ Recital 22 of the Data Retention Directive: "*This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with [the e-Privacy Directive], seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.*" (emphasis added).

⁵¹⁶ CJEU, *Digital Rights Ireland*.

⁵¹⁷ As it had done in the case *Volker und Markus Schecke and Eifert*, discussed above.

article and, therefore, necessarily has to satisfy the data protection requirements arising from that article”.⁵¹⁸ The CJEU therefore concluded that both Article 7 and Article 8 of the Charter were relevant to assess the validity of the Data Retention Directive by referring to their respective scope.

In a second stage, the CJEU analysed whether the Data Retention Directive was causing an interference with Article 7 and 8 of the Charter. In this respect, the CJEU noted that:

- “By requiring the retention of [traffic and location data] and by allowing the competent national authorities to access those data, [the Data Retention Directive] (...) derogates from the system of protection of the **right to privacy** established by [the 1995 Data Protection Directive and the e-Privacy Directive] with regard to the processing of personal data in the electronic communications sector” (emphasis added);
- “Likewise, [the Data Retention Directive] constitutes an interference with **the fundamental right to the protection of personal data** guaranteed by Article 8 of the Charter because it provides for the processing of personal data.”

The CJEU thus distinguished between Article 7 and 8 of the Charter. It further considered that both rights were limited by the Data Retention Directive in a way that was “wide-ranging” and “particularly serious”.⁵¹⁹

Finally, in a third stage, the CJEU analysed whether such a limitation on the exercise of the right to privacy on the one hand, and the fundamental right to data protection on the other hand, could be justified. The Charter gives guidance in this respect, since Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must (i) be provided for by law, (ii) respect their essence, and that (iii) subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet (iv) objectives of general interest or the need to protect the rights and freedoms of others.

Regarding the first criteria (i.e., the limitation must be “provided by law”), the CJEU logically considered that it was met, given that the limitations on the exercise of these rights were provided by an EU Directive. Regarding the second criteria (i.e., the limitation must “respect the essence” of the fundamental rights at stake), the CJEU distinguished between each right:

⁵¹⁸ CJEU, *Digital Rights Ireland*, para. 29.

⁵¹⁹ *Ibid.*, para. 37.

- As far as the fundamental right to privacy was concerned, the CJEU held that, *“even though the retention of data required by [the Data Retention Directive] constitutes a particularly serious interference with [the rights laid down Article 7 of the Charter], it is not such as to adversely affect the essence of those rights given that (...) the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.”* In other words, since the secrecy of the *content* of the messages was respected, the CJEU concluded that the *core* or *essence* of the fundamental right to privacy was preserved;
- As far as the fundamental right to data protection was concerned, the CJEU held that the retention of the communications data would not adversely affect the essence of that right, because the Data Retention Directive stated that certain principles of data protection and data security had to be respected by ICT service providers. The CJEU added in particular that *“[a]ccording to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.”* In other words, the CJEU seems to envisage the *“essence”* of the fundamental right to data protection as consisting of the key principles of data protection (and in particular the principle of data security), and ruled that since the Data retention Directive provided for the respect of such principles, the essence of Article 8 of the Charter was also preserved.

Moving to the next relevant criteria (i.e., *does the legislation at hand meet objectives of legitimate interests or the need to protect the rights of others?*), the CJEU pointed out that the material objective of the Data Retention Directive was to contribute to the fight against serious crime and thus, ultimately, to public security. It therefore concluded that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data *“genuinely satisfies an objective of general interest.”*⁵²⁰

Moving to the last criteria, the CJEU then analysed whether the Data Retention Directive respected the principle of proportionality, in the sense that the retention measures were necessary and appropriate with respect the objective of public security to be achieved.⁵²¹ To assess this, the CJEU had to take into account, *inter alia*, the nature of the rights at issue and the seriousness of the interference.⁵²² In this respect the CJEU ruled that: *“in view of the important role played by the*

⁵²⁰ *Ibid.*, para. 44.

⁵²¹ *Ibid.*, para. 45. According to the settled case-law of the CJEU, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (Case C-343/09 *Afton Chemical*, para. 45; *Volker und Markus Schecke and Eifert*, para. 74; Cases C-581/10 and C-629/10 *Nelson and Others*, para. 71; Case C-283/11 *Sky Österreich*, para. 50; and Case C-101/12 *Schaible*, para. 29)

⁵²² *Ibid.*, para. 47.

*protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by [the Data Retention Directive], the EU legislature’s discretion is reduced, with the result that review of that discretion should be strict.”*⁵²³ Later on in its preliminary ruling, the CJEU also added that **“the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter”**.⁵²⁴ Looking into the provisions of the Data Retention Directive and the seriousness of the interference, the CJEU came to the conclusion that the Directive *“d[id] not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter”*. At the end of the day, the CJEU thus held that the principle of proportionality had not been respected and declared the Directive invalid.⁵²⁵

Although the CJEU ultimately combined the right to data protection and privacy to conclude that the principle of proportionality had been breached, the CJEU did not systematically conflate both rights into one single hybrid right. At various stages of its reasoning indeed, the CJEU differentiated between Article 7 and Article 8 of the Charter when assessing whether the Data Retention Directive was posing a limitation on the exercise of these rights, and whether the respective *“essence”* of these rights had been affected. In that sense, it can be argued that this judgment participated to the emancipation of the right to personal data protection from the yoke of the right to privacy. It is only with respect to the last point that the CJEU decided to couple both rights, stating that the right to personal data protection played an important role for the respect of privacy, and vice versa. Given the elements retained by the CJEU for this last point, it may be the case that the CJEU decided to combine both rights in order to avoid repeating twice the same reasoning, without however annihilating their separate nature. Hence, it can be concluded that this judgment highlights both the distinctiveness and overlap between the scope of the right to privacy on the one side, and of the right to personal data protection on the other side.

2.3.2.4. The Schrems saga (2015 – 2020) – additional evidence of the secondary functionality of EU data protection law

The Schrems saga has led to two preliminary rulings of the CJEU on the question of the lawfulness of transfers of personal data from the EU towards the US. The first judgment was rendered on 6 October 2015 while the second judgment was rendered on 16 July 2020.⁵²⁶ The original dispute involved three parties in particular: Maximilian Schrems (an Austrian citizen, in its capacity as a data subject), Facebook

⁵²³ *Ibid.*, para. 48.

⁵²⁴ *Ibid.*, para. 53.

⁵²⁵ *Ibid.*, para. 71.

⁵²⁶ CJEU, Judgment of 6 October 2015, *Schrems* (Schrems I), Case C-362/1; CJEU, Judgment of 16 July 2020, *Facebook Ireland and Schrems* (Schrems II), Case C-311/18.

Ireland Ltd. (the social media company, in its capacity as controller) and the Irish Data Protection Commission (hereafter, the Irish DPA).

To understand the relevance of this saga with respect to the FRO of EU data protection law, it is first necessary to give a summary of its legal and factual background. According to the 1995 Data Protection Directive, transfers of personal data outside of European Economic Area (EEA) may only take place under certain conditions, with a view of protecting the rights and interests of data subject. In this context, the Commission was given the power to adopt adequacy decisions towards third countries when the latter were considered to offer an adequate level of protection for personal data.⁵²⁷ Granting such an adequacy decision would operate as a green light for international data transfers towards vetted third countries, and could thus facilitate the transfers of personal data from the EU towards these countries. In the absence of an adequacy decision, transfers of personal data from the EU to a third country could only take place under limited circumstances as specified under Article 26 and following of the 1995 Data Protection Directive, for example if the concerned data subjects had given their explicit consent,⁵²⁸ or if the data exporter and importer had entered into Standard Contractual Clauses (SCCs) drafted by the Commission.⁵²⁹

On 26 July 2000, the Commission adopted an adequacy decision vis-à-vis the US. This decision was referred to as the “Safe Harbour” decision.⁵³⁰ Many companies started transferring personal data from the EU to the US based on that mechanism. In the subsequent years however, several affairs, and in particular the Edward Snowden revelations, shed light on the fact that national intelligence agencies in the US, such as the NSA, were intercepting and analysing personal data through programmes of mass surveillance, without offering in return any appropriate safeguards.⁵³¹ Against this background, Maximilian Schrems decided to officially file a complaint against Facebook Ireland Ltd with the Irish DPA in 2013. The complaint was aimed at prohibiting Facebook Ireland from further transferring personal data of EU citizens

⁵²⁷ Article 25 of the 1995 Data Protection Directive.

⁵²⁸ Article 26(1)(a) of the 1995 Data Protection Directive.

⁵²⁹ Article 26(4) of the 1995 Data Protection Directive established that mechanism. The Commission adopted three different sets of SCCs pursuant to that Article in 2001, 2004 and 2010 respectively (Commission Decision 2002/16/EC of 27 December 2001, Commission Decision 2004/915 of 27 December 2004 and Commission Decision 2010/87 of 5 February 2010). On 4 June 2021, the Commission issued modernised SCCs under the GDPR. These modernised SCCs replaced the three sets of SCCs that were previously adopted under the regime of the 1995 Data Protection Directive. The modernised SCCs are available on the website of the Commission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

⁵³⁰ Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) *OJ L 215, 25.8.2000, p. 7–47*.

⁵³¹ Greenwald, G. & MacAskill, E. (2013, June 6). NSA Prism program taps into user data of Apple, Google and others. *The Guardian*; Greenwald, G. & MacAskill, E. (2013, June 8). Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian*; Washington Post (2013, July 10). NSA slides explain the PRISM data-collection program. *The Washington Post*; Snowden E. (2019). *Permanent Record*. Metropolitan Books.

towards Facebook, Inc., i.e., its mother company located in the US, given the alleged involvement of the latter in the mass surveillance programme “PRISM”.⁵³² The Austrian DPA first rejected Mr. Schrems’ complaint, stating that it was frivolous and vexatious. Mr Schrems therefore filed an application for judicial review with the Irish High Court.

On 18 June 2014, confronted to several interpretative issues, the Irish High Court decided to stay the proceedings and to refer several questions to the CJEU for a preliminary ruling. One of the main questions was whether the applicable Austrian data protection law which had transposed the 1995 Data Protection Directive should not be re-evaluated in the light of the subsequent entry into force of Article 8 of the Charter. On 6 October 2015, after analysing those questions and assessing the situation, the CJEU clarified several points with respect to the interpretation of the 1995 Data Protection Directive and, most importantly, declared the ‘Safe Harbour’ decision invalid.⁵³³ The CJEU had indeed found that the Commission had erred in its assessment when adopting an adequacy decision for the US, since the US was neither *de facto* nor *de lege* able to ensure a level of protection essentially equivalent to that guaranteed in the EU for data subjects, given their insufficient data protection laws, intrusive surveillance practices and difficulty challengeable enforcement system.

The case was however far from coming to an end, neither at the EU not at the national level. At the EU level, first, the invalidation of the Safe Harbour mechanism led the Commission to rapidly re-negotiate with the US a new transfer mechanism, and to adopt a second adequacy decision which established a new system for transfers towards the US, referred to as the “EU-US Privacy Shield”.⁵³⁴ This EU-US Privacy Shield established, *inter alia*, a Privacy Shield Ombudsperson, whose role was to facilitate the dialogue with EU data subjects in the event of a breach of EU data protection law by an US data importer (a novelty compared to the Safe Harbour decision). At the national level, despite the clear-cut judgment of the CJEU, the Irish DPA did not adopt a final decision with respect to the complaint of Maximilian Schrems, mainly because the lawfulness of the transfers from Facebook Ireland to Facebook US were not exclusively depending on the validity of the Privacy Shield. Indeed, in the aftermath of the *Schrems II* decision, Facebook Ireland started arguing that they were not relying on any adequacy decision for transferring personal data to their US headquarters, but rather on SCCs. Being unsure about the actions to be taken against Facebook Ireland, the Irish DPA brought a new action before the Irish High Court and asked the latter to refer another set of questions to the CJEU. On 4 May 2018, the Irish High Court agreed to this request and referred 11 questions to the CJEU, including on the validity of the SCCs as a transfer mechanism intended to

⁵³² *Ibid.*

⁵³³ CJEU, *Schrems I*, Case C-362/14.

⁵³⁴ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance).

guarantee an appropriate level of protection for personal data. The CJEU then rendered a second judgement on July 16, 2020, commonly referred to as *Schrems II*. In this judgment, the CJEU upheld the validity of the SCCs but invalidated the Privacy Shield decision, which it found incompatible with Article 7, 8 and 47 of the Charter.

Although the Schrems saga is very interesting at different levels, it is particularly relevant to note that the CJEU centred its reasoning around three different fundamental rights enshrined in the Charter: (1) the right to privacy; (2) the right to personal data protection, and (3) the right to an effective judicial remedy and to a fair trial (Article 47 of the Charter). It was stressed by the CJEU in particular that, once a data transfer towards the US would occur, data subjects had little chance to have their claim heard and to obtain a remedy before the US courts, should an infringement of EU data protection rules occur in the US. The CJEU found *inter alia* that, even with the introduction of the Privacy Shield Ombudsperson, there was no reasonable possibility for individuals to pursue legal remedies in order to have access to their personal data, or to obtain the rectification or erasure of such data. Based on these considerations, the CJEU therefore declared that the adequacy decision adopted by the Commission was invalid, and that transfers of personal data from the EU to the US based on that decision would not respect the “*essence*” of Article 47 of the Charter.⁵³⁵

In the context of this study, the main take-away from both the *Schrems I* and *Schrems II* judgment is thus the fact that EU data protection law was interpreted and applied not only for the benefit of the right to privacy and the right to personal data protection, but also the right to an effective remedy and fair trial, as protected under EU law, thereby partially materialising the secondary functionality of EU data protection law with respect to its FRO.

A second important take-away is that the CJEU concluded that the interference with the right to privacy, data protection and effective remedy, in the context of data transfers to the US, was so obviously disproportionate that it was encroaching the *essence* of these rights.⁵³⁶ As a result, the CJEU did not enter into long debates on whether these interferences could be considered as “*provided by law*”, “*necessary*” or “*proportionate*” under Article 52 of the Charter, but straightforwardly concluded to the invalidity of the adequacy decisions adopted by the Commission. In the opinion of the author, this reflects the bloating effect that the dialogue that is taking place between, on the one side, EU secondary law in the field of data protection and, on the other side, the Charter of Fundamental Rights, can have on the level of protection afforded to the fundamental rights and freedoms of data subjects. The effect of this dialogue and its impact on the functionality of EU data protection law will further be discussed in the final Chapter of this Study.

⁵³⁵ CJEU, *Schrems I*, Case C-362/14, para. 95 and *Schrems II*, Case C-311/18, para. 187.

⁵³⁶ Brkan, M. (2019b). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning. *German Law Journal*, 20(6):864-883.

2.3.3. GDPR era: towards a more multi-functional use of EU data protection law?

All the CJEU rulings discussed above (at the exception of Schrems II) were rendered before the 25th of May 2018, i.e., before the GDPR started applying in the EU. As further analysed below, the GDPR era is marked by an increasing number of cases where the right to an effective remedy (Article 47 of the Charter) and freedom of expression (Article 11 of the Charter) benefited from the interpretation of EU data protection law. These cases have thus shed additional light on the secondary functionality of EU data protection law and contributed to the fulfilment of its broad FRO. To illustrate this evolution, two preliminary rulings rendered by the CJEU in the GDPR era will be discussed here below. A third important preliminary ruling where EU data protection law was used to enhance consumer protection in the digital sphere will further be discussed in a subsequent Chapter of this study.⁵³⁷ Finally, in the next and final section of this Chapter, a table providing a general overview of the case-law of the CJEU in the field of EU data protection law will be used as a basis to show and discuss the gradual blooming of the primary and secondary functionality of the GDPR.

2.3.3.1. Telecommunication surveillance cases in the UK, France and Belgium

On 6 October 2020, the CJEU rendered two related judgments in the case *Privacy International*,⁵³⁸ on the one hand, and in the joined cases *La Quadrature du Net* and *Ordre des barreaux francophone et germanophone*,⁵³⁹ on the other hand. In both judgments, the CJEU clarified that EU data protection law, read in the light of the Charter, precludes national legislation requiring providers of electronic communications services to carry out general and indiscriminate transmission of traffic data and location data to public authorities or security and intelligence agencies for public security purposes. The national legislation at stake were respectively adopted in the UK, France and Belgium; they each laid down a general obligation for providers of electronic communications services ('PECS') to forward users' traffic data and location data to a public authority, or to retain such data in a general or indiscriminate way for the purpose of preventing or combatting serious crimes and safeguarding national security. The traffic and location data to be collected by PECS did not include the content of communications but would still allow to form a picture of the '*who, where, when and how*'⁵⁴⁰ of a communication. Hence, these data qualified as personal data under EU data protection law. In each of these Member States, public society challenged the concerned national law; in the

⁵³⁷ See in particular Section 3.3.2.3, on the CJEU judgment of 28 April 2022 in the case C-319/20 *Meta Platforms Ireland*.

⁵³⁸ CJEU, Judgment of 6 October 2020, *Privacy International*, Case C-623/17.

⁵³⁹ CJEU, Judgment of 6 October 2020 *La Quadrature du Net* and *Ordre des barreaux francophone et germanophone*, Joined Cases C-511/18 and C-520/18.

⁵⁴⁰ CJEU, *Privacy International*, para. 23.

UK, this challenge was brought by the NGO *Privacy International*; in France, by the NGO *La Quadrature du Net*, and in Belgium, by the French- and German-speaking Bar Association. In that context, the national courts competent to determine the compatibility of these national laws with EU law, and in particular with the e-Privacy Directive, referred several questions to the CJEU.

As far as the right to privacy and personal data protection were concerned, the CJEU considered that the transmission of traffic data and location data to a third party constitutes an interference with these rights, regardless of how that data is subsequently used.⁵⁴¹ The CJEU further found that such an interference must be regarded as being particularly serious, bearing in mind, in particular, “*the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications.*”⁵⁴² As far as freedom of expression was concerned, the CJEU pointed out that allowing such practice was likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance.⁵⁴³ In the opinion of the CJEU, this could further deter users of means of electronic communication from exercising their freedom of expression as guaranteed in Article 11 of the Charter.⁵⁴⁴ It is particularly interesting to note that the concerns of the CJEU in this respect were aggravated as far as some actors playing an important role in democratic societies would be affected, such as whistle-blowers, journalists, lawyers, and other persons subject to an obligation of professional secrecy. Blanket surveillance could indeed lead to the muzzling of these actors; a risk that was “*all the more serious given the quantity and breadth of the data retained*”.⁵⁴⁵ Having regard to Article 52(1) of the Charter, the CJEU found that such an interference with freedom of expression could not be considered as proportionate to the legitimate aim pursued (i.e., the prevention and combatting of serious crimes) in the absence of specific safeguards restricting ad framing the collection and use of these data to what it was strictly necessary.⁵⁴⁶ The fact, in particular, that a national legislation could allow for the indiscriminate and general retention of the personal data of thousands of users of electronic communication services, despite the absence of any link between the conduct of these persons and the objective pursued by the legislation at issue, was considered problematic from the perspective of the principle of proportionality.⁵⁴⁷ By contrast, the CJEU admitted that if a Member State would be facing a serious threat to national security that proved to be genuine and present or foreseeable, the e-Privacy directive, read in the light of the Charter, would not preclude recourse to an order requiring providers of electronic communications services to retain traffic data and location data, on the condition that the order in question would (i) define a

⁵⁴¹ CJEU, *Privacy International*, para. 70.

⁵⁴² *Ibid.*, para. 71.

⁵⁴³ *Ibid.*

⁵⁴⁴ *Ibid.*, para. 72.

⁵⁴⁵ *Ibid.*

⁵⁴⁶ *Ibid.*, para. 76.

⁵⁴⁷ *Ibid.*, para. 80.

period of retention that is limited in time to what is strictly necessary, and (ii) be subject to effective review either by a court or by an independent administrative body, in order to verify that the order in question would respect the applicable safeguards and would not lead to abuses.⁵⁴⁸

From the perspective of the research question of this study, it can thus be concluded that this judgment contributes to revealing the secondary functionality of EU data protection law, given that the e-privacy Directive was interpreted by the CJEU with the explicit aim to protect not only the right to privacy and the right to personal data protection of the users of electronic communication services, but also freedom of expression. The fact, in particular, that the CJEU highlighted the deterrent effect that broad and indiscriminate surveillance measures could have on the freedom of expression of specific individuals, such as whistle-blowers or persons subject to an obligation of professional secrecy, is particularly interesting. Indeed, rather than assessing the lawfulness of the automated processing of personal data 'in theory', the CJEU took into considerations its broader and long-term effects on individuals' rights and freedoms, before interpreting the e-Privacy directive in a functional way to prevent negative effects on freedom of expression 'in practice'.

2.3.3.2. Facebook Ireland and Others – a reasoning articulated around the broad FRO of EU data protection law

The judgment of the CJEU in the case *Facebook Ireland and Others*, which finds its origin in a dispute before the Belgian courts opposing the social media company Facebook to the Belgian DPA,⁵⁴⁹ offers yet another example of the increasing recognition afforded to the broad FRO of the GDPR. On 11 September 2015, the Belgian DPA brought legal proceedings seeking an injunction against Facebook Ireland, Facebook Inc. and Facebook Belgium before the Brussels Court of First Instance (the Brussels CFI). The object of those injunction proceedings was to force Facebook to stop collecting data on the browsing behaviour of both Facebook account holders (i.e., Facebook users) and persons who did not have an account with Facebook (i.e., non-users) but still accessed one of Facebook's publicly available pages or a third-party's website containing Facebook 'plugins-in'.⁵⁵⁰ The collected data included users and non-users' IP address, date and time of visit, and URL of the visited pages. Facebook was collecting these data by means of various DDTs, such as

⁵⁴⁸ CJEU, *La Quadrature du Net and Ordre des barreaux francophone et germanophone*, paras. 137-139.

⁵⁴⁹ The original parties to this dispute were Facebook (known today as Meta) and the President of the Belgian DPA (rather than the DPA itself, as the latter still lacked legal personality at the time and could thus not have brought these legal proceedings). For the sake of clarity, however, the author of this study will refer to 'Facebook' and the 'Belgian DPA'.

⁵⁵⁰ Facebook social plugins, which include the 'Like' button, the 'Share' button and comments, are tools that can be embedded on third parties' website and that allow internet users to share their experiences with their friends on Facebook although they are not navigating one of Facebook' websites (source: Facebook.com, Help Center). For example, one may be able to read a news article on the website of a media company and to like such article by clicking on Facebook 'Like' button, when such a button has been voluntarily embedded by the media company on its website.

cookies and social plug-ins.⁵⁵¹ As far as cookies were concerned, it was found that their specific type allowed them to remain 'active' for two years on the users' device.⁵⁵²

On 16 February 2018, the Brussels CFI held that it had jurisdiction over the case. On the substance, the Brussels CFI held that Facebook was not adequately informing Belgian internet users of the collection and use of their personal data, regardless of whether they were Facebook users and non-users. Consequently, Facebook was ordered to desist from placing cookies and from collecting data by means of social plug-ins, pixels or similar technological means on third-party websites, without asking for the valid consent of the internet users concerned, (ii) to desist from providing information that might reasonably mislead the data subjects as to the real extent of the mechanisms put in place by Facebook for the use of cookies, and (iii) to destroy all the personal data obtained by means of cookies and social plug-ins.⁵⁵³

Facebook brought an appeal against that judgment before the Court of Appeal of Brussels, which considered that it had jurisdiction over the case as far as Facebook Belgium was concerned. As part of its preliminary arguments, Facebook Belgium claimed however that the Belgian DPA had no right to bring such an action given the existence of the 'one-stop shop' mechanism provided under Article 56 GDPR. In particular, Facebook argued that only the Irish DPA (the Data Protection Commissioner or 'DPC') was competent to bring injunction proceedings against Facebook Ireland, the latter being the sole controller of the personal data of the users located within the EU. According to Article 56 GDPR, in the event of cross-border processing activities, it is indeed the DPA of the Member State where the main establishment of the controller is located that is competent to act as the 'lead supervisory authority' (hereafter referred to as the '**lead DPA**'). In this context, the Court of Appeal of Brussels decided to stay the proceedings and to refer several questions to the CJEU with respect to the 'one-stop shop' mechanism and the possibility for the Belgium DPA to still bring an action against Facebook Belgium, despite Facebook Ireland having been identified as the main controller, and thus the Irish DPA as the lead DPA for this cross-border case.

In its judgment, the CJEU recognised that the one-stop-shop mechanism was limiting the possibility for DPAs to handle a cross-border case when the controller in charge of the litigious processing activities was located on the territory of another Member State. The CJEU found that such a limitation was in principle still compatible with Article 7, 8 and 47 of the Charter, given that enforcement could still be carried out by the lead DPA with a view of ensuring the effective respect of the fundamental rights and freedoms of data subjects.⁵⁵⁴ Yet, the CJEU also recognised that the use of the

⁵⁵¹ CJEU, *La Quadrature du Net and Ordre des barreaux francophone et germanophone*, paras. 29-30.

⁵⁵² *Ibid.*, para. 32.

⁵⁵³ *Ibid.*

⁵⁵⁴ Article 67 GDPR.

'one-stop shop' mechanism should not, under any circumstances, have the consequence that *"a lead [DPA] does not assume the responsibility incumbent on it to contribute to providing effective protection of natural persons from infringements of their fundamental rights (...), as otherwise that consequence might encourage the practice of forum shopping, particularly by data controllers, designed to circumvent those fundamental rights and the practical application of the provisions of that regulation that give effect to those rights."*⁵⁵⁵

The CJEU further highlighted multiple scenarios where the GDPR, read in the light of the Charter, would still allow a DPA *that is not the lead DPA* to bring action against a controller before the courts of its own Member States, including:

- when the lead DPA fails to provide another DPA with information pursuant to the cooperation mechanism provided under Article 60 GDPR; the CJEU admits that, in that situation, the other DPA may adopt a provisional measure on the territory of its own Member State;
- when the lead DPA does not comply with the obligations for mutual assistance imposed on it by Article 61 GDPR; in this case, another DPA may ask the EDPB to render an opinion or decision, following which the other DPA could, with the approval of the EDPB, take the necessary measures to ensure compliance with the GDPR and, for that purpose, take legal action against a controller before the courts of its own Member State.

It clearly appears from this judgment that the CJEU articulated its reasoning around the FRO of the GDPR, guided by the willingness to ensure the effective protection of the rights and freedoms of data subjects, and in particular the rights guaranteed by Article 7, 8 and 47 of the Charter. Adopting a functional approach, the CJEU therefore concluded that a national DPA that is not the lead DPA can still take action against a controller in the context of a cross-border case, when it appears that the inaction or lack of cooperation of the lead DPA renders the 'one-stop-shop' mechanism ineffective and puts at risk the rights and freedoms of data subjects. The explicit reference to Article 47 of the Charter – i.e., the right of individuals to an effective remedy –, and to the need to prevent controllers from practicing forum shopping to escape liability, tends to confirm once again that the GDPR should not be envisaged as a tool to be interpreted and used solely for the protection of the right to privacy or personal data protection of individuals, but also for other fundamental rights, including the right to an effective remedy as guaranteed by Article 47 of the Charter.

⁵⁵⁵ CJEU, *La Quadrature du Net and Ordre des barreaux francophones et germanophone*, para. 68.

2.3.4. Concluding remarks: understanding the potential causes behind the shortfall in the secondary functionality of EU data protection law

Looking at the letter of the law, the explicit objective of EU data protection law is clear: the aim of that legislation is to protect *all* the fundamental rights and freedoms of individuals in the context of the processing of their personal data.⁵⁵⁶ Although such wording may have been the result of a legal tradition,⁵⁵⁷ it shaped EU data protection law into the human-centred and technology-neutral framework that it became today. As previously shown in the historical review of this study (section 2.2), the inclusion of such a broad FRO, both in the 1995 Data Protection Directive and in the GDPR, was a logical legislative choice given the fast evolution of new DDTs which were putting various fundamental rights and freedoms at risk of severe interferences, often in previously unforeseen ways. Over the years, the CJEU gave flesh to this FRO by almost systematically interpreting EU data protection law for the benefit of privacy and data protection, and lately also for freedom of expression and various procedural rights, as illustrated by the selection of cases summarized here above. In the opinion of the author, there is thus no doubt that EU data protection law has both the legitimacy and the potentiality of becoming a multifunctional framework for the defence of data subjects' fundamental rights against potentially harmful data processing practices, even if such multi-functionality still appears underexploited, as further discussed below.

2.3.4.1. Overview of the fulfilment of the FRO of EU data protection law within the case law of the CJEU

To give a visual overview of the fulfilment of the primary and secondary functionality of EU data protection law, the below table lists in a chronological order most of the preliminary rulings rendered by the CJEU between May 2003 and June 2022 on the interpretation to be given to the 1995 Data Protection Directive, the e-Privacy Directive and the GDPR.⁵⁵⁸ Judgments that do not contain any reference to fundamental rights or the Charter have been marked by 'N/A'. When a judgment has not (yet) been published, it is marked as 'NP'.

The below overview of the case-law of the CJEU in the field of data protection shows that, so far, EU data protection law has generously been interpreted and applied for the benefit of the fundamental rights to privacy and/or the fundamental right to personal data protection of data subjects. It can therefore be argued that the

⁵⁵⁶ Today, Article 1(2) of the GDPR states: "*This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*".

⁵⁵⁷ EU legislation must, by default, respect the fundamental rights of individuals as enshrined under the Charter (in the sense that the non-conformity of an EU act with fundamental rights protection is a ground for invalidating such an act). Hence, it is common to find, in an EU act, a reference according to which the given act respects the fundamental rights and freedoms enshrined in the Charter. And from a commitment to 'respect' to the objective of 'protecting' fundamental rights, there is only one step to take.

⁵⁵⁸ Judgments of the CJEU against Member States for failure to transpose or properly implement EU legislation in matters of data protection have been left out.

'primary functionality' of EU data protection law is sufficiently evidenced. The GDPR era also shows a surge of cases where EU data protection law is interpreted and applied for the benefit of one or multiple different fundamental rights ('**DFR**'), including the right to an effective judicial remedy, freedom of expression and, more recently, consumer protection. Yet, these DFR seem to be under-represented, such as non-discrimination, and some are simply missing from this case-law, such as the right to the integrity of the person. As a consequence, one may wonder whether EU data protection law would not still suffer from a shortfall with respect to the fulfilment of its FRO, as further discussed below.

TABLE 2

The below table gives an overview of the case-law of the CJEU in the field of data protection between May 2003 and August 2022, based on the nomenclature of the official website of the CJEU, i.e. curia.eu. If the judgment of the case in question contains an explicit reference to Article 8 ECHR or Article 7 of the Charter, and/or to Article 8 of the Charter, and/or to any other Article of the Charter (i.e. to a DFR), it is indicated and highlighted in green. If the judgment mentions an AFR, the latter is named in the relevant column. The table is divided in three eras corresponding to the effective date of application of three important instruments of EU law: the Charter (as from December 2000), the Lisbon Treaty (as from 1 December 2009) and the GDPR (as from May 2018).

		PRIVACY	PERSONAL DATA PROTECTION	ALTERNATIVE FUNDAMENTAL RIGHT(S)
POST ADOPTION OF THE CHARTER				
1.	Rundfunk (20 May 2003)	Article 8 ECHR	No	No
2.	Lindqvist (6 November 2003)	Article 8 ECHR	No	No
3.	Esch-Leonhardt (18 February 2004)	N/A	N/A	N/A
4.	Bank Austria Creditanstalt (30 May 2006)	N/A	N/A	N/A
5.	Nikolaou (12 September 2007)	Yes	Mere mention	No
6.	Bavarian Lager (8 November 2007)	Yes	Mere mention	No
7.	Promusicae (29 January 2008)	Yes	Mere mention	No
8.	Satamedia (16 December 2008)	Yes	No	No
9.	Huber (16 December 2008)	No	No	Equal treatment / non-discrimination
10.	LSG (19 February 2009)	Yes	No	No
LISBON ERA				
11.	Bav. Lager II (29 June 2010)	Yes	No	No
12.	Volker und Markus Schecke and Eifert (9 November 2010)	Yes	Yes	No
13.	Deutsche Telekom (5 May 2011)	No	Yes	No
14.	V v Parlement (5 July 2011)	Yes	No	No
15.	Valero Jordana (7 July 2011)	N/A	N/A	N/A
16.	Dennekamp I (23 November 2011)	Yes	No	No
17.	ASNEF and FECEMD (24 November 2011)	Yes	Yes	No
18.	Scarlet Extended (24 November 2011)	No	Yes	No
19.	SABAM (16 February 2012)	No	Yes	No
20.	Egan and Hackett (28 March 2012)	N/A	N/A	N/A
21.	Bonnier Audio (19 April 2012)	N/A	N/A	N/A
22.				
23.	Worten	N/A	N/A	N/A

	(30 May 2013)			
24.	Schwarz Case C-291/12 (17 October 2013)	Yes	Yes	No
25.	IPI (Englebert) (7 November 2013)	Yes	Yes	No
26.	X (12 December 2013)	Yes	Yes	No
27.	Digital Rights Ireland (8 April 2014)	Yes	Yes	Freedom of expression
28.	Google Spain (13 May 2014)	Yes	Yes	No
29.	YS e.a. (17 Juillet 2014)	Yes	Yes	Right to good administration
30.	František Ryneš (11 December 2014)	Yes	No	No
31.	McCullough (11 June 2015)	Yes	No	No
32.	Dennekamp II (15 July 2015)	Yes	No	No
33.	ClientEarth and PAN Europe v EFSA (16 July 2015)	N/A	N/A	N/A
34.	Bara (1 October 2015)	N/A	N/A	N/A
35.	Weltimmo (1 October 2015)	N/A	N/A	N/A
36.	Schrems I (6 October 2015)	Yes	No	Right to an effective judicial remedy
37.	Verein für Konsumenteninformation (28 July 2016)	N/A	N/A	N/A
38.	Breyer (19 October 2016)	N/A	N/A	N/A
39.	Tele2 Sverige (21 December 2016)	Yes	Yes	Freedom of expression
40.	Salvatore Manni (9 March 2017)	Yes	No	No
41.	Tele2 (Netherlands) (15 March 2017)	Yes	Yes	No
42.	Rīgas satiksme (4 May 2017)	N/A	N/A	N/A
43.	Puškár (27 septembře 2017)	Yes	No	No
44.	Nowak (20 December 2017)	N/A	N/A	N/A
GDPR ERA				
45.	Wirtschaftsakademie (5 June 2018)	Yes	Yes	No
46.	Jehovan todistajat (10 July 2018)	N/A	N/A	N/A
47.	Ministerio Fiscal (2 October 2018)	Yes	No	No
48.	Buivids (14 February 2019)	Yes	Yes	No
49.	Fashion ID (29 July 2019)	N/A	N/A	N/A
50.	Google - Territorial scope of the right to de- referencing (24 September 2019)	Yes	Yes	No
51.	GC and Others (24 September 2019)	Yes	Yes	No
52.	Land Hessen (9 July 2020)	N/A	N/A	N/A
53.	Schrems II	Yes	Yes	Right to an effective judicial remedy

	(16 July 2020)			
54.	Orange Romania (11 November 2020)	N/A	N/A	N/A
55.	Privacy International (6 October 2020)	Yes	Yes	Freedom of expression
56.	La Quadrature du Net and Others (6 October 2020)	Yes	Yes	Freedom of expression
57.	J & S Service (10 December 2020)	N/A	N/A	N/A
58.	H.K. (2 March 2021)	Yes	Yes	Freedom of expression
59.	Facebook Ireland and Others (15 June 2021)	Yes	Yes	Right to an effective judicial remedy
60.	Ligue des droits humains (21 June 2022)	Yes	Yes	Non-discrimination; Freedom of movement and of residence; Principles of legality and proportionality of criminal offences and penalties
61.	Latvijas Republikas Saeima (22 June 2021)	NP	NP	NP
62.	Kočner v EUROPOL (29 September 2021)	Yes	Yes	Right to good administration; Presumption of innocence
63.	Valsts ieņēmumu dienests (24 February 2022)	NP	NP	NP
64.	Autoriteit Persoonsgegevens (24 March 2022)	N/A	N/A	N/A
65.	Meta Platforms Ireland (28 April 2022)	No	Yes	Consumer protection
66.	Leistrizt (22 June 2022)	N/A	N/A	N/A
67.	Chief Ethics Commission (1 August 2022)	Yes	Yes	N/A

Looking at this table, the primary functionality of EU data protection law appears well evidenced. By contrast, the secondary functionality of EU data protection seems to lack behind. In the pre-Lisbon era, EU data protection law was never interpreted by the CJEU for the benefit of a fundamental right other than privacy, with the notable exception of *Huber*, where prohibition of discrimination on the ground of nationality was at stake.⁵⁵⁹ In the Lisbon era, there has been a small increase in the number of cases where EU data protection law was invoked to defend DFR, and in particular the right to an effective judicial remedy (Article 47 of the Charter),⁵⁶⁰ or freedom of expression (Article 11 of the Charter).⁵⁶¹ This trend was further confirmed and reinforced two years after the GDPR became applicable in the EU; in the years 2020 and 2022, in particular, no less than eight judgments from the CJEU participated to the protection of DFR through the interpretation and application of EU data protection law. All in all, it thus seems that the multi-functionality of EU data protection law is increasingly being exploited. Yet, one must also admit that this multi-functionality has so far remained confined to a few ‘lucky’ DFR, such as freedom of expression and procedural rights. By contrast, the CJEU has never interpreted or applied EU data protection law to protect other individual rights

⁵⁵⁹ As protected today under Article 21 of the Charter.

⁵⁶⁰ Article 47 of the Charter.

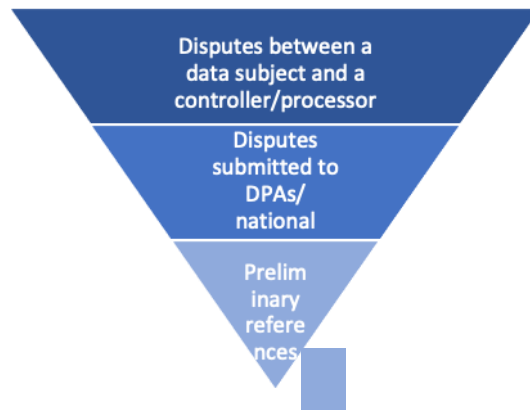
⁵⁶¹ See, in particular, CJEU judgments in *Tele2 Netherlands*, *Digital Rights Ireland*, *Privacy International*, *La Quadrature du Net and Ordre du barreau francophone et germanophone*, as well as *H.K.*

which have proven vulnerable to modern data processing practices, such as, for example, the right to integrity in the context of online harassment or non-discrimination in the context of algorithmic decision-making. One may therefore wonder whether EU data protection law is truly multi-functional for the defence of data subjects' fundamental rights, or whether it may somehow suffer from a shortfall.

2.3.4.2. The national roots of the shortfall of the secondary functionality of EU data protection law

Before reflecting on the potential causes behind the potential shortfall of EU data protection law in terms of fundamental rights protection, it must first be acknowledged that the case-law of the CJEU only represents a *part* of the overall body of binding decisions that have been taken with respect to the interpretation and application of EU data protection law. At a lower level, the case-law of national courts as well as the decisions taken by national data protection authorities (DPAs) might offer a different picture. It may be the case indeed that, at the national level, an increasing number of cases involving the violation of DFR are being discussed in light of the GDPR or other data protection laws. Reviewing the entire corpus of national case-law in the 27 Member States would however go beyond the scope of this study. Furthermore, although the above-mentioned case-law of the CJEU may indeed just be the tip of the iceberg, the author believes that it offers a realistic picture of the overall fulfilment of the FRO of EU data protection law for at least three reasons.

First, it can reasonably be assumed that the case-law of the CJEU, even if it does not offer a perfect reflection of national case-law, is representative of what is happening at the level of the Member States. A large majority of the judgments of the CJEU in the field of data protection law are indeed rendered in the context of the preliminary ruling procedure, as foreseen under Article 267 of the TFEU. Under this procedure, national courts have the opportunity and/or duty to refer questions to the CJEU regarding the interpretation to be given to EU law when a doubt arises in the context of a judicial dispute. This means that the CJEU may not pick and choose specific cases where an interpretative issue has arisen but is bound to answer questions referred to it by national courts. Rather than being the 'tip of the iceberg', the case-law of the CJEU in the field of data protection can thus be considered as the result of a filtration process. Hence, the shortfall in the fulfilment of the FRO of EU data protection law at the CJEU level is likely to find its source in national case-law.



Second, it can be argued that this shortfall does not only find its origin in national case-law, but it is even likely to be more sizeable at the level of national courts. There are indeed no specific procedural or structural obstacles that would prevent data protection cases whose focus is on a DFR to be brought to the attention of the EU judges. By contrast, the doctrine of the '*acte clair*'⁵⁶² could ultimately lead to an *under*-representation of data protection cases relating to Article 7 and 8 of the Charter, given that the CJEU has already rendered various judgements on the interpretation to be given to EU data protection law in light of those two rights. Hence, national judges may decide not to submit similar or identical cases to the CJEU, while being more likely to refer preliminary questions on the interpretation to be given to EU data protection law with respect to the need to ensure the respect of DFR against modern and potentially harmful data processing practices.

Third, for the sake of certainty, the author of this study looked into another sample of case-law at the national level, and in particular the most important administrative fines imposed by national DPAs between 2019 and 2021. The purpose was to find *prima facie* evidence that the shortfall identified at the EU level originated from the Member States. A review of the facts and of the legal grounds based on which the 100 most important DPAs' fines were imposed tends to confirm that, so far, national bodies have also primarily interpreted and applied EU data protection law with a view of protecting the right to privacy and/or personal data protection of the data subjects.⁵⁶³ In a large majority of these cases indeed, both the initial complaint by the data subject and the reasoning of the data protection authorities revolved around the need to protect individuals against any breach of the applicable data protection rules which could interfere with their right to respect for their private and family life,

⁵⁶² According to this doctrine, national courts do not have to refer to the CJEU a preliminary question on the interpretation of EU law if the answer to the question is clear, for example, because the CJEU has already answered that question in the past in the context of a similar or identical case. This doctrine was established by the CJEU itself in the landmark case *CILFIT* (CJEU, Judgment of 6 October 1982, *CILFIT / Ministero della Sanità*, C-283/81). See, on this subject, Fenger, N. & Broberg, M. (2011). Finding Light in the Darkness: On the Actual Application of the *acte clair* Doctrine', *Yearbook of European Law*, 30(1):180–212; Kornezov, A. (2016). The new format of the Acte Clair doctrine and its consequences. *Common Market Law Review*, 53(5):1317–1342.

⁵⁶³ This statement is based on an analysis by the author of this study of the main grounds of the 100 most substantial fines imposed by DPAs until October 2022, as listed on <https://www.enforcementtracker.com/>. This website is managed by CMS (Law/Tax), which collects itself information from various official sources, including the decision of the DPA themselves, when available. The main ground for the decision and the link to the original decision or the relevant source is included in this tracking tool.

or their right to be informed and have control over their personal data. In particular, a majority of these fines have been imposed for lack of compliance with the obligation of controllers and processors to (i) have a valid legal basis for processing personal data,⁵⁶⁴ (ii) to ensure a proper level of data security, and/or (iii) to properly inform the data subjects about the processing of their personal data.⁵⁶⁵ These three types of obligations are deeply rooted in the right to privacy and personal data protection of the data subjects as enshrined in Article 7 and 8 of the Charter, to which the DPAs sometimes refer. By contrast, none of these fines were imposed, for example, for a violation of the principle of non-discrimination in the context of automated individual decision making, or for a violation of the right to consumer protection in the context of misleading behavioural targeting, with the potential notable exception of the fine of 746 million EUR imposed by the CNPD on Amazon for unlawful processing of Amazon's users data, who are also (prospective) consumers.⁵⁶⁶

As further discussed in the last Chapter of this study, however, these last two years are also marked by an increased number of decisions from some DPAs, and in particular the Spanish and Italian DPAs, where DFR seem to benefit from the enforcement of EU data protection law. This could be interpreted as a growing trend among DPAs to acknowledge and exploit the multi-functional nature of EU data protection law for the fulfilment of its FRO. All in all, however, the analysis of this second sample of data protection case-law also tends to confirm that EU data protection law has so far mainly been mobilised for the benefit of Article 7 and 8 of the Charter, while a shortfall seems to persist with respect to its secondary functionality.

2.3.4.3. Potential causes behind the shortfall of the secondary functionality of EU data protection law

The word 'shortfall' can be defined as "*an amount that is less than the level that was expected or needed*".⁵⁶⁷ A shortfall in the number of cases where EU data protection law has been concretely used for the defence of DFR can thus mean two very different things: first, it could mean that the number of cases where a data processing practice has put a risk a DFR is *not as high as expected* in the EU (cf. DFR are not substantially being put at risk by data processing activities); second, it could mean that EU data protection law, despite its broad objective, is ill-fitted for combatting

⁵⁶⁴ Articles 6 to 10 of the GDPR.

⁵⁶⁵ Articles 13 and 14 of the GDPR.

⁵⁶⁶ A very brief acknowledgment of the existence of this decision has been published by the CNPD on its website (see <https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html>). This decision has however not been published, and the CNPD has refused to communicate it to the author of this study for research purpose. In its refusal decision, the CNPD has invoked multiple exceptions contained in the Luxembourg law on access to administrative documents, and in particular the exception relating to the existence of an on-going procedure, given that Amazon has appealed the CNPD's decision before the Administrative Tribunal of Luxembourg.

⁵⁶⁷ Cambridge dictionary (online).

violations of DFR by data controllers or processors, in the sense that EU data protection law does not function *as needed* (cf. potential lack of secondary functionality). Based on this important distinction, three main causes may be postulated to explain this apparent shortfall in the fulfilment of the broad FRO of EU data protection law.

First, this perceived shortfall in the fulfilment of the FRO of EU data protection law could be interpreted as a sign that **data processing activities are mainly putting at risk the fundamental rights to privacy and data protection of data subjects but would rarely interfere with other fundamental rights**. In other words, data processing practices would, by nature, be more likely to affect the right to privacy and data protection of the data subjects rather than DFR, and this, even in the face of modern data-driven technologies. If this is true, disputes opposing a data subject to a data controller with respect to the violation, by the latter, of a DFR would more rarely reach national courts, and even less the CJEU. This first potential reason, although plausible, has however already been partly rebutted in the Introduction of this study. It has been shown indeed that the exponential shift from atoms to bits and the emergence of modern DDT have brought new challenges for the protection of fundamental rights in the digital sphere, including for the right to due process, non-discrimination or freedom of expression.

Second, this perceived shortfall could be interpreted as a sign that **EU data protection law is not functional enough when it comes to protecting rights and freedoms other than privacy or personal data protection**. In this respect, it must indeed be recalled that the first data protection laws that were adopted in the 60s and the 70s were primarily meant to protect the right to respect for private and family life of European citizens against mass surveillance by state authorities. These national laws were thus specifically designed to protect the right to privacy and personal data protection of individuals. The different legal instruments which were later adopted by the EU in the field of data protection are the historical products of these laws, and they therefore share the same DNA. It may thus be the case that EU data protection law is functional for protecting the right to privacy and the right to personal data protection of individuals (primary functionality) but is ill-fitted when it comes to ensuring the respect of DFR (secondary functionality). This could explain why current data protection rules are more rarely invoked, interpreted or applied by the CJEU, national courts or DPAs with a view to solve situations where data processing activities would infringe, for example, the right to integrity, the right to vote, consumer protection, non-discrimination or another fundamental right. If that would be true, this would mean that EU data protection law would not be a multi-functional framework for the protection of the fundamental rights of data subjects, but rather a bi-functional framework, in the sense that only the fundamental rights to privacy and data protection would truly benefit from it.

Third, this perceived shortfall could be interpreted as a sign that **data subjects – as well as data protection authorities, NGOs, interest groups and other stakeholders – have not yet comprehended the full potential and multi-functionality of EU data protection law, and have thus failed to rely on these rules in instances where they could have potentially been applied for protecting DFR.** This would imply that EU data protection law *could* be an effective and multi-functional tool for fundamental rights protection, if only the concerned actors would mobilise it for the defence of DFR. To some extent, this potential cause could also be considered as a sign of the dysfunctionality of EU data protection law, in the sense that the tools that it offers for the defence of DFR would not be ‘obvious’ enough for the actors concerned – in particular, with respect to supervision and enforcement. Such dysfunctionality could mainly find its sources in both internal and external factors. External factors could include, for example, the slow pace of justice (by contrast to the fast pace of DDT development), the lack of knowledge of data subjects about their rights, the insufficient budget allocated to DPAs to fulfil their mission, or the existence of a certain confusion or conflicts of competences between the mission of those DPAs and of other public bodies involved in the protection of fundamental rights and freedoms.

In the opinion of the author, each of the above-mentioned causes have participated, at least partly, to the apparent shortfall in the fulfilment of the FRO of EU data protection law. Hence, each of these potential causes will be discussed transversally in the following chapters of this study.

CHAPTER 3 – OUTLINING THE MAIN FACTORS OF FUNCTIONALITY OF THE GDPR FOR THE DEFENCE OF DATA SUBJECTS’ FUNDAMENTAL RIGHTS AND FREEDOMS

Foreword

As a reminder, the overreaching research question of this study is the following:

How multi-functional is EU data protection law, and the GDPR in particular, for protecting data subjects’ fundamental rights and freedoms against novel and potentially harmful data processing practices?

The purpose of this Chapter is to highlight the most apparent internal factors that contribute to the effectiveness and functionality of the GDPR for the defence of data subjects’ fundamental rights and freedoms. In other words, the aim of this Chapter is to identify which provisions of the GDPR both allow and facilitate its application by its addressees in a manner that can be beneficial not only for the right to privacy or personal data protection of the data subjects, but also for DFR. Outlining these factors will both serve as an introduction to the content of the GDPR and as steppingstone to test its functionality in the next Chapter of this study.

For the sake of clarity and structure, this Chapter will be organised around what the author of this study considers as being the three ‘pillars’ of the functionality of the GDPR: (i) the Scope of the GDPR; (ii) the Substance of the GDPR in terms of principles, rights and obligations, and (iii) the Supervision and sanction system of the GDPR. References to other instruments of EU data protection law, such as the Law Enforcement Directive or the e-Privacy Directive, will only be discussed incidentally where necessary to answer the research question of this study.

3.1. FIRST STRUCTURAL PILLAR OF FUNCTIONALITY OF THE GDPR: A BROAD MATERIAL, PERSONAL AND TERRITORIAL SCOPE

The scope of a law is central in enabling its application and thus effectiveness and functionality. Quite logically, the broader the scope of a law is, the more likely it will apply to various situations for the benefit of the persons it is meant to protect. By contrast, if a law has a very narrow scope, it would rarely be applicable and would therefore be less functional for the concerned addressees. Hence, a broad scope can become a structural element of the effectiveness and functionality of any law. Conversely, limitations to the scope of a law may increase its ineffectiveness or dysfunctionality. As discussed below, it will be shown that the scope of EU data protection law is particularly broad and therefore enables data subjects to rely on data protection rules in a variety of situations, which makes it particularly functional for the defence of fundamental rights in general. To highlight the extent and limits of the scope of EU data protection law, the below sections will focus in turn on (1) the material, (2) the territorial and (3) the personal scope of the GDPR. The reason why the author has decided to first discuss the material scope of the GDPR relates to the fact that important notions will be introduced in that section, and in particular the notion of ‘personal data’ and of ‘processing’. It is necessary to understand these notions before being able to explore other related notions, such as the notion of ‘data subject’ and of ‘controllers’, which play a key role in determining the territorial and personal scope of the GDPR.

3.1.1. The Material Scope of the GDPR, or the so-called “*law of everything*”

568

Article 2(1) of the GDPR defines the material scope of the regulation as follows:

*“This Regulation applies to the **processing of personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.”*

The material scope of EU data protection law is thus mainly dependent on the definition and interpretation given to the notion of ‘processing’ (as discussed in Section 3.1.1.1 below) and of ‘personal data’ (as discussed in Section 3.1.1.2 below). In parallel, Article 2(2) GDPR establishes several limitations to the material scope of the GDPR, whose impact on the functionality of the entire framework will also need to be assessed (Section 3.1.1.3). Finally, as part of her concluding remarks (Section 3.1.1.4), the author will highlight how the broadness of this material scope contributes to the functionality of EU data protection law for the defence of multiple

⁵⁶⁸ Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1):40-81.

fundamental rights and freedoms of the data subjects, while in parallel responding to the concerns of some scholars such as Nadezhda Purtova, according to which the GDPR could become dysfunctional by potentially turning into “*the law of everything*”.⁵⁶⁹

3.1.1.1. The broad notion of ‘processing’ and its effect on the functionality of EU data protection law

For the GDPR to apply, personal data must not merely exist; they must first and foremost be processed. The term ‘processing’ in itself is broadly defined under Article 4(2) GDPR as “*any operation or set of operations which is performed on personal data or on sets of personal data, (...)*”. The same article non-exhaustively lists some of these operations, such as the collection, recording, storage, use, disclosure, transmission, dissemination, erasure or destruction of personal data.⁵⁷⁰ The jurisprudence of the CJEU has almost systematically confirmed the broad meaning of the term ‘processing’ in its case law. As synthesized by Tosoni and Bygrave, the CJEU has found, in particular, that the definition of ‘processing’ covers the following operations, among others: the loading of personal data on an internet page;⁵⁷¹ the collection of personal data from documents in the public domain, the publication of personal data in printed form, the transfer of personal data on a CD-ROM, the sending of text messages containing personal data, the capture, transmission, manipulation, recording, storage or communication of sound and image data;⁵⁷² the communication of personal data in response to a request for access to documents;⁵⁷³ the communication of the name and address of an internet subscriber or user;⁵⁷⁴ the activities of a search engines such as Google, which searches, retrieves and displays information, including personal data, in the form of search results;⁵⁷⁵ the taking and storing of human fingerprints;⁵⁷⁶ the retention of data for the purpose of possible access to them by the competent national authorities;⁵⁷⁷ the video recording of persons;⁵⁷⁸ the transfer of personal data from an EU Member State to a third country;⁵⁷⁹ the transcription and keeping of personal data in a public register;⁵⁸⁰ the drawing up of a list of individuals;⁵⁸¹ the act of publishing a video recording, which contains personal data, on a video website on which users can send, watch and share videos;⁵⁸² and the collection and disclosure by transmission of the personal data of visitors to a website by means of a third-party

⁵⁶⁹ *Ibid.*

⁵⁷⁰ Article 4(2) of the GDPR and Article 3(2) of the Law Enforcement Directive.

⁵⁷¹ CJEU, Case C-101/01, *Lindqvist*, para. 2.

⁵⁷² CJEU, Case C-73/07, *Satamedia*, paras. 35–37

⁵⁷³ CJEU, Case C-28/08 P, *Bavarian Lager*, para. 69.

⁵⁷⁴ CJEU, Case C-461/10, *Bonnier Audio and Others*, para. 52.

⁵⁷⁵ CJEU, Case C-131/12, *Google Spain*, paras. 26–31.

⁵⁷⁶ CJEU, Case C-291/12, *Schwarz*, paras. 28–29.

⁵⁷⁷ CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, para. 29.

⁵⁷⁸ CJEU, Case C-212/13, *Ryneš*, para. 25; Case C-345/17, *Buivids*, para. 35.

⁵⁷⁹ CJEU, Case C-362/1, *Schrems I*, and Case C-311/18, *Schrems II*.

⁵⁸⁰ CJEU, Case C-398/15, *Manni*, para. 35.

⁵⁸¹ CJEU, Case C-73/16, *Puškár*, para. 103

⁵⁸² CJEU, Case C-345/17, *Buivids*, para. 39.

plug-in.⁵⁸³ In other words, virtually any type of operation on personal data can be considered as ‘processing’, from the simple action of sending a professional email to someone, to storing the results of the blood analysis of a patient, registering an IP address, or recording images of people in a public space.

As specified in Article 2(1) GDPR, such processing can be conducted either by automated means or by other means when the data are intended to form part of a filing system. As a general rule, two types of processing operations can thus be distinguished; (i) the automated processing of personal data and; (ii) the non-automated filing of personal data. As explained by Tosoni and Bygrave, processing by automated means (often called ‘automated processing’) refers to all processing done by means of computer technologies, whereas processing other than by automated means primarily refers to manual processing performed by one or several humans.⁵⁸⁴ To illustrate this distinction, one may think, on the one hand, about the storage of digital patient files on a secured server by an hospital, and, on the other hand, about the paper filing of patient medical dossiers by a general practitioner. Both type of storage can be considered as a type of processing of personal data in the sense of Article 4(2) GDPR, and both the hospital and the general practitioner will therefore be subject to similar obligations under the GDPR.

As far as processing by automated means is concerned, it is worth reminding that the GDPR is technologically neutral. Therefore, the GDPR applies to the automated processing of personal data regardless of the technology used for that purpose.⁵⁸⁵ This ‘technology neutral’ approach was voluntarily adopted to avoid any risk of circumvention.⁵⁸⁶ Whether personal data are processed through a smartphone, a laptop or in the cloud will therefore have no impact on the applicability of EU data protection law. This enables the GDPR to remain relevant and absorb new or emerging DDTs within its material scope – a particularly important aspect for its long-term functionality.

As far as *non*-automated processing is concerned, only operations whereby personal data are contained (or intended to be contained) in a so-called ‘filing system’ will fall within the scope of the GDPR. Article 4(6) GDPR defines a ‘filing system’ as “*any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.*” The CJEU has already unrestrictedly interpreted the notion of ‘filing system’ in the *Jehovan todistajat* case, by lowering the bar with respect to the level of structure that the filing system must have to qualify as such. In particular, the CJEU

⁵⁸³ CJEU, Case C-40/17, *Fashion ID*, para. 76.

⁵⁸⁴ Tosoni L. & Bygrave, L. (2020). Article 4(2). Processing. Kuner, C., Bygrave, L. & Docksey, C. (eds). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, p. 119.

⁵⁸⁵ Recital 15 of the GDPR provides in this respect: “*In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.*”

⁵⁸⁶ Recital 15 of the GDPR. See also Tosoni. L. & Bygrave L. A. (2020), *op. cit.*, p. 143.

determined that personal data must not be structured in any specific way to be considered as forming part of a filing system, as long as the data remain easily accessible based on one or more criteria. These criteria do not have to be particularly sophisticated – for example, a filing system organised on the basis of a sole criteria, such as an alphabetical geographical or chronological criteria, can still be considered as a filing system under Article 4(6) GDPR, as long as the personal data contained in it can be “*easily retrieved for subsequent use*”.⁵⁸⁷ The *Jehovan todistajat* judgment has further clarified that even if the personal data are not systematically or orderly entered into the system (cf. the Jehovah witnesses were writing down some information about the individuals they met as ‘memory aids’, but only part of these data were subsequently used to draw up lists of individuals who did not wish to receive further visits),⁵⁸⁸ these operations could still be considered as ‘processing’ in the sense of Article 4(2) GDPR. Hence, even a poorly organised or incomplete filing system may fall within the scope of the GDPR, as long as the purpose of that system is to allow the personal data in question to be accessed or retrieved.⁵⁸⁹

One may of course wonder why the GDPR regulates only certain types of manual processing activities. This choice may be explained on the basis of historical reasons. The concept of ‘filing system’ was indeed retained from the 1995 Directive,⁵⁹⁰ as well as in many national data protection laws of the 1970s and 1980s, at a time where most public administrations were still using both paper and computer filing to store information about citizens (e.g. birth certificates ; proof of residence ; tax declarations; etc.).⁵⁹¹ Another reason which may explain why the manual filing of personal data is still regulated under the GDPR lies in the fact that such type of processing can present the same dangers for individuals’ rights and freedoms than automated processing.⁵⁹² Indeed, regardless of the incomplete or unstructured nature of the filing system, as long as personal data can be accessed and retrieved, there is a risk that their unfair, abusive or illegitimate use could cause prejudice to the data subjects. Hence, even non-automated processing is regulated when the personal data are kept in a manner which allows their future processing.

Although grounded in the very objective of the GDPR, the validity of the distinction between manual filing that falls within the scope of the GDPR and other types of non-automated processing that do not fall within that scope could be questioned when the actual risk associated with such processing remains the same for the data subjects. As an illustration, one may consider some of the measures adopted in the context of the COVID-19 pandemic, such as denying entry to places or preventing access to some services based on the bodily temperature of the individuals, or the

⁵⁸⁷ CJEU, *Jehovan Todistajat*, para. 61.

⁵⁸⁸ *Ibid.*, para. 59.

⁵⁸⁹ *Ibid.*, para. 20 and paras. 53-62.

⁵⁹⁰ Article 2(c) of the 1995 Directive.

⁵⁹¹ See above, Section 2.1.2 of this study. See also Hijmans, H. (2020). *Article 1 Subject-matter and objectives*. Kuner, C., Bygrave, L. & Docksey, C. (eds). *op. cit.*, pp. 51–53.

⁵⁹² See Amended Proposal of the 1995 Data Protection Directive, p. 10, explaining that the definition of ‘file’. See also Tosoni, L. & Bygrave, L. A. (2020). *op. cit.*, p. 140.

presentation of a vaccination or recovery certificate. Depending on the means deployed to carry out these checks, the GDPR may or may not apply. Some DPAs have indeed recalled that the checking of human bodily temperature through non-automated means (such as an infrared thermometer) does not fall within the scope of application of the GDPR if the actual results are not further stored, communicated or otherwise processed through automated means or as a part of a filing system.⁵⁹³ As such, this finding seems consistent with the definition given to the notion of ‘processing’ under Article 4(2) GDPR, as well as the case-law of the CJEU, but it may in some circumstances, create an undue discrimination between different categories of data subjects, which would go directly against the FRO of the GDPR. In a case opposing the Brussels South Charleroi Airport to the Belgian DPA (the APD), for example, the APD found that carrying out temperature checks with thermal cameras on passengers was a type of automated processing that fell *within* the scope of the GDPR because the cameras were recording images.⁵⁹⁴ There is indeed no doubt as to the fact that such operations (i.e., the digital recording and storage of passengers images and of their body temperature) was a type of processing of personal data by automated means.⁵⁹⁵ Because of the absence of legal basis for such processing (among others), the APD ultimately imposed a fine of 200.000 EUR on the Brussels South Charleroi Airport.⁵⁹⁶ By contrast, if the temperature checks had been carried out manually, without the data being filed – for example, with an infrared thermometer handled by a security guard at the entrance of the airport –, the APD could not have reached the same decision. In both scenarios however, the effects on the individuals would have to a large extent remain the same, that is, being potentially prevented from boarding their flight because of a higher-than-normal bodily temperature.

Keeping this distinction in mind, some controllers may be tempted to circumvent the GDPR by having recourse to non-automated processing practices where the data are only momentarily kept or stored under a form that is not structured. This could, of course, render the GDPR highly dysfunctional. It must be admitted however that, when a person takes a decision on the basis of personal data that can have legal effects or similarly significant effects (such as denying passengers entry based on their body temperature), that person will normally seek to keep evidence of the process and result, either for liability reasons (e.g. to be able to justify such a decision in the event of a dispute or investigation) or for practical reason (e.g. to be able to recognise and deny entry to the same individual if the latter makes a second attempt). Keeping such evidence will normally require the personal data to be stored

⁵⁹³ This seems to be at least the opinion of the CNIL in France and of the APD in Belgium. See CNIL (2020, Septembre 23). *Coronavirus (COVID-19): les rappels de la CNIL sur la collecte de données personnelles par les employeurs*. <https://www.cnil.fr/en/node/119866>; See APD (2021, February 4). *Prise de température dans le cadre de la lutte contre le COVID-19*. <https://www.autoriteprotectiondonnees.be/professionnel/themes/covid-19/prise-de-temperature>.

⁵⁹⁴ APD, Decision 48/2022 of 4 April 2022, DOS-2020-02823, <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-48-2022.pdf>.

⁵⁹⁵ *Ibid.*, paras. 34 to 37.

⁵⁹⁶ *Ibid.*, para. 74.

either in digital format or in a paper filing system. Hence, the risk of systemic circumvention of the GDPR by controllers through the manual processing of personal data does not seem plausible, especially in a world where digitalisation has become a competitive advantage.

This also leads to the observation that any processing operation must necessarily be conducted *by someone*. The notion of ‘processing’ therefore links the personal data which are being processed to the person who is responsible for such processing under the GDPR. This person can either be a controller or a processor, depending on the level of decision-making power that it has with respect to the means and purposes of the processing (see Section 3.1.3 below on the personal scope of the GDPR).

From the perspective of the effectiveness and functionality of EU data protection law, it is worth noting that the responsibility of the controller or the processor is triggered regardless of whether a processing operation is performed voluntarily or accidentally.⁵⁹⁷ The degree of knowledge that a controller or processor has with respect to a given processing operation has therefore no impact on the application of the GDPR.⁵⁹⁸ Hence, even accidental collection or destruction of personal data can fall within the material scope of the GDPR. Similarly, passive operations, such as the storage of personal data, can also be considered as ‘processing’ under Article 4(2) GDPR. A controller or processor may thus not escape the scope of application of the GDPR by claiming that it had no knowledge of the processing operation, or that its role was merely a passive one. At best, it could only invoke these elements as attenuating circumstances (if not resulting from its own negligence) in the event of a violation that could trigger corrective measures, such as an administrative fine imposed by the competent DPA. As further seen in the fourth Chapter of this study, this is particularly relevant with respect to the responsibility of internet service providers and their intermediaries, including social media platforms such as Facebook or TikTok which generally host the content produced and published by third parties, i.e., their users.

It is also interesting to note that there exists no requirement as to the duration, extent (in terms of amount of data) or effects of the processing on the individuals.⁵⁹⁹ There is, in other words, no ‘*de minimis*’ rule as to which type of operation can be considered as ‘processing’ in the sense of Article 4(2) GDPR. As an illustration, the Italian DPA found that the recording of images of individuals for ‘*a few tenths of a second*’ in the random-access memory of an electronic device constitutes a type of

⁵⁹⁷ As noted by Tosoni and Bygrave, “it is difficult to conceive any operation performed on personal data which would fall outside the definition of ‘processing’”. See Tosoni L. & Bygrave, L. A. (2020). *op. cit.*, p. 119.

⁵⁹⁸ The notion of processing under Article 4(2) GDPR is indeed not conditional on the existence of a voluntary action.

⁵⁹⁹ Tosoni L. & Bygrave, L. A. (2020). *op. cit.*, p. 119.

automated processing which falls within the scope of the GDPR, and can thus trigger its application.⁶⁰⁰

Based on the above considerations, and despite the sometimes-questionable distinction between non-automated processing where data are being filed, and other types of manual processing, it can be concluded that the notion of ‘processing’ covers a very wide range of activities.⁶⁰¹ This, in turn, allows data subjects, DPAs and other addresses to make use of the GDPR in various situations, including where a processing operation would or could interfere with data subjects’ rights and freedoms. The broad meaning which is ascribed to the notion of ‘*processing*’ thus participates to the functionality of EU data protection law in general. In particular, the fact that DPAs or data subjects must not prove, in order to be able to exercise their powers or their rights under the GDPR, that the processing operation fulfils any *de minimis* requirement, or that the controller or processor was aware of the processing or performed it voluntarily, can be considered as factors of functionality of the GDPR. This functionality is further reinforced, in the opinion of the author, by the broad meaning which has also been ascribed to the notion of ‘personal data’ as further discussed below.

3.1.1.2. The extensible notion of (special categories of) personal data and its effect on the functionality of data protection law

The delineation between ‘personal data’ and ‘non-personal data’ is of paramount importance to determine the material scope of the GDPR.⁶⁰² Similarly, the distinction between ‘personal data’ and ‘special categories of personal data’ has an impact on the functionality of the GDPR with respect to its FRO, given that special categories of personal data are subject to a legal regime that is more protective of the rights and freedoms of data subjects. While the two first sections will distinguish each type of data and highlight the generous interpretation that the CJEU has given to each of them, the next section will focus on the expanding grey zone between ‘personal data’ and ‘non-personal’ data, and the reason why such expansion may ultimately serve the functionality of EU data protection law.

(i) The generous interpretation of the notion of ‘personal data’ by the CJEU and other authoritative bodies

⁶⁰⁰ Italian DPA (2017, July 25). *Notizie Brevi* (archived webpage), mentioned by Tosoni L. & Bygrave L. A. (2020). op. cit., p. 119, footnote 9.

⁶⁰¹ *Ibid.*, p. 118.

⁶⁰² Finck, M. & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1):11-36.

Article 4(1) of the GDPR defines personal data as “*any information relating to an identified or identifiable natural person (‘data subject’)*”. Four ‘building blocks’ are typically analysed within that definition:⁶⁰³

- (a) the term ‘information’;
- (b) the expression ‘relating to’;
- (c) the notion of ‘identified’ or ‘identifiable’ individual; and
- (d) the meaning of ‘natural person’.

As seen below, these four building blocks have mostly been interpreted by the Article 29 Working Party,⁶⁰⁴ the EDPB and the CJEU in a manner which has gradually extended the material scope of EU data protection law.

(a) Information is information, even if subjective or inaccurate and regardless of its form

The first building block of the notion of personal data is ‘information’. Both the Recitals of the GDPR and the case-law of the CJEU confirm that the term “*information*” should not be interpreted restrictively. Beyond traditional identifiers such as a name or passport number, any information on the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person can also qualify as personal data.⁶⁰⁵ This may include information about one’s appearance, geolocation, behaviours, level of education or professional skills,⁶⁰⁶ but also other far-reaching information such as one’s IP address⁶⁰⁷, handwriting style,⁶⁰⁸ or even car chassis number.⁶⁰⁹ As stated by the CJEU in *Nowak*, the use of the generic expression ‘information’ in the legal definition of personal data “*reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective*”.⁶¹⁰ Hence, the information does not have to be private, accurate, or objective to qualify as ‘personal’. A professional email address publicly available on LinkedIn, a fake EU Digital COVID-19 certificate or the opinion of an art critic with respect to a painting, for example, can all be considered as personal data, as long as they relate to an identifiable individual. As further discussed in the following Chapter of this thesis,⁶¹¹ this broad interpretation of the term ‘information’ becomes particularly functional for data subjects who wish to combat harmful data processing practices involving the dissemination of false

⁶⁰³ See Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data (WP 136) 01248/07/EN.

⁶⁰⁴ The Article 29 Working Party (also ‘Article 29 WP’) is the predecessor of the EDPB. It was established under Article 29 of the 1995 Data Protection Directive and had primarily advisory competences with respect to the interpretation and application of EU data protection law.

⁶⁰⁵ Article 4(1) GDPR specifically refers to all these categories of data as personal data.

⁶⁰⁶ Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data (WP 136) 01248/07/EN, p. 6.

⁶⁰⁷ CJEU, Judgment of 19 October 2016, *Breyer*, C-582/14.

⁶⁰⁸ CJEU, Judgment of 20 December 2017, *Nowak*, C-434/16.

⁶⁰⁹ Opinion of AG Bobek in Case C-175/20 (SIA ‘SS’) delivered on 2 September 2021, ECLI:EU:C:2021:690.

⁶¹⁰ *Ibid.*, para. 34.

⁶¹¹ See Chapter 4, Section 4.1 on online harassment.

information about them, including in the context of defamation or harassment lawsuits. Finally, it is worth noting that information relating to an individual can take many forms, and that the GDPR does not exclude any of them *per se*.⁶¹² Hence, information qualifying as personal data can either be alphabetical or numerical, analogical or digital, and be contained in documents, audio recordings, videos or pictures, among others.⁶¹³

(b) Information can ‘relate to’ an individual in content, purpose or effect

The second building block of the notion of personal data is that the information must ‘relate to’ an individual. From the perspective of the functionality of EU data protection law, it could be argued that the GDPR could become dysfunctional if the expression ‘*relating to*’ was interpreted so restrictively that it would prevent DPAs from exercising their powers, or data subjects from exercising their rights, because it would be considered that the data do not directly relate to an individual. As an example, in the 2014 judgment *Y.S. and Others*, the CJEU took the restrictive view that the legal analysis formulated by an immigration officer to decide on the case of an applicant for a residence permit did not as such constitute personal data ‘*relating to*’ that applicant.⁶¹⁴ The CJEU considered indeed that only the data relating to the applicants *in content*, such as their name, date of birth, nationality, gender, language or the statements they actually made, should be considered as personal data. As a consequence, the data subjects could be recognised a right to access information about them which had served as a factual basis for the immigration officer to reach a decision, but not to the whole legal reasoning behind that decision. *De facto*, this prevented the data subjects from obtaining access to the entire file and to critically review and contest the legal reasoning based on which the decision of the immigration officer had been motivated. This, in turn, may have limited the data subjects’ right to good administration (Article 41 of the Charter) and the right to an effective remedy and to a fair trial (Article 47 of the Charter).

After the judgment of the CJEU in *Y.S. and Others*, the general understanding was that a document, file or dataset could be withheld when it contained both information relating to an individual and other type of information, such as the thoughts, opinions or comments of a (representative) of the controller or of a third party. In the event of an access request under Article 15 GDPR, the controller would then only be under the obligation to disclose the few data relating to the data subject in content, but not the rest of the file. As a consequence, access to mixed datasets, such as HR files, KYC files, etc., became increasingly contentious, given that such datasets usually contain a mix of personal data about an individual and the

⁶¹² Finck, M. & Pallas, F. (2020). *op. cit.*, pp. 11–36.

⁶¹³ Article 29 Working Party, Opinion on the concept of personal data, p. 7; CJEU, Judgment of 14 February 2019, *Buivids*, Case C-345/17, para 31.

⁶¹⁴ CJEU, Judgment of 14 July 2014, *YS and Others*, Case C-141/12, paras. 33-48

notes, comments or thoughts of the controller which were formulated on the basis of these data.⁶¹⁵

In the opinion of the author, however, such a distinction cannot be justified in light of the definition of personal data under Article 4(1) GDPR or the overall objective of the GDPR. When a file or dataset contains both personal data *about* an individual (e.g. about his/her job performances, revenues, behaviours, etc.) and another person's notes, comments or thoughts inferred from or taken on the basis of these data, the personal data should be regarded as being embodied within these notes, comments or thoughts. In particular, if such notes, comments or thoughts could have not been formulated without the personal data in question, their interdependence could justify that the entire dataset or file be considered as personal data relating to the individual. This interpretation seems supported by the overall objective of the GDPR, which is to ensure a high level of protection for natural persons in the context of the processing of their personal data, especially in the context of profiling.⁶¹⁶ Indeed, a more restrictive approach to the notion of personal data could unduly restrict the right to access of data subjects to mixed datasets in instances where the impact of such processing on them could be particularly significant. As argued by Ausloos *et al.*, access to opinions or reasonings embodying personal data is key to a variety of other rights and obligations in the GDPR, such as rectification, objection, erasure, as well as the broad assessment of fairness and non-discrimination.⁶¹⁷

If the CJEU had always adopted a similarly narrow interpretation of the notion of information '*relating to*' an individual, EU data protection law would have probably become less and less functional for data subjects seeking to assert their rights or interests against decisions taken on the basis of personal information. Three years after that judgment, however, the CJEU adopted a noticeably more generous interpretation of the notion of personal data in the 2017 case *Nowak*,⁶¹⁸ where it stated that data could also relate to an individual because of its *purpose* or *effect*. By expanding the notion of personal data in that way, the CJEU thus also broadened the material scope of EU data protection law and made it more functional for data subjects seeking to assert their rights under that legislation. Today, it is indeed generally admitted that data must not necessarily be *about* an individual with respect to their content to qualify as personal; rather, it suffices that they *relate to* an individual, either in *content*, in *purpose* or in *effect*. To illustrate those three concepts, one may refer to the information contained in the exam transcript of a student. If the student submitted written answers, for example, the latter could qualify as personal data *in content* as far as they reveal information *about* the

⁶¹⁵ Ausloos, J., Mahieu, R. & Veale, M. (2019) Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10(3):283-309, para. 40.

⁶¹⁶ As defined in Article 4(4) GDPR.

⁶¹⁷ Ausloos, J., Mahieu, R. & Veale, M. (2019). *op. cit.*, pt. 41.

⁶¹⁸ CJEU, *Nowak*, C-434/16, para. 35.

student's degree of knowledge or opinion on a particular topic. In the context of a Multiple Choices Questions, the boxes checked by a student can also be considered as personal data relating to that student *in purpose*, since the chosen answers will be scrutinized for the purpose of evaluating the student. Finally, the grade that the student has obtained can be considered as information relating to the student *in effect* because it will determine whether the latter passed the test or not, with all the consequences that such a failure or success could entail. A student could thus legitimately request access to an exam transcript, including the notes or comments of the corrector, given that these notes or comments are intrinsically linked to the answers provided by the data subject and relate to the latter both in purpose and in effect. This example shows the wide range of information that can qualify as personal data 'relating to' an individual under EU data protection law, therefore extending the protective scope of that legislative framework well beyond the notion of information 'about' an individual.

From the perspective of legal certainty and consistency, it is regrettable to note however that the seemingly contradicting views adopted by the CJEU in *Y.S. and Others*, on the one hand, and *Nowak*, on the other hand, have had persisting effects at the national level, and have sometimes deprived data subjects from accessing important information.⁶¹⁹ In some cases, indeed, national courts and DPAs have adopted a narrower interpretation of the notion of personal data by tending to exclude information about an individual deriving from a third-party opinion or reasoning, without considering that personal data can also relate to a person in purpose or in effect. As an illustration, one may refer to a judgment of 1 March 2021 by the Amsterdam District Court concerning Uber drivers. The dispute concerned several access requests made by Uber drivers to obtain a copy of the personal data that Uber was processing about them, including drivers' profiles and drivers' tags. With respect to the drivers' profiles, the District Court noted that, according to Uber, the profiles in question were not real 'profiles', but rather internal memos containing the personal thoughts of Uber's employees to be shared with Uber customer services. Still according to Uber, these internal memos were exclusively intended for internal consultation and deliberation. Referring to *Y.S. and Others*, and taking the view that these profiles did not constitute personal data whose accuracy or lawfulness could be challenged by the data subjects,⁶²⁰ the District Court concluded that Uber was not obliged to provide copy of these memos, but only of the personal data "**about the [drivers]**"⁶²¹ that formed the factual basis of these memos. The District Court failed however to explain why the rest of the information contained in these memos could not be considered as personal data relating to the Uber drivers *in effect* or *in purpose*, thereby ignoring the more recent interpretation

⁶¹⁹ Ausloos, J., Mahieu, R. & Veale, M. (2019). *op. cit.*

⁶²⁰ Amsterdam District Court, Judgment n° C/13/687315 / HA RK 20-207 of 1 March 2021, available at <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020>, para. 4.41.

⁶²¹ *Ibid.* In full and in original: "*Dit leidt ertoe dat Uber alleen gehouden is om de gegevens over verzoekers die de feitelijke basis van de notities vormen te verstrekken en niet de interne notities als zodanig.*" (emphasis added)

given by the CJEU to the notion of ‘personal data’ in the *Nowak* case. The District Court applied the same reasoning with respect to drivers’ tags, despite these tags being used by Uber customer service to assess and keep track of Uber drivers’ behaviours. These tags could read, for example, ‘inappropriate behaviour’ or ‘police’, in the event it had been reported that a driver had not behaved politely towards a customer or had been subject to a police control. Despite the Uber drivers pointing out that these tags could contain very negative qualifications that could have significant consequences on them, the District Court took the (highly questionable) view that “*such [tags] cannot be checked by the data subject for correctness*” and were therefore “*not subject to the right of inspection*”.⁶²²

Other DPAs and courts, including some courts in the Netherlands, have however embraced the broader interpretation of the notion of personal data as developed by the CJEU in *Nowak*. As an illustration, on 21 March 2021, i.e., a few days after the Uber judgment discussed about, another Dutch court ruled in case opposing an individual to a Scientific Research Institute, that data subjects had the right to obtain a copy of emails relating to them sent by a controller, even if these emails did not exclusively contain data *about* them.⁶²³ The Court rejected the argument of the Scientific Research Institute according to which these emails contained the personal thoughts of its employees, or were purely used for internal consultation or deliberation, since the emails in question had been sent to third parties outside of the organisation. The District Court noted in particular that “*if the data contribute to determining the way in which the data subject is assessed or treated in society, that data is considered personal data. Personal data do not only include data on the basis of which a natural person can be identified, but also factual or appreciative data about characteristics, opinions or behaviour of a natural person.*”⁶²⁴ In the opinion of the author, this reading of Article 4(1) GDPR is more in line with the case-law of the CJEU on the notion of personal data, as well as with the underlying FRO of that Regulation. By being granted access to the entire dataset on the basis of which a decision has been taken, data subjects have indeed a better chance to challenge the fairness or lawfulness of the processing, and thus to protect their interests, rights and freedoms, either as workers, (former) employees or consumers. This broader interpretation of the notion of information ‘relating to’ a natural person therefore contributes to the functionality of the GDPR as a whole.

⁶²² *Ibid.*, para. 4.44. In full in the original language: “*Ook hier geldt (...) dat een dergelijke aanduiding door de betrokkene niet kan worden gecontroleerd op de juistheid daarvan. De Tags als zodanig vallen dus niet onder het inzage-recht.*”

⁶²³ Rb. Midden-Nederland, Judgment C/16/502323/HA RK 20-122 of 23 March 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2021:1354#_34118c93-e68a-43f6-8e50-cfaebab1560b.

⁶²⁴ *Ibid.* In full and in the original language: “*(...) als de gegevens medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, die gegevens als persoonsgegevens worden aangemerkt. Niet alleen gegevens op basis waarvan een natuurlijk persoon geïdentificeerd kan worden, maar ook feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen van een persoon zijn dus persoonsgegevens. Voor zover dergelijke gegevens geautomatiseerd worden verwerkt of voorkomen in bestanden is het inzage-recht daarop van toepassing.*”

(c) A person must be considered as ‘identifiable’ not only on the basis of the data in possession of the controller, but on the basis of all reasonable means which can be deployed by a controller or a third party to identify that person

The third building block of the definition of ‘personal data’ is that the information in question must relate to an ‘*identified*’ or ‘*identifiable*’ individual. In the opinion of the Working Party 29, individuals ought to be considered identifiable where they can directly or indirectly be ‘distinguished’ from other individuals, even if some information about their identity, such as their full name, remains uncertain.⁶²⁵ In *Digital Rights Ireland*, for example, the CJEU established that metadata (such as location data or IP addresses) should be considered as personal data even if they only allow for the indirect identification of individuals through a series of information (such as one’s IP address, approximate location, the time of communications, etc.).⁶²⁶ The question which logically arises from this, is the one of the means of identification. Pursuant to the GDPR, data only become personal if the controller, processor, or any other person is able to identify the data subject through ‘*means reasonably likely to be used*’.⁶²⁷ If the data remains insufficient to single out a person through reasonable means, such data would thus qualify as non-personal and fall outside the scope of the GDPR.

In the judgment *Breyer*, the CJEU has made two important clarifications in this respect. First, the CJEU has stressed that it is not required that all the information enabling the identification of the data subject are in the hands of one person.⁶²⁸ In other words, controllers should not only take into account the data or the means that are available to *them* to identify the individuals in question, but also the data and the means that are available to third parties. Second, the CJEU has clarified that only *lawful* means of identification should be considered, as well as means that do not require a *disproportionate effort* in terms of time, cost and man-power.⁶²⁹ As a consequence, the assessment to be made should neither include illegal means of identification, such as the hacking of a database or the theft of an encryption key, nor include unrealistic means that would require massive financial investments or efforts. All in all, the CJEU has therefore opted for a relative approach with respect to the notion of ‘*identifiability*’ of data subjects under the GDPR (in opposition to an absolute approach).⁶³⁰ This relative approach is sometimes also referred to as a risk-based approach,⁶³¹ according to which controllers or processors must analyse on a case-by-case basis whether there exists a reasonable risk of identification of the data

⁶²⁵ Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, 01248/07/EN.

⁶²⁶ CJEU, *Digital Rights Ireland*, para. 26.

⁶²⁷ Recital 26 GDPR.

⁶²⁸ CJEU, *Breyer*, para. 43.

⁶²⁹ *Ibid.*, para. 46.

⁶³⁰ Spindler G. & Schmechel P. (2016). Personal Data and Encryption in the European General Data Protection Regulation. *JIPITEC*, 7: 163-177.

⁶³¹ Finck, M. & Pallas, F. (2020). *op. cit.*

subjects through legal and proportionate means. This point, and its impact on the 'grey zone' between the notion of personal data and on-personal data, will further be discussed in section (iii) here below.

(d) Personal data must relate to a living natural person

The fourth and final building block of the definition of personal data is that the information must relate to a living person. Hence, Article 4(1) GDPR, read in combination with Recital 27 of the GDPR, makes clear that the GDPR does not apply to legal persons⁶³² or deceased individuals.⁶³³ Since this study focuses on the functionality of EU data protection law for the defence of the fundamental rights and freedoms of *individuals*, the author will not enter in the on-going debate regarding whether the protective regime of the GDPR should also (or at least in part) be extended to legal persons.⁶³⁴ The notion of 'data subjects' will however be further clarified in Section 3.1.3 below on the personal scope of the GDPR.

(ii) The generous interpretation given by the CJEU to the notion of special categories of personal data under Article 9 GDPR and its effect on the veto power of data subjects

Another factor which, in theory, makes the GDPR particularly functional for data subjects willing to assert their rights and freedoms is the generous interpretation that the CJEU has recently given to the notion of 'special categories of personal data' under Article 9 GDPR. In accordance with this Article, special categories of data include data revealing (a) racial or ethnic origin, (b) political opinions, (c) religious or philosophical beliefs, or (d) trade union membership, as well as (e) genetic data, (f) biometric data for the purpose of uniquely identifying a natural person, (g) data concerning health or (h) data concerning a natural person's sex life or sexual orientation.⁶³⁵

Special categories of data have been labelled as such under the GDPR because they are considered particularly sensitive. Hence, as stated in Recital 51 of the GDPR, these data "*merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms*". In particular, misuse of sensitive data could have serious consequences for individuals, such as exclusion or unfair discrimination.⁶³⁶ This will be exemplified in practice in the fourth Chapter of this study when assessing the functionality of the GDPR in the context of e-

⁶³² van der Sloot, B. (2015). Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System'. *Computer Law and Security Review*, 31, p. 26.

⁶³³ Recital 27 GDPR. See, also, European Archives Group (EAG) (2018, October). Guidance on data Protection for Archive Services, https://ec.europa.eu/info/sites/default/files/eag_draft_guidelines_1_11_0.pdf, p. 9: "*The GDPR protects personal data of living persons. It does not apply to the personal data of deceased persons.*"

⁶³⁴ van der Sloot, B. (2015), *op. cit.*

⁶³⁵ Article 9(1) GDPR.

⁶³⁶ Georgieva, L. & Kuner, C. (2020). *Article 9. Processing of special categories of personal data*. Kuner, C., Bygrave, L. & Docksey, C. (eds). *op. cit.*, p. 369.

recruitment (see, in particular, Section 4.2). At this stage, it is already relevant to note that the GDPR explicitly mentions three times the risk of discrimination arising from the processing of sensitive personal data, in its Recital 71, 75 and 85 GDPR respectively. It can be inferred from these recitals that preventing discrimination is thus one of the *rationes legis* for a stricter regime to apply to these special categories of data. This, in turn, tends to confirm that the broad FRO of EU data protection law extends beyond privacy, and also covers other fundamental rights and principles, such as equality or non-discrimination.

As a general rule, the GDPR simply prohibits the processing of sensitive personal data.⁶³⁷ Sensitive personal data are thus subject to a stricter regime than non-sensitive data under the GDPR. This prohibition is however not absolute. Ten exceptions exist, as listed in Article 9(2) GDPR. The first of these exceptions is the consent of the data subject. The other exceptions relate to very specific situations, such as when healthcare professionals process information relating to their patients,⁶³⁸ or when religious institutions process personal data relating to their members.⁶³⁹ These restrictive legal grounds will be discussed in more detail in Section 3.2.2.2(i), below. At this stage, it suffices to understand that the qualification of data as ‘sensitive’ will overall restrict the instances in which these data can be processed, and accentuate the obligations of controllers, including, for example, in terms of data security⁶⁴⁰ or consent collection.⁶⁴¹ For example, if a controller relies on the consent of data subjects to process their sensitive data, such consent will only be valid if it is *explicit*. This requires a clear positive action from the data subjects, such as signing a notice or checking a box. If the consent of the data subjects is later found to be invalid (because implicit, unspecific or ambiguous, for example), or if a data subject decides to withdraw his or her consent (a right that may be exercised “*at any time*”),⁶⁴² the controller cannot, as an alternative, invoke its own legitimate interests to continue processing the concerned data. Indeed, the ‘legitimate interests’ of controllers is not listed as a valid legal ground in Article 9(2) GDPR. In the opinion of the author, the strict legal regime applicable to sensitive data, combined with the possibility for data subjects to withdraw their consent at any time, renders this framework particularly functional. Data subjects can indeed force controllers to put an end to the processing of their sensitive data by simply indicating that they do not (longer) agree to such processing, without having to provide any explanation or reason. In other words, the simple fact that sensitive data are being processed based on the consent of the data subjects concerned will give a

⁶³⁷ Article 9(1) GDPR.

⁶³⁸ Article 9(1)(b) GDPR.

⁶³⁹ Article 9(1)(d) GDPR.

⁶⁴⁰ Article 32 of the GDPR indicates indeed that controllers must ensure a “*level of security appropriate to the risk*”. Since the loss, divulgation or alteration of sensitive data can have serious consequences on the data subjects, controllers must logically implement specific technical and organisational safeguards ensuring the integrity and confidentiality of sensitive data.

⁶⁴¹ In particular, it is required from the controller to ensure that such consent is *explicit* (Article 9(2)(a) GDPR), on top of the general requirements for the consent of the data subjects to be valid as spelled out in Article 7 GDPR.

⁶⁴² Article 7(3) GDPR.

right of veto to these data subjects.⁶⁴³ This veto power can be considered particularly functional since it can be exercised against the controller at no cost and does not require any evidence gathering or even explanations on the part of the data subject.

As far as the border between sensitive personal data and non-sensitive personal data is concerned, one of the on-going discussions is whether information which could *indirectly* reveal, for example, the ethnicity, religious belief, or sexual orientation of a person, should also be considered as 'sensitive'. As an illustration, one could refer to the publication of the picture of a person wearing a veil, which could indirectly reveal the fact that this person is Muslim, or information about the gender of a spouse, which could indirectly reveal the sexual orientation of both the persons concerned. If such was the case, the right of veto of the data subjects under Article 9(2)(a) and 7(3) GDPR would apply to an increased number of situations, which could in turn greatly facilitate the use of the GDPR by data subjects to put an end to data processing practices which could (potentially) be harmful to their rights, freedoms or interests.

These debates on the border between the notion of personal data and sensitive personal data took a new turn recently, following the broad interpretation of the notion of sensitive personal data embraced by the CJEU in a judgment dated 1 August 2022.⁶⁴⁴ This case opposed a public officer – OT – to a Lithuanian public authority. According to Lithuanian law, any individual seeking to work or working in the public service must lodge an electronic declaration of private interests prior or within thirty days from the date of their election, recruitment or appointment.⁶⁴⁵ These declarations contain various information about the identity and professional activities of the declarants but also information about their spouse, cohabitee or partner, as well as close relatives.⁶⁴⁶ The purpose is to shed light, *inter alia*, on any (risk of) conflict of interests that the declarant or a person close to the declarant could have with respect to the concerned position. As a general rule, a partial version of these declarations are published on the website of the Lithuanian Chief Ethics Commission, thereby making this information public. OT, who served at the time as director of an establishment operating in the field of environmental protection, was requested to fill in such a declaration but objected to its publication. In the course of the proceedings opposing OT to the Chief Ethics Commission, the national court decided to stay the proceedings and to refer two questions to the CJEU for a preliminary ruling. In particular, by its second question, the Lithuanian judge asked, in essence, whether Article 9(1) of the GDPR should be interpreted as meaning that the publication, on the website of the Chief Ethics Commission, of personal data that are liable to disclose *indirectly* the political opinions, trade union

⁶⁴³ *Ibid.*

⁶⁴⁴ CJEU, Judgment of 1 August 2022, *OT vs Vyriausioji tarnybinės etikos komisija* (Chief Ethics Commission), Case C-184/20.

⁶⁴⁵ Law No VIII-371 of the Republic of Lithuania on the reconciliation of public and private interests in the public service of 2 July 1997 (Žin., 1997, No 67-1659).

⁶⁴⁶ *Ibid.*, Article 6.1 (2).

membership or sexual orientation of a natural person constitutes processing of sensitive personal data.⁶⁴⁷ The CJEU answered to this question by the positive, thereby bringing within the scope of Article 9 GDPR a wide variety of data that can reveal sensitive information about a person, including a person's sexual orientation, even if such a link is not direct or immediate, but requires an intellectual operation involving deduction, comparison or cross-referencing.⁶⁴⁸ As far as the declaration of interest in the case at hand was concerned, it was thus considered that the name of a spouse or partner should be considered as sensitive data, as the gender of the spouse or partner could be inferred from that name (names being often gender-specific), and the sexual orientation of both individuals could in turn be deduced from this information.

The question remains how straightforward and certain this game of deductions or inferences should be for a piece of information to be considered as 'sensitive' under Article 9 GDPR. For example, if the picture of a man is published on social media, and that picture clearly shows him wearing a red cap with the words "Make America Great Again" on it at a rally organised by Trump's supporters, there is little doubt that such a picture must be considered as falling within Article 9 GDPR, given that it reveals information about the political opinion of that man. By comparison, if the picture of a man wearing the same cap is published on social media, but that man is simply doing his groceries or driving a car, it becomes more difficult to determine with certainty whether this man really is a Trump's supporter, or if he might have chosen to wear that cap for another reason. If that picture can be crossed with other information, however, such as the fact that this man is married to a woman who is a publicly known Trump supporter, both the picture and the marital status of that man could potentially fall within Article 9 GDPR, in the sense that it could reveal both the political opinion and sexual orientation of that person. Because a lot of data may directly or indirectly contribute to revealing information about a *special* categorised of data, it may become difficult to distinguish sensitive data from non-sensitive data. Yet, it was clearly not the intent of the EU legislator to bring almost all personal data within the ambit of Article 9 GDPR. This calls, in turn, for additional clarifications from the CJEU on the minimum or maximum level of assessment that must be conducted to determine whether a given (set of) data can indirectly reveal sensitive information about a person.

In the opinion of the author of this study, the clarifications brought by the judgment in *Breyer* on the notion of 'identifiability' may, by analogy, provide guidance in this respect. In particular, keeping the broad FRO of the GDPR in mind as well as the *ratio* being the enhanced protection regime established by Article 9 GDPR, it could be argued that the assessment to be made must take into consideration all the means that are reasonably likely to be used to deduce or infer sensitive information. Hence, illegal means, or means that would require disproportionate efforts in terms of time

⁶⁴⁷ CJEU, *Chief Ethics Commission*, Case C- 184/20, para. 117.

⁶⁴⁸ *Ibid.*, paras. 120 and 123.

or resources, should be excluded from this assessment (see Section 3.1.1.2(i)(c) above).

Despite these small uncertainties, it remains clear that the generous interpretation given by the CJEU to the notion of ‘special categories of data’ has generally enhanced the protective regime established under Article 9 GDPR, including by reinforcing the veto power of data subjects under Article 7(3) and 9(2)(a) GDPR in all instances where the processing is based on their consent. Hence, this judgment has overall contributed to the functionality of these provisions.

(iii) The expanding ‘grey zone’ between the notion of personal and non-personal data, and its effect on the scope and functionality of EU data protection law

Two years after the GDPR, the EU legislator also adopted a regulation on the processing of non-personal data, whose aim was to facilitate the free flows of such data across the 27 Member States and beyond (hereafter, the the ‘RNPDP’).⁶⁴⁹ Article 3(1) of that Regulation summarily defines the notion of ‘non-personal data’ in opposition to the one of ‘personal data’. In particular, it states that non-personal data means any data ‘*other than personal data as defined in point (1) of Article 4 of [the GDPR]*’. Hence, under EU law, any data which is not personal in the sense of the GDPR must necessarily be considered as a *non*-personal. Non-personal data can include, for example, information relating to a legal person (such as its corporate name or annual accounts), information relating to the environment (such as evidence of climate change or the biodiversity of a given place), or data relating to the economy (such as a country’s balance of trade, or information on the stock market). Similarly, DDT and processing practices relying on non-personal data can include, for example, an algorithm relying on economic data to predict the Gross Domestic Product of a country; a software processing farming data to monitor and optimise the use of pesticides and water; or an algorithm analysing and giving output on maintenance needs for industrial machines.⁶⁵⁰

As stated in the 9th Recital of the RNPDP, non-personal data can also take the form of aggregate and anonymised datasets used for big data analytics. In other words, non-personal data may originate from once personal data which have been manipulated to the point of becoming anonymous.⁶⁵¹ In the same Recital, it is however made clear that “*if technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data (...)*”. The RNPDP thereby sheds light on the possibility to re-identify data subjects from a set of (once

⁶⁴⁹ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

⁶⁵⁰ These examples are the one given in the 9th Recital of the Preamble of Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303, 28.11.2018, p. 59–68*.

⁶⁵¹ Finck, M. & Pallas, F. (2020). *op. cit.*, p. 11.

considered) anonymised data, including through the use of machine-learning or other techniques. Such techniques are often referred to as ‘re-identification techniques’.⁶⁵² The scope of the GDPR and of the RNPD therefore compete against each other, along with the opposing notions of ‘*personal data*’ and ‘*non-personal data*’. Analysing the rules of the RNPD would go beyond the scope of this study. Yet, it remains relevant to highlight the ‘grey zone’ that may exist between the notion of personal data and the notion of non-personal data, and its effect on the functionality of EU data protection law in terms of the broadening of its material scope.

As a general rule, practices which do not involve the processing of personal data are less likely to harm the fundamental rights and freedoms of individuals. This is because an array of risks will be mitigated or neutralised upstream, such as the risk of accidentally disclosing (sensitive) personal data about an individual, or the risk of discriminating a person based on individual characteristics. The material scope of EU data protection law is hence limited to the processing of data that qualify as ‘personal’, as opposed to ‘non-personal’. Various elements may however blur the line between the notion of ‘personal data’ and ‘non-personal data’, usually to the benefit of a broader scope of EU data protection law. Four situations should be mentioned in particular: (a) DDT conceived on the basis of non-personal data which are ultimately used by or applied on (groups of) identifiable individuals; (b) technological advances enabling the re-identification of individuals through the processing of (once) anonymized data; (c) the ‘contamination’ of dataset by personal data; and, more generally (d) the continuous shift from atoms to bits which could hypothetically render all data ‘personal’ in the future. This section will precisely focus on this ‘grey zone’ and its effect on the functionality of EU data protection law.

(a) The application of DDTs conceived on the basis of non-personal data on identifiable individuals

Technological tools that are conceived on the basis of non-personal data might still fall within the scope of EU data protection law if their final application involves the processing of personal data. As an example, an insurance company may develop, based on a massive amount of anonymised data, a new algorithm capable of better predicting the risks associated with certain categories of drivers. At the time of its conception, such a DDT would normally escape the scope of the GDPR since it does not involve the processing of personal data. As soon as such an algorithm would be used on prospective or existing clients to adjust their insurance premiums however, it would re-enter the scope of the GDPR. The clients in question would then be able to exercise their data protection rights in their capacity as data subjects, including requesting meaningful information about the logic involved behind that algorithm.⁶⁵³

⁶⁵² Gong, S., Cristani, M. Yan, S. & Loy, C. (2014). *Person Re-Identification. Advances in Computer Vision and Pattern Recognition*. Springer; Henriksen-Bulmer, J. & Jeary, S. (2016). Re-identification attacks—A systematic literature review. *International journal of information management*, 36(6):1184–1192.

⁶⁵³ Article 13(2)(f) of the GDPR.

This example show that DDTs conceived on the basis of non-personal data may still fall under the application of EU data protection law if they are later used on identifiable or identified individuals. The fact that the GDPR does not intend to regulate any specific type of technology but rather the processing of personal data can thus be seen in itself as a factor of effectiveness and functionality, in the sense that the ‘end-individuals’ on which any DDT is applied will remain protected.

Some DDTs may however not require the processing of personal data at all – not even at the time where they are being used *by* or *on* individuals. Even if the risks associated with such DDTs for the fundamental rights of the individuals concerned are lower, some violations may still arise (e.g. an automatic soap dispenser which do not recognise coloured hands;⁶⁵⁴ discrimination of groups of unidentified individuals)⁶⁵⁵. In the opinion of the author, however, this limitation to the material scope of EU data protection law does not render it dysfunctional. Rather, it shows that EU data protection law – as any other law – has a limited material scope. Furthermore, it must be considered that these other DDTs were not meant to be regulated from the perspective of EU data protection law but may still fall under the scope of other legislations, including consumer protection, competition law, anti-discrimination legislation or product liability. It also shows that, contrary to what can sometimes be argued, the GDPR is not meant to regulate all situations where individuals are confronted to DDT. Rather, it is meant to regulate situations where the rights or interests of individuals could be unduly restricted because their personal data are being processed by a controller, including (but not exclusively), through a DDT.

(b) The tension between anonymisation and re-identification techniques

As already mentioned above, anonymised data are not subject to the GDPR because they do not relate to identifiable natural persons, thereby minimising the potential risks that can be associated with their processing. In this context, processors and controllers may be tempted to rely on anonymisation, either with the honest intention to better protect the rights of individuals, or with the (sometimes less honest) intention to avoid having to comply with EU data protection law. As an illustration, the CJEU nowadays grants anonymity where possible or required by concealing the identity of the parties in its judgments in order to protect their right

⁶⁵⁴ See, for example, this article by Synclair Goethe, T. (2019, March 2). Bigotry Encoded: Racial Bias in Technology. *Reporter*. <https://reporter.rit.edu/tech/bigotry-encoded-racial-bias-technology>.

⁶⁵⁵ On the concerns relating to group privacy, see Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology*, 30(4):475-494; Loi, M. & Christen, M. (2019). Two Concepts of Group Privacy. *Philosophy & Technology*, 1:18. In case of anonymization of a personal dataset, even if the anonymization process is truly irreversible as required (Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014), some bias may still persist. DDT trained on the basis of a biased (anonymized) dataset, even if they are not used for individual automated decision making, may therefore still produce discriminatory outcomes against groups of unidentified individuals.

to privacy.⁶⁵⁶ In parallel, private actors such as pharmaceutical companies or Big Data players increasingly rely on anonymised dataset for conducting research, not only for protecting the privacy of the individuals concerned, but also in order to avoid having to comply with the GDPR.⁶⁵⁷

Generally speaking, anonymisation can be seen as advisable when reducing the risks relating to the processing of personal data for the rights and freedoms of the data subjects. Yet, anonymisation may also prevent data subjects from keeping control over their personal data and enjoying their rights under the GDPR. This is the reason why the operation of anonymising personal data itself is still legally considered as a (last) processing operation on personal data which need to comply with the GDPR.⁶⁵⁸ In practice, this means that the data subjects must have been previously informed about the intended anonymization of their personal data for one or several subsequent purposes (research, business development, or other) and may have to provide their consent in this respect. This also means that the data subjects can always *object* to the anonymization of their personal data on grounds relating to their particular situation.⁶⁵⁹ A controller may therefore be barred from anonymising personal data if the data subjects in question consider that this could be detrimental to their rights or interests. There are however two legal grounds on the basis of which the controller may ignore such an objection: (1) if the controller “*demonstrates compelling legitimate grounds for the processing **which override the interest, rights and freedoms of the data subject** (...)*”;⁶⁶⁰ and (2) if the personal data are being anonymized “*for scientific or historical research purposes, or statistical purposes, (...) necessary for the performance of a task carried out for reasons of **public interest***.”⁶⁶¹ One may notice that each ground is still explicitly concerned with the rights and freedoms of the data subjects, as they aim at establishing a fair balance with these rights and other interests. All in all, it may therefore be concluded that anonymization does not render EU data protection law inapplicable or dysfunctional for data subjects; rather, it is a possibility left to controllers which is legally regulated, and which will always require a balancing of the fundamental

⁶⁵⁶ Article 95 of the Rules of Procedure of the Court of Justice provides in this respect: “*Where anonymity has been granted by the referring court or tribunal, the Court shall respect that anonymity in the proceedings pending before it. At the request of the referring court or tribunal, of a party to the main proceedings or of its own motion, the Court may also render anonymous one or more persons or entities concerned by the case.*” (...)

⁶⁵⁷ See, *inter alia*, Narayanan A. & Shmatikov V. (2008). Robust De-anonymization of Large Sparse Datasets. *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 111:25; Afzali, G. A. & Mohammadi, S. (2018). Privacy preserving big data mining: Association rule hiding using fuzzy logic approach. *IET Information Security*, 12(1):15-24; Keerie, C. & al. (2018). Data sharing in clinical trials - practical guidance on anonymising trial datasets. *Trials*, 19(1):25; Tucker, K. & al. (2016). Protecting patient privacy when sharing patient-level data from clinical trials. *BMC Medical Research Methodology*, Suppl 1(S1):77; Hern A. (2019, July 23). ‘Anonymised’ data can never be totally anonymous, says study. *The Guardian*. <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds>.

⁶⁵⁸ Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data (WP 136) 01248/07/EN, p. 3.

⁶⁵⁹ Article 21(1) of the GDPR.

⁶⁶⁰ *Ibid.*

⁶⁶¹ Article 21(6) of the GDPR.

rights and freedoms of the individuals, the interests of the controller and the interest of society as a whole.

Furthermore, for personal data to become non-personal through anonymization, the anonymization process must be robust enough, in the sense that the risk of re-identifying the individuals must almost be non-existent. For that purpose, various anonymization techniques can be used side-by-side to increase the robustness of the anonymisation process, such as deletion of personal characteristics, noise addition,⁶⁶² permutation,⁶⁶³ aggregation or k-anonymity.⁶⁶⁴ When assessing the robustness of an anonymization process, the controller or processor must also take into account the various techniques which exist to re-identify the data subjects, such as linking,⁶⁶⁵ singling out,⁶⁶⁶ or inference.⁶⁶⁷ For example, even if a medical researcher decides to anonymize data relating to patients by erasing their name and gender, and randomly shuffling the patients' age (permutation), it may still be possible to re-identify these patients based on other physiological characteristics (singling out), or by gleaning information about them with the help of other sources of information that are available (linking).

With new DDT relying on machine-learning, re-identification techniques have become more and more performant. As an illustration, one may refer to a 2017 experiment, where two researchers from Germany acquired the allegedly 'anonymous' browsing habits of more than three million German and were able to re-identify most of them by simply analysing the different URLs. They retrieved, among others, personal data relating to the banking habits, tax declaration and health of Valerie Wilms, member of the German federal parliament (*Bundestag*), as well as data relating to the sexual orientation and pornographic consumption of a German judge.⁶⁶⁸ More recently, in 2019, members of the University of Louvain in Belgium and of the Imperial College London published a paper showing that

⁶⁶² This technique consists of modifying attributes in the dataset so that they are less accurate whilst retaining the overall distribution. For example, in a customer database listing the initials and age of customers, addition could consist in randomly modifying the age of each individual by +1, 0 or -1 (WP29, Opinion 05/2014, p. 12).

⁶⁶³ This technique consists of shuffling the values of attributes in a table so that some of them are artificially linked to different data subjects (WP29, Opinion 05/2014, p. 13).

⁶⁶⁴ Aggregation or k-anonymity is a technique that aims to prevent a data subject from being singled out by grouping the latter with, at least, k other individuals. This technique falls within the family of 'generalisation' techniques (WP29, Opinion 05/2014, p. 16).

⁶⁶⁵ This technique consists in linking information from various sources in order to obtain a more complete set of information enabling for the re-identification of individuals (for example, an anonymised dataset could be coupled with additional data which are available online to re-identify the data subjects). See WP29, Opinion 05/2014, p. 11.

⁶⁶⁶ This technique consists of isolating some or all records enabling to identify an individual (WP29, Opinion 05/2014, p. 11).

⁶⁶⁷ This technique consists of deducing, with significant probability, the value of an attribute from the values of a set of other attributes, including by comparing the attributes of a data subject with the one of others, and progressively excluding other data subjects (WP29, Opinion 05/2014, p. 11).

⁶⁶⁸ The researchers in question were data scientist Andreas Dewes and journalist Svea Eckert. The results of their findings were first presented in a short documentary on German television (*Nackt im Netz: Auch intime Details von Bundespolitikern im Handel*, Panorama, Das Erste, 3 Novembre 2016, available at <https://daserste.ndr.de/panorama/archiv/2016/Panorama-vom-03-November-2016,panoramaarchiv358.html>).

machine-learning tools can almost always successfully re-identify individuals within allegedly ‘anonymized’ dataset. In the context of that study, the researchers bought dataset containing thousands of ‘anonymized’ profiles of US citizens, and demonstrated that 99,98% of these individuals could be re-identified by using just 15 characteristics, including age, gender, and marital status. This led Dr Julien Hendrickx, co-author of the paper, to conclude: “We’re often assured that anonymisation will keep our personal information safe. Our paper shows that de-identification is nowhere near enough to protect the privacy of people’s data.”⁶⁶⁹

As novel data analysis techniques make it easier to re-identify anonymised dataset, robust anonymisation of personal data becomes harder to achieve.⁶⁷⁰ Moreover, even when an anonymization process relies on different techniques to make such anonymization robust enough *at a given time*, this does not preclude the risk that such anonymization process could be reversed *in the future* with acquisition of new dataset, or the help of novel, more performant or unforeseen re-identification techniques. This means, in turn, that data that were once considered as falling outside of the scope of EU data protection law can easily re-enter it. The qualification of anonymized data thus calls for “*an ongoing monitoring on the part of the initial data controller of the data environment of the dataset that has undergone anonymization*”.⁶⁷¹ On this basis, it can also be argued that anonymised data merely benefit from a temporary status as non-personal data, as they can potentially fall back within the scope of the GDPR with the passage of time.⁶⁷² Because of this, some authors have qualified the status of anonymized data as ‘dynamic’.⁶⁷³

Taking this reality into account, Recital 26 of the GDPR, the Working Party 29⁶⁷⁴ and its successor the EDPB⁶⁷⁵ have established high standards when it comes to anonymization under EU data protection law. In particular, the determination of

⁶⁶⁹ Press release - Research University of Louvain and Imperial College London, *Anonymising personal data ‘not enough to protect privacy’, shows UCLouvain’s new study*, 23 June 2019, available [here](#).

⁶⁷⁰ On the subject, see also Narayanan A., & Shmatikov V., (2008). *op. cit*; Ohm P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57:1701; Datta, A., Sharma, D. & Sinha, A. (2012). Provable de-anonymization of large datasets with sparse dimensions. Degano P. & Guttman J. D. (eds.). *International Conference on Principles of Security and Trust*. Springer, pp. 229–248; De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports*, 3 :1376; De Montjoye, Y.-A., Radaelli, L., Singh, V. K., & al. (2015) Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*. 347(6221):536–539; Narayanan, A. & Shmatikov, V. (2019) Robust de-anonymization of large sparse datasets: a decade later. *Computer Science*. Princeton University. <https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf>.

⁶⁷¹ Stalla-Bourdillon, S. & Knight, A. (2017). Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data. *Wisconsin International Law Journal*, 34(284), p. 301.

⁶⁷² Farzanehfar, A. Houssiau, F. & De Montjoye, Y.A. (2021). The risk of re-identification remains high even in country-scale location datasets. *Patterns*, 2(3).

⁶⁷³ Stalla-Bourdillon, S. & Knight, A. (2017). *op. cit.*, p. 321.

⁶⁷⁴ *Ibid.*

⁶⁷⁵ EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research adopted on 2 February 2021, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf.

whether information is anonymous must be made on a case-by-case basis by the application of ‘the test of identifiability’ outlined in Recital 26 GDPR:

“To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”

Techniques of anonymization and re-identification are the subject of intense research whose findings compete with one another.⁶⁷⁶ In the opinion of the author however, the GDPR adequately takes this evolving reality into account by not imposing a set of fixed standards for anonymisation; rather, it embraces a flexible approach where the definition of ‘personal data’ and the notion ‘anonymised data’ can evolve along with technological advances. In the opinion of the author, this technology-neutral approach prevents processors from escaping the scope of the GDPR by grossly anonymising dataset. In parallel, it can also ensure a long-lasting protection for data subject against defective anonymization practices which could put their rights or freedoms at risk.⁶⁷⁷

In summary, it can therefore be concluded that the technology neutral stance of the GDPR, the fact that anonymization itself is still considered as a processing operation, the high standards which must be met for data to be truly considered ‘anonymised’, and the dynamic approach to anonymization, are all elements which accentuate the grey zone between the notion of ‘personal data’ and ‘non-personal data’, and broaden the material scope of EU data protection law in general, while ensuring its functionality with respect to its FRO.

(c) The contamination of non-personal dataset by personal data

Thirdly, one may also refer to the theory of contamination,⁶⁷⁸ according to which a dataset which only contain a small fraction of personal data may have to be treated as a personal dataset in its entirety because the few personal data that it contains cannot be extracted from it or distinguished from the rest of the data. In other words, the presence or introduction of a few personal data within a set of non-

⁶⁷⁶ See, in this respect, WP29, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.

⁶⁷⁷ Recital 26 of the GDPR and Working Party Article 29 (now EDPB), Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.

⁶⁷⁸ Expression coined by Judge Maja Brkan in her capacity as supervisor during various discussions with the author of this study.

personal data may ultimately ‘contaminate’ the other entire dataset, with the effect of bringing it within the scope of the GDPR. This contamination effect seems to find its source in Article 2(2) of Regulation 2018/1807 which provides:

“(…) Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of [the GDPR]”.

Data can be considered as ‘*inextricably linked*’ when there is no reasonable technical mean to extract personal data from non-personal data within a dataset, or when such an extraction would render the use of the dataset useless. By contrast, it may sometimes be possible to extract personal data from a dataset in order to create a distinction between a sub-set of non-personal data and a sub-set of personal data, and to limit the application of the GDPR to the latter. To illustrate this, one may take the example of a Customer Management System (CRS) built by a company to be able to contact its customers and manage its contracts with them. If 99,9% of the customers of this company would be legal persons, and only 0,1% would be natural persons, it may be advisable for that company to extract the personal data from that system, and create a separate CRS for its 0,1% of customers who are natural persons. If that is possible, the original CRS would then only contain information on legal persons, or on contracts and orders signed or issued by legal persons, and the company would thus not have to comply with the GDPR with respect to that system. For example, if a data breach would occur, and part of the data in the original CRS would be lost, no notification to the competent DPA would be necessary.⁶⁷⁹ Similarly, if the company would decide to deploy a new type of self-learning algorithm within the original CRS, with a view of anticipating the orders of its clients based on their past purchasing behaviours, it would not be necessary to inform them about it,⁶⁸⁰ or to conduct a Data Protection Impact Assessment.⁶⁸¹

Sometimes, the contamination of a non-personal dataset can however be so subtle that the controller or processor may not become aware of it. A small fraction of data within an anonymised dataset could for example become ‘personal’ again because additional information on some data subjects have been made public, or because of the emergence of novel re-identification techniques.⁶⁸² In those instances, it may simply not be possible or reasonable for the controller to find out which data have become personal again, and which have remained anonymous, especially when such an analysis would require unreasonable monitoring or resources. Hence, even if only a small fraction of these data would be concerned by this change, the controller or processor might have no other option than considering the entire database as falling within the scope of application of the GDPR.

⁶⁷⁹ As normally required by Article 33 GDPR.

⁶⁸⁰ As normally required if data subjects were concerned under Article 13 GDPR.

⁶⁸¹ Article 35 GDPR.

⁶⁸² See Section (iii)(b), above, on the tension between anonymization and re-identification techniques.

It must be noted, in this respect, that the GDPR does not contain any *de minimis* rule, whereby the processing of a dataset (such as its storage) would fall outside of the scope of the GDPR if such dataset only contains a negligent portion of personal data. As a result, controllers and processors cannot prevent potential contamination from increasing the scope of their obligations under the GDPR. This, in turn, may be considered as accentuating the grey zone between the notion of personal data and non-personal data, and indirectly expanding the material scope of EU data protection law.

The theory of contamination may also support the broader interpretation given to the notion of information ‘relating to’ a natural person, as discussed above (see section 3.1.1.2(b)). Indeed, when a dataset contains both data about an individual and information added by a third party with a view of assessing, evaluating or otherwise forming an opinion about the data subject, the entire dataset could be considered as personal data, since they will likely relate to the data subject either in content, or in purpose and effect. Indeed, the fact that the reasoning or personal thoughts of the third party could not have been formulated or expressed without using the personal data as a basis indicates that these personal data are *intrinsically linked* to this reasoning, comment, or personal thoughts. In the opinion of the author, such an interpretation is consistent with the objective and content of the GDPR, and also has the merit to also increase its overall functionality.

(d) The Negroponte shift and its impact on the scope of the GDPR

A final important element which participates to the grey zone between the notion of ‘personal data’ and ‘non personal data’, and which may extend in the future the scope of the GDPR, is the Negroponte shift itself (see Introduction, section B). In a ‘datafied’ world where technologies become more and more performant and present, all data could indeed become personal, and an indefinite number of situations could thus fall within the material scope of the GDPR. In a seminal paper published in 2017, Nadezhda Purtova points out that the GDPR could soon become “*the law of everything*”.⁶⁸³ This expression translates the idea that data protection law could potentially govern and apply to almost all human activities as the digitalisation of society keeps moving forward. If the shift from atoms to bits continues to increase exponentially, bringing us to an all-connected future, there is indeed a possibility that “*everything will be or will contain personal data, leading to the application of data protection to everything*”.⁶⁸⁴ According to Purtova, two elements in particular may both cause and accelerate this process: (1) the notion of the ‘identifiability’ of data subjects, which may become obsolete due to the rapid progress of (re)identification technologies and the failure of anonymisation; and (2)

⁶⁸³ Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10:1, pp. 40-81.

⁶⁸⁴ *Ibid.*, p. 40.

the generous interpretation given by the CJEU to the notion of information ‘*relating to*’ an individual. To illustrate this point, Purtova gives a provocative example by arguing that weather data could become personal data in the context of smart cities. She refers in particular to a project called Stratumseind 2.0, aiming at predicting, preventing and de-escalating deviant behaviour in certain neighbourhoods by engaging the police or adapting the street lighting.⁶⁸⁵ Among the relevant data gathered for the purpose of this project are WiFi data, video footages, voice recordings and data from weather stations, as it was observed that sun and rain could influence people’s (deviant) behaviours. According to Purtova, although not directly about people *in content*, weather data could theoretically qualify as personal when analysed for the *purpose* of identifying and preventing acts of vandalism, especially if such data is combined with other information that enable to identify the individuals walking down the streets. In other words, as data processing practices are increasingly penetrating almost all aspects of human lives, the world may turn into a continuum where every atom is translated into a bit, and where the GDPR could become applicable to an infinite range of situations, thereby becoming the “*law of everything*”.⁶⁸⁶

On the one side, the expansion of the scope of the GDPR through the Negroponte shift may seem desirable, since it will possibly increase the level of protection of the rights and freedoms of data subjects in an indefinite number of situations where data are being processed. On the other side, there exists a risk of dilution and non-compliance on the part of controllers and processors if the GDPR starts applying in a far-reaching manner to all life situations. Purtova fears in particular that, if the scope of the GDPR continues to expand, everybody will have to comply one day with “*a highly intensive and non-scalable regime of rights and obligations that results from the GDPR*”, and that it will not be possible for such a regime to be upheld in a meaningful way.⁶⁸⁷ Far from defending a narrower interpretation of the notion of personal data, Purtova alerts on the consequences of imposing the same high intensity of obligations in all data processing situations.⁶⁸⁸ More specifically, she stresses the risk of EU data protection law turning into a monstrous cumbersome framework that some controllers or processors may find impossible to obey, and would thus rebel against. As a basis for her argument, she refers to Lon Fuller’s tale “*The Morality of the Law*”, where a ruler – King Rex – adopts a senseless set of new laws, which prohibits citizens among others to “*cough, sneeze, hiccough, faint or fall down in the presence of the king*”.⁶⁸⁹ Fuller’s theory holds that all purported legal rules should meet eight minimal conditions in order to count as genuine laws, including the fact that they must be “*possible to obey*”.⁶⁹⁰ Behind this tale, lies the idea that laws that are almost impossible to comply with are bound to be

⁶⁸⁵ *Ibid.*, pp. 57-58.

⁶⁸⁶ *Ibid.*

⁶⁸⁷ *Ibid.*, p. 42.

⁶⁸⁸ *Ibid.*

⁶⁸⁹ Fuller, L. (1969). *The Morality of Law*. Yale University Press, pp. 36–37.

⁶⁹⁰ *Ibid.*, p. 28.

disregarded or disobeyed by the population. Drawing from this tale, Purtova argues that, because of its broad material scope, EU data protection law may in practice be impossible to comply with and hence could be ignored or discredited by the persons to whom it is addressed. Although this risk exists, the author of this study believes that it is mitigated by several legal and jurisprudential safeguards, four of which will be mentioned below.

First, although it is true that the notion of personal has so far been broadly interpreted by the CJEU and other competent authorities, it still has limitations. In the opinion of the author, the test of identifiability discussed above still operates as a 'guard rail' preventing the notion of personal data from deviating too far. This test indeed requires taking into consideration the "*reasonable means*" which exist to identify a person. This risk-based analysis is grounded in factual and objective factors, such as the costs of and the amount of time required for identification, the available technology at the time of the processing and technological developments. And since anonymization and re-identification techniques are meant to indefinitely compete with one another, driven by opposite yet equally powerful interests, the author believes that it is highly unlikely that, one day, re-identification techniques will 'beat' anonymization techniques in all circumstances.

A second important safeguard in this respect is that the interpretation given by the EDPB, DPAs, national courts and the CJEU to the notion of 'personal data' – far from being purely technocratic – is usually driven by the dual objectives of EU data protection law, i.e., its FRO on the one hand, and its IMO on the other hand. In the opinion of the author, these authoritative bodies will continue ensuring that EU data protection law remains consistent with these two dual objectives, sometimes by putting limitations to its scope, or by adjusting the level of obligations resulting from its application. The Working Party 29, in one of its very first opinion, stressed the importance of interpreting EU data protection law in accordance with its FRO, in the following terms: "*[EU data protection law] clearly state[s] the ultimate purpose of the rules contained therein: to protect the fundamental rights and freedoms of natural persons (...). This is a very important element to take into account in the interpretation and application of the rules of both instruments. It may play a substantive role in determining how to apply the provisions of [EU data protection law] to a number of situations where the rights of individuals are not at risk, and it may caution against any interpretation of the same rules that would leave individuals deprived of protection of their rights*" (emphasis added). In the opinion of the author, it is therefore highly unlikely that EU data protection law would completely lose all its meaning because of the expansion of its scope. The existing enforcement practices of courts and DPAs already tend to confirm that the latter are keen to adopt a restrictive, reasonable and/or reality-grounded approach. DPAs and courts indeed often adjust corrective measures to the nature of the infringement and the potential difficulties in complying with a rule, by taking into account all relevant attenuating or aggravating circumstances, including the nature, gravity and

duration of the infringement, the intentional or negligent character of the infringement, the occurrence of an unforeseen or emergency situation (such as the COVID-19 pandemic), the existence of rapid technological changes, or the actions taken by the controller or processor to mitigate the damage suffered by data subjects.⁶⁹¹

A third important point is the fact that compliance and disobedience do not only depend on controllers and processors, but also on data subjects and DPAs. Unlike King Rex's laws indeed, the GDPR not only imposes obligations on controllers and processors, but also confers rights on data subjects and powers on DPAs. Hence, while data controllers and processors may be tempted to disobey data protection rules because they would consider them "*difficult if not impossible to comply with*", DPAs and data subjects on the other side could become fervent supporters of its application. In the opinion of the author, the expanding scope of EU data protection law should be considered not only in its potentially dysfunctional dimension (as far as duty-bearers are concerned) but also in its functional dimension (as far as data subjects and DPAs are concerned). Purtova does not discuss this tension, which may steer the courts and competent authorities towards a meaningful and functional interpretation and application of EU data protection rules in the long run.

Last but not least, there exists several clear limitations to the material scope of the GDPR, which will in any case prevent it from becoming the '*law of everything*'. These limitations are provided in Article 2(2) GDPR itself. Among those situations, the 'household exemption' is of particular importance in guaranteeing that the GDPR does not unduly invade the life of private individuals who may be processing personal data in the course of personal activities, such as when writing a digital diary, corresponding with their friends, or planning a family holiday. This specific exemption, and the way it safeguards the functionality of the GDPR, will be discussed in more details in Section 3.1.1.3 here below.

All in all, the author therefore believes that the Negroponte shift – far from disserving the rights and freedoms of data subjects – could become beneficial to them. The fact that the GDPR could one day become the law of *almost* all processing operations should not be seen as intrinsically problematic. To the contrary, the 'datafication' of the world may ultimately provide more venues for individuals to have their rights and freedoms respected. Moreover, the expanding scope of EU data protection law is not infinite; there exist several exemptions and exceptions meant to ensure that the GDPR does not become unnecessarily burdensome. Purtova herself admits that by stating that "*the broad interpretation of the concept 'personal data' and the resulting broad legal protection are not the core of the*

⁶⁹¹ Most of these elements are also listed in Article 83 of the GDPR on the conditions for DPAs to impose and administrative fine on a controller or processor following an infringement of data protection rules by the latter.

problem (...)." Rather, Purtova warns about the difficulty for controllers and processors to actually comply with a potentially "*all-encompassing*" framework.⁶⁹²

Of course, the author agrees that compliance may become challenging for some actors, especially for small controllers or processors which got indirectly caught in the material scope of the GDPR and may be confronted to issues such as re-identification or contamination. Yet, the author also believes that the four safeguards mentioned above, and in particular the clear limitations set in Article 2(2) GDPR (analysed below), as well as the reality-grounded stance of the authorities and other competent bodies in charge of interpreting and applying EU data protection law,⁶⁹³ will prevent the entire framework from becoming senseless or unsustainable. Furthermore, the author believes that the functionality of EU data protection law itself in ensuring the protection of important fundamental rights and freedoms in the digital sphere may participate to its long-term legitimacy and enforceability. This specific point will further be discussed in the concluding remarks on the scope of the GDPR and exemplified in the following Chapter of this study through several case-studies. Before this, however, it is first important to discuss the limits to the material scope of the GDPR, as established in Article 2(2) of the GDPR itself.

3.1.1.3. Limitations to the material scope of the GDPR as a way to respect the prerogatives of Member States and balance diverging rights and interests

If the broad scope of the GDPR is indeed a structural element of its multi-functionality, as argued above, the limitations to this scope must also be taken into account within this analysis. In that perspective, due regard must be paid to Article 2(2) of the GDPR, which specifies that the GDPR does not apply to the processing of personal data in four types of situations. The question whether these limitations could, overall, hinder the multi-functionality of EU data protection law must be appreciated in light of its purpose and function in society, as further developed below.

(i) Brief analysis of the public law exceptions set in Article 2(a), (b) and (d) GDPR, and of their restrictive interpretation by the CJEU

⁶⁹² Purtova, N. (2018). *op. cit.*, p. 78.

⁶⁹³ In particular, Article 83 of the GDPR requires DPAs to consider various factual elements when deciding whether to impose an administrative fine, such as the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them, the degree of responsibility of the controller or processor, the degree of cooperation with the DPAs that the controller/processor has shown in order to remedy the infringement and mitigate the possible adverse effects, etc.

Article 2(2) of the GDPR delineates the material scope of the GDPR by providing that this Regulation does not apply to the processing of personal data in four types of situations:

- (a) when processing takes place in the course of an activity which falls “*outside of the scope of Union law*” (e.g. by a Member State for the purpose of national security);
- (b) when processing is conducted by Member States carrying out activities relating to the EU common foreign and security policy (e.g. the organisation of EU civilian and military missions around the world);
- (c) when processing is conducted by a natural person in the course of a “*purely personal or household activity*” (e.g. keeping a personal diary or sending private emails to friends or relatives); and
- (d) when the processing is carried out by competent authorities in criminal matters, including the safeguarding against and the prevention of threats to public security (e.g. the filing and sharing of data relating to detection of criminal offences by the police).

Exceptions (a), (b) and (d) can be referred to as ‘public law exceptions’, since they all relate to processing activities carried out by state authorities for public purposes, such as public security or the enforcement of criminal law. The exception listed under letter (c), by contrast, belongs to the field of private law, and is often referred to as the ‘household exemption’.

In theory, each of these exceptions could deprive data subjects from the possibility to rely on the GDPR for defending their fundamental rights or freedoms and could thus contribute to the dysfunctionality of the entire framework if too extensively used or too widely interpreted. In practice, however, these limitations have been counter-balanced by other instrument of EU data protection law, such as the Law Enforcement Directive, and have always been interpreted restrictively by the CJEU.⁶⁹⁴ The first and second limitations set out in Article 2(2) GDPR will not be extensively discussed in this study as they relate to the legislative competence of EU itself. As already explained indeed, this study primarily focuses on the *internal* factors of functionality of EU data protection law (i.e., the elements which can be found within the text of the law itself). External factors influencing the functionality of EU data protection law, such as the political stability of a country, the existence of a backlog in the judicial system of some Member States, or (in this case) the limited competences of the EU legislator, fall outside of the scope of this study. Similarly, the

⁶⁹⁴ See, among others, CJEU, Case C-101/01, *Lindqvist*, Case C-25/17, *Jehovan todistajat*; Case C-311/18, *Schrems II*; or, more recently, Case C-306/21, *Koalitsia*.

last limitation mentioned in Article 2(2) GDPR – i.e., the processing of personal data by competent authorities in criminal matters – will not be extensively discussed in this study, because it is compensated by the application of another instrument of EU data protection law, i.e., the Law Enforcement Directive (‘LED’). The LED, which entered into force at the same time as the GDPR, set rules for data processing by law enforcement agencies, such as the police, which are very similar to the GDPR, even if they generally allow for more limitations.⁶⁹⁵ In other words, the LED can be seen as filling the gap left by Article 2(2)(d) GDPR.⁶⁹⁶ Since the primary focus of this study is the functionality of the GDPR, the author will not explore whether the LED adequately palliates the non-applicability of the GDPR to criminal matters.

It cannot be denied, however, that if the ‘public law exceptions’ set in Article 2(2)(a) and (b) GDPR had been interpreted and applied extensively, they could have turned into Trojan horses impeding the functionality of the GDPR from the inside. Hence, it remains essential for the effectiveness and functionality of EU data protection that such exceptions are interpreted restrictively. This is exactly what the CJEU did in several landmark cases, and in particular in *Lindqvist*, *Puškár*, *Schrems*, as well as in the joined cases *La Quadrature Du Net* and *Ordre des barreaux francophones et germanophones*, as briefly highlighted here below.

In *Lindqvist*, it had been argued by Mrs Lindqvist that individuals who make use of their freedom of expression to create internet pages in the course of a leisure activity are not carrying out an economic activity falling within the scope of EU law, and therefore that such individuals do not have to comply with EU data protection law. Against this rhetoric, the CJEU ruled that the activities mentioned by way of example in the ‘public law exceptions’ were all related to important purposes of public interest conducted by state authorities, such as public security, defence, or processing operations in criminal matters, and that this exception therefore did not apply to processing activities conducted by private individuals, whether economic or not.⁶⁹⁷ In *Puškár*, the CJEU went one step further by stating that, even if a processing activity was carried out by the State for *potentially* detecting a criminal offence (in this case, tax fraud), EU data protection law would still apply to such processing activity. In the case in the main proceedings, the personal data at issue had been collected and used by the Slovakian authorities for the purpose of collecting tax and combating tax fraud. Mr. Puškár – the claimant in the main proceedings – had attempted to object to the inscription of his name on a governmental list of so-called ‘white horses’ (individuals potentially acting as straw men for one or several

⁶⁹⁵ Hoofnagle, C., van der Sloot, B. & Zuiderveen Borgesius, F. (2019). *op. cit.*, p. 75.

⁶⁹⁶ For example, the owner of an apartment looking for a short-term tenant on a specialised website may be discriminating against coloured people. This will not be considered as “processing of sensitive personal data” under the GDPR, because the owner is looking for a short-term tenant as part of purely personal activities. However, the website itself may be sanctioned under the GDPR if it requires prospective tenants to upload a picture of them revealing their ethnic origins, and give owners access to these pictures before any contract may be formed. See in this respect the new strategy adopted by Airbnb: <https://news.airbnb.com/update-on-profile-photos/>.

⁶⁹⁷ CJEU, Case C-101/01, *Lindqvist*, para. 43.

companies), and had requested the erasure of his name from this list by relying on the 1995 Data Protection Directive, which was applicable at that time.⁶⁹⁸ In this context, arose the question whether the processing activity at stake did not fall outside of the scope of the Directive because carried out by state authorities for the purpose of crime detection, i.e., an area traditionally falling outside of the scope of EU law.⁶⁹⁹ Making a restrictive interpretation of this exception, the CJEU ruled that even if the data of Mr. Puškár could be used in criminal proceedings, they had not been collected “for the *specific purpose of the pursuit of such criminal proceedings (...)*”⁷⁰⁰ (emphasis added). Hence, the CJEU ruled that Mr. Puškár could exercise his rights under the 1995 Data Protection Directive against the Slovakian authorities.

In *Schrems II*, the CJEU had to rule on the validity of the adequacy decision adopted by the Commission for the transfers of personal data from the EU to the US. The claimant in the main proceedings (Maximilian Schrems) was arguing that such transfers were unlawful because the US could not be considered as guaranteeing an adequate level of protection for personal data of EU citizens, given the intrusive surveillance practices of the NSA. The transfers in question were carried out by Facebook Ireland (i.e., the EU data exporter) towards Facebook, Inc. (i.e., the US data importer). In this context, the question arose whether the 1995 Data Protection Directive/ the GDPR could apply to the transfer of personal data by an economic operator established in a Member State (Facebook Ireland) to another economic operator established in a third country (Facebook US), in circumstances where the data could possibly be processed by the authorities of that third country for the purposes of public security, such as counter-terrorism surveillance. In other words, the CJEU was requested to determine whether such processing activity was falling within the exception set in Article 2(2)(a) GDPR, because of the surveillance operations conducted by the NSA or by similar intelligence agencies. In this respect, the CJEU pointed out that the main processing activity at stake was *not* carried by a state authority, but rather by two economic operators (i.e., Facebook Ireland and Facebook, Inc.).⁷⁰¹ Keeping this fact in mind, the CJEU clarified that the processing activities of two economic operators “cannot fall outside the scope of the GDPR” simply on the ground that the personal data which were transferred from one country to another were “liable to be processed by the authorities of the third country concerned, for the purposes of public security, defence and State security.”⁷⁰² As a result, the CJEU confirmed that the processing activities in question were falling within the scope of EU data protection law.

The judgments of the CJEU in the case *Privacy International* and the joined cases *La Quadrature Du Net* and *Ordre des barreaux francophone et germanophone* further tend to confirm that EU data protection law may infiltrate almost all areas which

⁶⁹⁸ *Ibid.*, para. 26.

⁶⁹⁹ *Ibid.*, para. 35.

⁷⁰⁰ *Ibid.*, paras. 39-40.

⁷⁰¹ CJEU, Case C-311/18, *Schrems II*, para. 85.

⁷⁰² *Ibid.*, paras. 88-89.

were once the sovereign prerogative of Member States, including, to some extent, national security. In these two cases indeed, the CJEU ruled that the e-Privacy Directive, once interpreted in light of Article 7 and 8 of the Charter, does not allow the bulk retention and transmission of traffic and location data by private operators, unless Member States can prove serious threats to national security.⁷⁰³ These rulings show how the CJEU may still interpret EU data protection law for the benefit of data subjects' fundamental rights in a manner that is permeable to questions of national security – an area which has traditionally remained outside of the European integration process, but tends to be indirectly framed by EU law.⁷⁰⁴ As further discussed in the final Chapter of this study, Article 8 of the Charter plays a functional role as well in that context. In particular, it operates as a bridge between, on the one side, the limited scope of EU secondary law and, on the other side, national laws and policies falling within the exclusive competences of Member States.

More recently, the CJEU has confirmed that the GDPR applies to the processing of personal data in the context of the organisation of national elections. By adopting a restrictive reading of Article 2(2)(a) GDPR, the CJEU has indeed confirmed that national elections cannot be considered as a matter of public security *per se*, and that the processing of voter's data therefore fall within the scope of EU law. As a result, DPAs are competent to use their powers under the GDPR to supervise the processing of voters' personal data, including by imposing a limitation or a ban on the processing of some data where deemed necessary for compliance purpose (in this case, a ban on the recording of images by private actors of the counting of ballots).⁷⁰⁵

As said above, the legislative competence of the EU legislator is an external factor of the effectiveness and functionality of EU data protection law. Since this study primarily focuses on the internal factors of functionality of EU data protection law, and in particular of the GDPR, such exceptions will not be discussed any further. The above-mentioned case-law clearly shows however that these public law exceptions have always been interpreted restrictively, usually to the ultimate benefit of the rights and freedoms of data subjects. Besides these 'public law exceptions', another limitation to the material scope of the GDPR exists, i.e., the 'household exemption'. Understanding this exemption is particularly relevant for the purpose of this study. If interpreted too broadly indeed, such an exemption could impede the material scope and thus functionality of the GDPR. By contrast, if interpreted too restrictively, many trivial processing activities conducted by individuals in the course of their daily life may fall within the scope of the GDPR, which may in turn render EU data protection law too burdensome and thus dysfunctional. The below sub-section will precisely

⁷⁰³ CJEU, Judgments of 6 October 2020 in Case C-623/17, *Privacy International*, and in Joined Cases C-511/18, *La Quadrature du Net and Others*, C-512/18, *French Data Network and Others*, and C-520/18, *Ordre des barreaux francophones et germanophone and Others*

⁷⁰⁴ Zalnieriute, M. (2022). A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union. *Modern Law Review* 85.1, 198-218. Web.

⁷⁰⁵ CJEU, *Koalitsia "Demokratichna Bulgaria - Obedinenie"*, Judgment of 20 October 2022.

discuss the extent and limits of the household exemption and assess its impact on the functionality of the GDPR.

(ii) Extent and limits of the household exemption – establishing a balance to allow the GDPR to function in society

Article 2(2)(c) GDPR provides that this Regulation does not apply to the processing of personal data by a natural person “*in the course of a purely personal or household activity*”.⁷⁰⁶ Personal or household activities include, for example, private correspondence (e.g. exchanging emails or texts with family, friends or members of a private chat group), the holding of records of addresses or other contact details for personal purposes (e.g. updating a paper or digital address book used for personal purpose), or more generally social networking, including on social media, as long as the social media account or page remains directed towards the private sphere, in the sense that it is not open to an indefinite number of people.⁷⁰⁷

It is important to already clarify that, although the individuals conducting a purely personal activity may not have to comply with the GDPR, the intermediaries which make such processing possible in their professional capacity remain liable under EU data protection law.⁷⁰⁸ Hence, when individuals share family pictures on their private Facebook account, they may not have to comply with the GDPR (and thus will not have, for example, to inform the family members in question about such processing prior to publishing the picture), but Facebook, Inc. by contrast will have to comply with the GDPR, including by ensuring the security of the data in storage, answering any erasure requests from a data subject, or keeping a record of processing activities up-to-date.⁷⁰⁹

By establishing this household exemption, the aim of the EU legislator was thus not to create a ‘no-rights zone’, but rather to allow individuals to process personal data in the course of their private life without having to comply with a burdensome set of obligations, such as the duty to inform the individuals concerned at the time of the collection of their personal data, or the obligation to verify that each processing activity has a valid legal basis under Article 6, 9 or 10 GDPR. In other words, Article 2(2)(c) GDPR aims to establish a balance between, on the one side, the right to personal data protection of data subjects and, on the other side, the rights and freedoms of individuals who process personal data in the course of purely personal activities (including their right to privacy, freedom of thought or freedom of

⁷⁰⁶ Article 2(2)(c) GDPR.

⁷⁰⁷ CJEU, Case C-101/01 *Lindqvist*, Judgment of 6 November 2003, para. 47; CJEU, Case C-25/17, *Jehovan todistajat*, Judgment of 10 July 2018, para. 42.

⁷⁰⁸ Recital 18 of the GDPR, last sentence.

⁷⁰⁹ For example, the owner of an apartment looking for a short-term tenant on a specialised website may be discriminating against coloured people. This will not be considered as “processing of sensitive personal data” under the GDPR, because the owner is looking for a short-term tenant as part of purely personal activities. However, the website itself may be sanctioned under the GDPR if it requires prospective tenants to upload a picture of them revealing their ethnic origin.

expression). The 4th Recital of the GDPR expresses the need for such a balance in the following terms:

*“The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to **its function in society** and be **balanced against other fundamental rights**, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity”* (emphasis added).

The references to the non-absolute nature of the fundamental right to personal data protection and to its function in society echo the idea that the GDPR must remain a functional framework, in the sense that it should not disproportionately restrict the rights and freedoms of others, including of controllers who are natural persons. To assess whether such an exemption contributes to or hinders the functionality of the GDPR, it is essential however to analyse which type of activities can be considered as ‘*purely personal*’ and which one cannot, as clarified by the GDPR itself, the CJEU, the EDPB or national DPAs.

A first important element in this respect is the divide between one’s personal and professional life. The GDPR itself clarifies indeed that the terms “*purely personal*” and “*household*” must be understood as excluding professional or commercial activities.⁷¹⁰ Hence, keeping the contact details of customers or clients on a smartphone should not be considered as a ‘*purely personal purpose*’, even if the smartphone is also used for private purposes, and also contain the contact details of friends or family members. Sometimes, of course, the line between personal and professional activities can be difficult to distinguish, especially when one creates personal bounds with individuals encountered in a professional environment. In the opinion of the author, the context in which the processing takes place should be analysed on a case-by-case basis in order to determine whether such processing is conducted by an individual for purely personal reasons or not. In particular, the relation between the individuals concerned and the intention of the controller when processing the data should be carefully considered.

As an illustration, it could be argued that even if a close relation may exist between, for example, the children of a kindergarten and their caregivers, the latter will still have to comply with the GDPR when collecting or processing information relating to

⁷¹⁰ Recital 18 GDPR.

those children in the courses of the activities of the kindergarten, such as when registering dietary requirements (e.g. food allergies or intolerances), monitoring the children's behaviours in a shared calendar (e.g. sign of sickness, behavioural changes, etc.), or taking and sharing pictures of the children on the social media page of the kindergarten with a view of informing (prospective) parents on the type of activities in which the children take part (e.g. crafting ; singing; etc). By contrast, if a caregiver develops a personal relation with a family outside of the professional environment of the kindergarten, the messages that the caregiver may exchange with the parents, or the pictures that the caregiver may take with their child outside of her working hours could be considered as being covered by the household exemption, depending on the overall context in which such processing took place (e.g. was the purpose of the communications professional or purely private? Were the pictures published on the social media page of the kindergarten or kept in a photos library on the private phone of the caretaker? etc.).

Even in the absence of a professional context, the line between 'a *purely personal activity*' and other activities may sometimes be difficult to distinguish. One may refer, for example, to the sharing of videos on YouTube or TikTok, the recording of images for domestic surveillance purpose, or the posting of stories or comments on internet websites which include information about other individuals. In this respect, it must be acknowledged that the CJEU has already adopted a quite restrictive reading of the household exemption in its case-law, to the benefit of a broader scope of the GDPR. In *Lindqvist*, in particular, the CJEU has ruled that social networking or blogging must comply with the GDPR when information relating to other individuals is shared with an indefinite number of people on the internet, and is thus directed '*outwards*' from the private setting of the person sharing that content.⁷¹¹ A decade later, in *Ryneš*, the CJEU also specified that domestic video-surveillance cameras which are (even partially) directed towards a public space, such as a public street, is a type of processing of personal data which falls within the material scope of the GDPR, given that the cameras are directed outwards from the private property of the individual and towards a public space.⁷¹² In *Jehovan Todistajat*, the CJEU also took the view that door-to-door preaching activities, although intrinsically linked to the faith of the preachers, could not benefit from the household exemption, given that such activities aimed at recruiting new members and were thus directed *outwards* from the private setting of the preachers.⁷¹³ Individuals may therefore not stretch the notion of a '*purely personal activity*' to activities that are (even slightly) directed *outwards* from their private sphere.⁷¹⁴

From a fundamental rights perspective, if the GDPR had also applied and therefore put restrictions on the processing of personal data by individuals in the context of

⁷¹¹ CJEU, Case C-101/01, *Lindqvist*, Judgment of 6 November 2003, para. 47.

⁷¹² CJEU, Case C-212/13, *Ryneš*, Judgment of 11 December 2014.

⁷¹³ CJEU, Case C-25/17, *Jehovan todistajat*, Judgment of 10 July 2018, para. 44.

⁷¹⁴ CJEU, Case C-25/17, *Jehovan todistajat*, Judgment of 10 July 2018, para. 44.

purely personal activities (such as when organising their private affairs, ensuring the security of their home, or exercising their freedom of expression in a private context), it would have not been practical or functional in a democratic society, and would have certainly not served mankind. By contrast, if the GDPR would have not regulated the processing of personal data by individuals *at all*, even when such processing would have been directed outward from their private sphere, it could have left these third parties quite powerless against abuses and could therefore have been detrimental to the fundamental rights and freedoms of data subjects. In the opinion of the author, the manner in which the CJEU has interpreted Article 2(2)(c) GDPR thus creates the necessary room to accommodate these (sometimes) conflicting interests and rights, and to ensure that the mechanics of the GDPR operate smoothly “*in relation to its function society*”. The ‘household exemption’, although limiting the material scope of EU data protection law, can therefore also be considered as a factor of functionality of the overall framework.

As discussed in the next Chapter of this study, the author believes that the borders of the ‘household exemption’ as established by the CJEU are particularly important when envisaged in the context of the online sharing of personal data on the internet. If the household exemption would be interpreted more restrictively by national DPAs or courts, it could indeed prevent victims of online abuses to exercise their data protection rights against abusers or internet service providers. At the end of the day, whether the household exemption appropriately frames the application of EU data protection law or on the contrary impairs its functionality must be appreciated in practice, taking into account, *inter alia*, the emergence of new DDTs that may undermine the level of protection of the fundamental rights of data subjects. The next Chapter of this study will precisely test the functionality of the GDPR with respect to its material scope in the context of online networking and potential cases of harassment (see in particular Section 4.1.4 below).

3.1.1.4. Concluding remarks: the objective and technology-neutral approach to the notion of ‘personal data’ and of ‘processing’ as factors of functionality of EU data protection law

Based on all the above considerations, it appears that four elements render the material scope of the GDPR particularly functional for data subjects seeking to assert their rights, or for DPAs and national courts seeking to enforce the GDPR. The first of these factors, which has been discussed above, is the broad meaning which has been ascribed to the notions of ‘processing’ and of ‘personal data’ in the legislation and the case-law of the CJEU, as well as the expanding scope of data processing activities through multiple phenomena, such as the Negroponte shift, the failure of anonymisation, or the contamination theory. As argued above indeed, the broad interpretation given to these two central notions has increased the variety of situations where data subjects can rely on EU data protection law to assert their rights and freedoms.

Besides this, a second factor which, in the opinion of the author, contributes to the functionality of EU data protection law, is the *objectiveness* of its material scope. Indeed, the application of the GDPR does not require any value judgment or subjective reasoning as to whether the right to privacy of data subjects, or any other important right or freedom, has been disproportionately interfered with. The mere objective fact that personal data are being processed will trigger the application of EU data protection law. In other words, no subjective pre-assessment as to whether a fundamental right or freedom may have been violated is necessary for EU data protection law to apply.

Thirdly, another important factor which participates to the functionality of the GDPR is the *absence of any quantitative condition* attached to the notion of ‘processing’ or ‘personal data’. As seen above indeed, there is no *de minimis* rule under EU data protection law. The processing of even *one type* of personal data, such as an IP address or a single picture, will trigger the application of EU data protection law. Similarly, even if the processing operations are minimal in scope or in time (e.g. limited to the anonymisation or deletion of personal data only), this will not prevent the data subjects from exercising their rights, or exempt the controller or processor performing such operations from complying with the GDPR. This means that any type of processing operation susceptible of affecting the rights and freedoms of data subjects – regardless of its voluntary or accidental nature, the amount of data, and whether it lasted a tenth of a second or a decade – can fall within the scope of the GDPR, which in turn will enable data subjects to benefit from its protective effect.

Lastly, in the opinion of the author, a fourth factor of the functionality of the GDPR relates to the fact that data processing operations that depend on the input of data subjects usually leave traces or evidence that can later be used to challenge their lawfulness. As an illustration, when a data subject repeatedly receives unsolicited marketing emails from a company, there will be no doubt about the fact that personal data have been processed; the marketing emails themselves will operate as evidence that the company has indeed processed the personal data of that individual. By contrast, if a salesman knocks on somebody’s door (although uninvited), it will be more difficult for the person in the house to prove such a behaviour in the context of a complaint. This element of ‘provability’ of data processing activities will in most instances facilitate the use of EU data protection law by data subjects. A *condition sine qua non* for this factor of functionality to exist, however, is that the data subject must be aware of the processing in the first place, either because they have been informed of it (as should be the case),⁷¹⁵ or because the processing activity produces visible effects (e.g. confirmation email; copy of the result of an automated decision; etc.). There may be cases where a controller does not fully comply with its information obligations under Article 13-14 GDPR, or where no tangible evidence are provided; in these cases, the processing activities can

⁷¹⁵ Article 12 to Article 14 of the GDPR.

remain (at least partly) invisible, thereby leaving data subjects or DPAs unaware of the fact that EU data protection law may apply. This, however, would imply that the controller already infringes the GDPR by failing to properly inform the data subject about the processing in the first place. This potential element of dysfunctionality of EU data protection law must thus be appreciated together with the transparency obligations incumbent on controllers (see Section 3.2.2, below), the right to information of data subjects (see section 3.2.3 below), and the existence of supervision mechanisms as well as deterrent sanctions (see section 3.3 below), which can ultimately help bringing the existence of a processing activity to light, and thus palliate this issue.

3.1.2. The territorial scope of the GDPR, or the law which applies 'everywhere'

The territorial scope of the GDPR can also be considered, at least *prima facie*, as a structural factor of the effectiveness and functionality of EU data protection law. The global reach of EU data protection law, which already existed under the 1995 Directive, has always been an essential component of its effectiveness and functionality. As already discussed above indeed, personal data can easily and quickly be transferred from one jurisdiction to another at almost no costs (see Section 2.1.3). Hence, if the effects of EU data protection law had been strictly limited to the territory of the EU, it would have been easy for controllers or processors to circumvent these rules by establishing subsidiaries abroad and conducting all their processing activities outside of the EU.

Since the adoption of the 1995 Data Protection Directive, much ink has been spilled on the far-reaching territorial scope of EU data protection law in numerous books and articles.⁷¹⁶ The purpose of this section is not to analyse in detail the doctrine, legal provisions and case-law on such extraterritoriality. Rather, the purpose is to generally point out that the GDPR has achieved a level of protection for data subjects that go beyond the borders of the EU, and which put the protection of their fundamental rights and freedoms at its heart.

In particular, Article 3 GDPR provides:

⁷¹⁶ See, for example, Gömann, M. (2017). The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement. *Common Market Law Review*, 54(2), 567-590; Vermeulen, Gert, and Lievens, Eva. Reconciling the (extra)territorial Reach of the GDPR with Public International Law. *Data Protection and Privacy Under Pressure. Transatlantic Tensions, EU Surveillance and Big Data*. Maklu, 2017. 77-100. Web; Granmar, C. (n.d.). *Global applicability of the GDPR in context*. Available at <http://su.diva-portal.org/smash/get/diva2:1274839/FULLTEXT01.pdf>; Kindt, E. (2016). Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 32(5), 729-748. Kuner, C. (2017, February 1) The Internet and the Global Reach of EU Law. 'The Internet and the global reach of EU law', in: Marise Cremona and Joanne Scott (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* 112-145 (Oxford University Press 2019); LSE Legal Studies Working Paper No. 4/2017; University of Cambridge Faculty of Law Research Paper No. 24/2017.

“1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.”

The extra-territorial reach of the GDPR derives from two types of situations : (i) it confer rights on data subjects located *outside of the EU* when the processing is conducted by a controller or processor located *in the EU*⁷¹⁷ ; and (ii) it imposes obligations on controllers or processors located *outside of the EU* when the latter process personal data of data subjects who are *in the EU*, either for offering them goods or services, or for monitoring their behaviours.

As an illustration, a Greek travel agency which processes the personal data of Chinese citizens for the purpose of offering them a personalised tour of the Greek islands will have to comply with the GDPR, regardless of the fact that the data subjects in question are living in China (as envisaged by Article 3(1) GDPR). The element which renders the GDPR applicable in this example is that the controller itself (i.e., the Greek travel agency) is located *in the EU*. It does not matter whether the processing operations conducted in the context of the activities of the Greek travel agency are taking place within or outside of the EU. For example, even if the Greek agency would store the personal data of its (prospective) Chinese customers on the server of its mother company located in the US, the GDPR would still regulate such processing operations.⁷¹⁸

⁷¹⁷ Every time the author refers to the EU in this section, such reference should be understood as covering both the EU and EEA territory. The GDPR is indeed a text of EEA relevance, which thus also applies in Iceland, Liechtenstein, and Norway. For the sake of brevity, however, the author will only use the abbreviation ‘EU’ rather than ‘EU/EEA’. Also, the expressions ‘EU data subject’ and ‘non-EU data subject’ should respectively be understood as referring to individuals located *in the EEA* or *outside of the EEA* at the time of the processing of their personal data.

⁷¹⁸ This has already been specified under the regime of the 1995 Data Protection Directive in the case *Google Spain*.

Similarly, a travel agency located in India which processes the personal data of individuals located in the EU with a view of offering them a personalised journey in India will have to comply with the GDPR. The territorial element which renders the GDPR applicable in this example is the fact that the non-EU controller (i.e., the Indian travel agency) is offering services to data subjects *located in the EU* (as envisaged by Article 3(2)(a) GDPR). Another important element is that it does not matter if the goods or services offered by the controller involve a monetary transaction. Hence, even if the data subjects do not accept the final offer made by the Indian travel agency, the processing operations that have been undertaken for the purpose of providing them with this offer will still be subject to the GDPR (e.g. collection of information about the prospective travellers, such as their name, email address, age, overall budget, travel preferences, etc.).

Finally, the GDPR will also apply when a non-EU controller or processor processes the personal data of EU data subjects for the purpose of the “*monitoring of their behaviours*” (as envisaged by Article 3(2)(b) GDPR). Such would be the case, for example, if an advertising company located in Australia was monitoring the online behaviours of internet users located in the EU to display personalised advertising on certain websites. The territorial element which renders the GDPR applicable in this example is the fact that the non-EU controller is tracking the behaviours of data subjects *located in the EU*.

These examples show that the GDPR can still apply beyond the external borders of the EU. It cannot be denied however that this system still suffers from a major weakness: the difficulty to enforce EU data protection law abroad. The difficulty to enforce EU rules abroad is however a limitation common to any piece of legislation with extra-territorial reach usually linked with the lack of communication or effective cooperation of EU and foreign enforcement bodies. This element can therefore be considered as an external factor of dysfunctionality. Given that the scope of this study is limited to the internal factors of functionality of EU data protection law, this problematic will not be extensively discussed by the author of this study. What remains relevant however is that, when drafting the GDPR, the EU legislator anticipated this potential element of dysfunctionality in the enforcement mechanisms of EU data protection law, and therefore inserted several articles aiming at palliating it. One may refer in particular to the following articles:

- **Article 27 of the GDPR:** this Article obliges foreign controllers and processors falling within the scope of the GDPR pursuant to its Article 3(2) to establish a representative in the EU, such as a sister company or a branch of the company. This obligation to appoint a representative in the EU offers an easier access to the controller in question and may thus facilitate communications, the exercise of data subject’s rights towards the controller, as well as enforcement procedures conducted by a DPA or a national court. It must be noted however that this Article 27 may in itself be difficult to

enforce, should a controller or processor fail to establish such a representative in the EU.

To illustrate the limits of this safeguard, one may refer to a complaint filed by the not-for-profit privacy organisation *noyb* with the Luxembourg DPA, the CNPD, in 2021 against the company RocketReach with respect to several violations of the GDPR. RocketReach is a company located in Bellevue, US, which collects, organises and sells the profiles of millions of individuals worldwide for the purpose of talent acquisition and recruitment.⁷¹⁹ Despite the fact that RocketReach is monitoring and profiling individuals located in the EU by collecting data about them from various sources, it did not establish any representative on the territory of an EU Member State, in breach of Articles 3(2) and 27 GDPR. Instead of investigating the matter, however, the CNPD declared that it did not have jurisdiction to do so, precisely because the controller was located abroad and had no representative in the EU. In the opinion of the author, although the CNPD erred in finding that they did not have jurisdiction over RocketReach,⁷²⁰ it would have nonetheless been practically impossible for the latter to directly sue the company in the US given the difficulties in enforcing the GDPR before a foreign jurisdiction (cf. language barrier; costs related to a procedure in the US; etc.). Furthermore, for this type of cases, educating the data subjects on the risk of sharing personal data with non-EU controllers that do not have a representative in the EU would not be sufficient to solve the issue, given that personal data about them are collected from various sources without their consent or participation. By contrast, when the data subjects are faced with the choice to share their personal data with a foreign controller, the existence of an EU representative may become a sign of compliance that could reassure the data subjects in question, and thus provide a competitive advantage to the controller in question compared to other foreign controllers offering similar services or goods that would not have established an EU representative. In general, it can indeed be assumed that data subjects would feel more comfortable entering into a contractual relation with a foreign controller that has a branch in the EU, as this gives them the possibility to exercise their rights more easily, either directly (by contacting the representative) or indirectly (by filing a complaint with a DPA against that representative). In this respect, it is worth noting that the GDPR allows controllers and processors to get certified under approved certification mechanisms, as envisaged in Article 42 GDPR. These data protection certifications, seals or marks can be issued by a DPA or an approved

⁷¹⁹ See RocketReach official website at https://rocketreach.co/about_us.

⁷²⁰ The absence of an EU representative pursuant to Article 27 GDPR does not deprive a DPA from the possibility to initiate a legal action directly against the concerned foreign controller for alleged violations of the GDPR, including for the violation of Article 27 GDPR itself. This is confirmed by Article 27(5) GDPR, which provides: *“The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.”*

certification body, with the aim to enhance transparency over compliance.⁷²¹ A requirement that could be imposed on foreign controllers or processors willing to get one of these certifications, seals or marks could be to have a representative in the EU pursuant to Article 27 GDPR. This would allow data subjects to quickly assess the level of data protection of relevant products and services and be reassured about the fact that a legal action can be initiated in the EU against the representative in the event of a breach of the GDPR by the foreign controller.

- **Articles 46 of the GDPR:** this Article requires EU-based controllers or processors to put in place (contractual) safeguards when they transfer personal data to a third party located outside of the EU/EEA, in order to avoid that the level of data protection guaranteed in the EU drops once data are transferred to a data importer located in a third country; and
- **Article 50 of the GDPR:** this Article provides for rules on international cooperation for the protection of personal data. It enables the EU to cooperate with foreign authorities to hold foreign controllers or processors accountable. International cooperation may however be difficult to achieve since it depends on the willingness of third countries to engage time and resources in helping the EU to enforce data protection law within their territory.⁷²²

These three articles can be considered as increasing the functionality of EU data protection law overall, in the sense that they preventively address the difficulties of enforcing EU data protection law abroad. Despite those measures, some controllers can still decide to adopt strategies to minimise the amount of data processing operations that could fall under the territorial scope of the GDPR. As an illustration, shortly before the first day of application of the GDPR on 25 May 2018, Facebook virtually moved 1.5 billion non-EU users' profiles out of reach of the GDPR by transferring them from the servers of Facebook Ireland (i.e., a company subject to the GDPR) to the servers of Facebook, Inc. (i.e., located in California, US, and therefore not directly subject to the GDPR).⁷²³ If Facebook had not made such a transfer, all the concerned users would have *de lege* benefitted from the protection of the GDPR, even though not living in the EU, because the controller (Facebook Ireland) would have been in the EU. This illustrates how EU data protection law may ultimately fail at protecting individuals against harmful data processing practices

⁷²¹ Recital 100 of the GDPR. Article 42 of the GDPR.

⁷²² Taking into account the existing cultural and legal divergences in the field of data protection, it is very difficult to imagine a strong international cooperation between the EU and countries like China or the US. Cooperation further becomes inconceivable in countries where diplomatic relations with the EU are tensed or non-existent.

⁷²³ *Facebook moves 1.5bn users out of reach of new European privacy law*, by Alex Hern, 19 April 2018, available at : <https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law>.

where the controllers or processors are not located in the EU and actively put in place strategies to avoid the application of the GDPR to (part of) their processing activities. Such limitation could be an important factor of ineffectiveness or dysfunctionality of EU data protection law, especially taking into account the ease with which personal data may be transferred to different actors across the globe. Given that such considerations belong to the realm of *external* factors of (dys)functionality, they will however not be extensively discussed in the last two Chapters of this study. What remains relevant, at this stage, is to acknowledge that the GDPR can apply beyond the physical borders of the EU, where a link exists with the EU. In theory, this broad territorial scope thus enables the GDPR to apply ‘everywhere’, for the general benefit of data subjects.

3.1.3. The personal scope of the GDPR, or the law which concerns ‘everyone’

The GDPR does not contain any specific provisions on its personal scope of application. Rather, such personal scope may be inferred from the structure and content of the GDPR as a whole. When discussing the personal scope of the GDPR, three different categories of actors can be distinguished in particular: (i) data subjects, in their capacity as rights holders; (ii) controllers or processors, in their capacity as duty bearers and (iii) and the DPAs, in their capacity as supervisory authorities. This section will briefly highlight the main elements that will trigger the application of the GDPR vis-à-vis each of these categories of actor, and how this personal scope may also participate to the functionality of EU data protection law.

3.1.3.1. Data subjects as right holders – “*data relate to me, therefore I am*”

EU data protection law gives the name of ‘data subjects’ to its right holders. The expression ‘data subject’ is not defined as such in the GDPR but is comprised within the definition of ‘personal data’. Article 4(1) GDPR indeed defines personal data as “*any information relating to an identified or identifiable natural person (‘data subject’)*”. The notion of ‘data subject’ is thus intrinsically linked to the notion of personal data. Consequently, the broad meaning which has been ascribed to the notion of ‘personal data’ also indirectly benefit data subjects under the GDPR. Because every personal data necessarily relates to a data subject, one cannot go without the other. The functional elements pertaining to the notion of ‘personal data’ (and in particular, its broadness, objectiveness, non-quantitative threshold, and provability) therefore also spill over the notion of data subject.

Data subjects do not have to fulfil any additional conditions for becoming right holders under the GDPR. There exists, for example, no specific requirement relating to the age, nationality, citizenship or *compos mentis* of the individuals concerned.

Both children and adults, regardless of whether they are EU citizens and/or able to enter into contractual relations, may thus exercise their rights under the GDPR (either directly or through a representatives) as soon as information relating to them are being processed. The absence of any additional condition for individuals to gain the status of 'data subject' therefore makes this notion particularly functional for the concerned addressees.

As already mentioned above, a clear limitation to the notion of 'data subject' is that only *living* natural persons can benefit from such a status under EU data protection law. By contrast, legal persons, deceased persons or other living things (such as animals or plants) cannot be considered as '*data subjects*' under EU data protection law.⁷²⁴ This, of course, appears logical given that the primary objective of the GDPR is to ensure the protection of the fundamental rights and freedoms of natural persons whose personal data are being processed. In the opinion of the author, extending the personal scope of EU data protection law to other categories of right holders would contradict the very objective and DNA of data protection law, as discussed in the second Chapter of this study (see in particular Section 2.1.5, above). Furthermore, this limitation to the personal scope of EU data protection law has been interpreted restrictively since the adoption of the 1995 Data Protection Directive already, in the sense that information relating to deceased persons can still be considered as personal data if they relate in content, in purpose or in effect to living individuals, such as relatives of the deceased persons. As an illustration, a family tree can provide information about both deceased persons and living descendants and must therefore still be considered as containing personal data. In some instances, information about an ancestor can even fall within the category of *sensitive* personal data, as protected under Article 9 or 10 GDPR. Such would be the case, for example, with respect to information that an individual has suffered from a mental illness or a hereditary disease during their lifetime, given that such information can also relate to a living sibling or a child.⁷²⁵ In some instances, the DNA profile of living individuals can also help confirming a crime committed by one of their ancestors. Given that the knowledge of a serious crime committed by deceased family members can leave a stigma on their descendants, such information could still be considered as relating to these descendants in *effect*.⁷²⁶ Information relating to deceased persons may thus still require protection under EU data protection law, as the case may be.⁷²⁷

⁷²⁴ This is made clear in several Recitals of the GDPR as well as guidance documents published by the Article 29 Working Party or the EDPB. In particular, the 27th Recital of the GDPR provides: "*This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.*"

⁷²⁵ WP29, Opinion 06/2013 on open data and public sector information ('PSI') reuse, adopted on 5 June 2013, WP207 1021/O00/EN, p. 24.

⁷²⁶ EURAT project group "Ethical and Legal Aspects of Whole Genome Sequencing", *Position Paper on the Release of Genomic Data to Patients and Study Participants*, Heidelberg, December 2019, DOI: 10.11588/fmk.2020.0.76125, pp. 65-66.

⁷²⁷ WP29, Opinion 06/2013 on open data and public sector information ('PSI') reuse, adopted on 5 June 2013, WP207 1021/O00/EN, p. 24.

All in all, the wide interpretation given to the notion of ‘personal data’, coupled with the pervasiveness of data processing activities in today’s globalised world and the broad territorial scope of EU data protection law, mean that every individual on earth is – or will probably be at some point – a ‘data subject’ under the GDPR. Furthermore, the fact that gaining such a status does not require the fulfilment of any additional condition beyond the processing of personal data makes it particularly easy for individuals to become right holders. This, in turn, render the GDPR particularly functional for individuals seeking to assert their data protection rights. The more data subjects will invoke EU data protection law, the more practitioners, DPAS, courts or other data subjects may gain knowledge about it, and may be keen to rely on it, thereby increasing its functionality in practice through a ‘snowball effect’. In view of this broad personal scope, EU data protection law might as well one day become the law that concerns everyone.⁷²⁸

3.1.3.2. Controllers and processors as duty bearers – “*I process data, therefore I must*”

Controllers and processors are two categories of duty bearers under EU data protection law. The below section will briefly distinguish each category of actors and the distinct regime of responsibility which apply to them. The author will then discuss how the different types of relations between these actors have been regulated to prevent a dilution of responsibility, and to safeguard the effectiveness and functionality of EU data protection. In a final section, the main factors of functionality attached to the notions of controller and processor and to the rules regulating their relations will be highlighted.

(i) A factual approach to the notion of ‘controller’ and ‘processor’

Any person processing personal data is necessarily a controller or a processor. There is no other status, and no exception in this respect. The nature, corporate form or objective of the person concerned has no impact on its qualification under the GDPR. Only one criterion is relevant: this person must be processing personal data. Controllers and processors can thus be both natural or legal persons; public authorities or private entities; multinational groups or a single self-employed worker; profit-driven companies or NGOs.

With respect to controllers, Article 4(7) GDPR provides:

“controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of

⁷²⁸ This expression echoes the one coined by N. Purtova, according to which the GDPR may be “*the law of everything*”.

such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”

With respect to processors, Article 4(8) GDPR provides:

“‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”

It clearly appears from these two definitions that the main difference between controllers and processors lies within their decision-making power. While controllers ‘determine’ the purposes and means of the processing, and therefore ‘control’ the personal data, processors merely execute the processing activities on behalf of the formers, after having been instructed to do so. Determining who is a ‘controller’ or a ‘processor’ therefore requires a factual assessment of any given situation.⁷²⁹ This factual analysis should encompass a series of questions relating to the decision-making power of the persons concerned, such as: who initiated the processing and for what purpose?; who decided which personal were to be collected and used for fulfilling that purpose?; who decided how long these data will be stored, or what technical means will be used (software and hardware)?; etc. At the end of the day, the person who has – in fact – determined the essential elements of the processing will be considered as the controller, even if that person did not perform or execute the processing activities himself/herself/itself, but instructed a processor to do so. The controller may also delegate the taking of some decisions to a processor, especially as far as far as technical or organisational questions are concerned.⁷³⁰ Yet, factually, only the controller can endorse the final option which will be retained. By contrast, processors can merely formulate suggestions before processing personal on behalf and under the instructions of the controller. As such, processors have thus no real decision-making power with respect to the essential elements of the processing. This also means that, when they are processing personal data on behalf of a controller, processors cannot use the personal data to achieve their own distinct purposes. If they do so, they will necessarily become controllers themselves.

One same person can of course qualify both as a controller and a processor, depending on the processing activities concerned. As an illustration, a payroll service provider, in charge of calculating and paying the salaries of the employees of a company, will be acting as the *processor* of that company when collecting, storing and using the personal data of the company’s employees in accordance with the instructions of the latter. At the same time however, this payroll service provider will also act as a controller when processing the personal data of its *own* employees for

⁷²⁹ WP29, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, 00264/10/EN, WP169, p. 8.

⁷³⁰ WP29, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, 00264/10/EN, WP169, p. 15.

paying their salaries, granting them leaves of absence, or deciding to promote them. In practice, it is thus rare that a controller or a processor will exclusively process personal data in that capacity; rather, almost all persons processing personal data will have a dual role of processor and controller, depending on the processing activity concerned.

The decision-making power of the controller can primarily derive from three different sources: (1) an explicit legal competence; (2) an implicit competence; and/or (3) a purely factual influence.⁷³¹ The Working Party 29 illustrates those three sources of control as follows: a social security institution which is entrusted by law with public tasks (such as granting social allowances or reimbursing medical fees to citizens) must be considered as the controller of the personal data necessary to fulfil these tasks. In that case, the 'control' stems from an *explicit legal* competence. Similarly, when an employer transfers the personal data of its employees to the tax authorities, the tax authorities must be considered as controllers because explicitly tasked with such a duty under the law. The employer, for its part, can also be considered as a controller when sharing its employees' personal data, even if the duty to transfer such data to the tax authorities is only *implicitly* assigned to it in the law. In this case, the 'control' stems from an *implicit* competence. Finally, when no explicit or implicit competence exists for processing personal data, the control will stem from the factual influence exercised by a person on the processing of personal data. When a company decides to send marketing emails to its existing customers, for example, it factually determines the purpose and essential elements of the processing. Even if the company relies on an intermediary to send these emails, the decision to process the data or that specific purpose originated from the company. In this case, the 'control' stems from the factual influence exercised by the company on the processing activity. Even when the law implicitly or explicitly assigns a particular role to an entity which requires the processing of personal data, one must ensure that the control is also *factually* exercised by that entity. As stated by the Working Party 29 indeed, the concept of controller is intended to "*allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis.*"⁷³² At the end of the day, determining whether a person is a controller or processor will thus always require a factual assessment of the situation. No purely legal or formal criterion can override the result of such an assessment. A legal provision or the terms of a contract can thus not be decisive in this respect. This is particularly true as far as private agreements are concerned; parties are indeed not allowed to allocate responsibility where they think fit by adopting a contractual provision qualifying one party as a controller or a processor if this qualification does not correspond to reality.⁷³³ All in all, this functional approach to the notion of 'controller' and 'processor' prevents duty bearers to select the regime of obligations

⁷³¹ Ibid. pp. 10-11.

⁷³² Ibid., p. 9.

⁷³³ Ibid., p. 11.

that will be applicable to them under the GDPR, or to escape their factual responsibility.⁷³⁴

With respect to the functionality of EU data protection law, it is particularly important to highlight that virtually *any* person can qualify as a controller or a processor, including natural persons when their processing activities are directed outwards from their private sphere. For example, an individual publishing a video on social media showing a public gathering against COVID 19-related governmental restrictions can be considered as a 'controller' if some of the demonstrators in that video are identifiable. At the same time, the social media platform will also be considered as a controller in this case, since it determines how these personal data can be further shared among its users, how long it will be stored, etc. The fact that the GDPR does not discriminate between legal and natural person, public and private entity, or 'big' and 'small' actors, increases overall the functionality of EU data protection law for data subjects which are willing to exercise their rights. In the example mentioned above, one of the identifiable demonstrators appearing in that video could thus address an erasure request both to the individual who published the video or the social media platform itself, thereby increasing the chance of the video being taken down, as the case may be. The factual approach to the notion of 'controller' and 'processor' therefore protects data subjects against formal agreements which may artificially change the qualification of the parties involved in the processing of personal data.

(ii) A functional role behind the distinction between controllers and processors

The applicable regime of obligations under the GDPR will differ depending on whether a person is a controller or a processor. Hence, the notion of 'controller' and 'processor' are functional notions intended to allocate responsibilities among duty bearers, especially where these duty bearers are processing the same personal data.⁷³⁵ This does not mean, however, that the applicable regime of obligations is completely different for each category of duty bearers. As a matter of facts, both controllers and processors are subject to the same general set of obligations under the GDPR. Each of them must, for example, comply with the key principles of data processing (Article 5 GDPR), designate an EU representative when they are themselves located outside of the EU (Article 27 GDPR), keep a record of processing activities up-to-date (Article 30 GDPR), cooperate with the competent DPAs where necessary (Article 31 GDPR), ensure the security of the processing, and in particular the confidentiality and integrity of personal data (Article 32 GDPR), appoint a DPO when the nature and extent of their processing activities require it (Article 37 GDPR),

⁷³⁴ WP29, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, 00264/10/EN, WP169, p. 8.

⁷³⁵ WP29, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, 00264/10/EN, WP169, pp. 4-5.

or implement appropriate safeguards before operating any transfer of personal data outside of the EU (Article 46 GDPR).

Besides those shared obligations, controllers must however also comply with an additional set of obligations, such as determining which valid legal basis can be relied on for each processing activity (Articles 6 -10 GDPR), informing the data subjects about the processing of their personal data (Articles 13 -14 GDPR), answer requests from data subjects exercising their right to information, rectification, erasure, or any other data protection right (Article 15 -22 GDPR), notifying data breaches to the competent DPA or data subjects, where necessary (Article 33-34 GDPR), and conducting a data processing impact assessment (hereafter, 'DPIA') before starting any novel data processing activity likely to result in a high risk to the rights and freedoms of natural persons (Article 35 GDPR).⁷³⁶ These additional obligations are only incumbent on the controllers either because they are intrinsically linked to their decision-making power (e.g. determining the legal basis of each processing activity), or because repeating them twice would be superfluous or could lead to inconsistencies (e.g. providing information to data subjects about the processing) .⁷³⁷ A controller may however requests one of its processors or a third-party to fulfil one of these additional obligations on its behalf, even the responsibility will primarily remain with the controller.⁷³⁸ Controllers have thus a greater compliance burden and a higher level of responsibility under the GDPR compared to processors. To avoid a dilution of responsibility, the EU legislator has adopted several provisions in the GDPR, which can be considered as safeguarding the coherence and functionality of the entire framework, including when data subjects seek to hold a controller accountable for any infringement of their rights or freedoms. These safeguards will further be discussed below.

(iii) Safeguards against the dilution of controllers and processors' responsibility

In the field of corporate social responsibility, a crucial issue when it comes to human rights violations is the one of accountability and the dilution of responsibility through supply chains.⁷³⁹ To illustrate this issue, one may refer to the 2013 Rana Plaza

⁷³⁶ Kosta, E. (2020). Article 35 Data protection impact assessment. In C. Kuner, L. Bygrave, C. D., & L. Drechsler (Eds.). *The EU General Data Protection Regulation: A commentary*. Oxford University Press, pp. 665-679.

⁷³⁷ For example, if the controller informs the data subjects about the processing of their personal data, it would be superfluous for each processor down the line to provide the same information. Similarly, since the controller is the one who determines the means and purposes of the processing, it is logical that the obligation to conduct a DPIA lies with the controller and does not have to be repeated in parallel by the processor (as the latter may not even have access to the necessary information to evaluate the risk; for example).

⁷³⁸ Article 5(2) and Article 24 GDPR.

⁷³⁹ See, inter alia, Giuliani, E. (2016). Human Rights and Corporate Social Responsibility in Developing Countries' Industrial Clusters. *Journal of Business Ethics*, 133.1, pp. 39-54; Sinkovics, N., Hoque, S. F., and Sinkovics, R. (2016). Rana Plaza Collapse Aftermath: Are CSR Compliance and Auditing Pressures Effective?. *Accounting, Auditing & Accountability*, 29(4): 617-49.

collapse which led to the tragic death of 1,134 persons.⁷⁴⁰ The building contained, among others, clothing factories which were providing garments to important US and EU fashion retailers. Local police and an industry association had warned that the building was unsafe, but no effective measures had been put in place to prevent the collapse. After the tragedy, much of the blame was put on the Bangladeshi government, which did not properly enforce the national building code.⁷⁴¹ The spotlight was however also put on the multinational companies whose orders from local factory owners had led to an unsustainable growth of the garment industry in Bangladesh.⁷⁴² EU and US fashion retailers in particular were accused of exploiting poorly paid workers with little regard for their safety.⁷⁴³ Yet, these entities were not held accountable as they could reject the responsibility on their sub-contractors and the Bangladeshi governments. A parallel can be made between this well-known issue of dilution of responsibility in the field of corporate social responsibility, and similar accountability issues in other fields, including data protection.

Theoretically, indeed, a controller could escape part of its responsibility under EU data protection law by delegating various processing activities to a processor, which could in turn enter into different agreements with sub-processors located in the EU or abroad, making it potentially difficult for data subjects or DPA to hold the primary controller accountable in the event of a breach of data protection law by a sub-processor. The EU legislator has however put in place three safeguards aiming at preventing the dilution of responsibility of controllers or processors through the 'chain of processing'. These safeguards are: (a) the unitary approach to the concept of controller and processor; (b) the regulation of joint-controllership and (c) the regulation of controller-to-processor, and of processor-to-sub-processor relations.

(a) The unity of the concept of 'controller' and 'processor' as a first safeguard against the dilution of responsibilities

The concept of 'controller' and 'processor' must be envisaged from a unitary perspective. The employees of a company, for example, will not be considered as separate controllers from the company itself when processing personal data in the course of the activities of the company. This is because any person working directly under the authority of a controller or of a processor will not be considered as a third party but will be considered as an extension of that controller or processor.⁷⁴⁴ Hence, employees are not personally liable under the GDPR when processing personal data as part of their employment activities. Rather, the company itself remains responsible to comply with all their duties under the GDPR. For example, if a data

⁷⁴⁰ Labowitz, S. & Baumann-Pauly, D. (2014, April 16). Business as Usual Is Not an Option: Supply Chains & Sourcing after Rana Plaza. NYU Stern Center for Business and Human Rights (Report). New York City. p. 64.

⁷⁴¹ "Disaster at Rana Plaza; Corporate Social Responsibility", *The Economist*, 4 May 2013 407.8834 (2013), p. 12.

⁷⁴² *Ibid.*

⁷⁴³ *Ibid.*

⁷⁴⁴ WP29, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, 00264/10/EN, WP169, p. 31.

breach occurs because of the negligence of an employee, and sensitive data are disclosed or lost, the company itself may be held accountable for such a breach. If an employee, however, exceeds their competences by processing personal data in a way that is not required or allowed under their employment contract, such an individual may also become personally liable under the GDPR, and qualify as a separate controller with respect to this excessive processing, in accordance with the applicable provisions of tort law of the Member State concerned, as the case may be.

From the perspective of the functionality of EU data protection law, this prevents controllers or processors to reject the blame on an employee or a third party involved in the processing, and therefore increases the chances of data subjects to successfully file a claim against (one of) the responsible controller(s) or processor(s). In particular, data subjects do not have to identify the actual person responsible for a data protection breach within a company or within a group of companies; rather, they can simply target the controller or processor which they assume is responsible for the violation, or which is the most likely to take responsibility for it. The same applies for DPAs when starting an investigation or adopting corrective or punitive measures against an infringer. In the opinion of the author, this renders EU data protection law more practical and thus more functional as far as enforcement is concerned (on that topic, see Section 3.3 below).

(b) The regulation of ‘joint-controllership’ as a second safeguard against the dilution of responsibilities

The unitary approach to the concept of ‘controller’ is furthermore reinforced by the conceptualization and regulation of ‘joint-controllerships’. Under the GDPR indeed, when different controllers jointly process personal data (even when not belonging to the same group of companies), each of them can be held accountable for any infringement of data protection law which may arise during these joint processing activities, without the need for the data subject to identify beforehand which controller in particular is to blame. This notion of ‘joint controllership’ therefore also prevents the dilution of the responsibility of controllers vis-à-vis data subjects.

Article 26 of the GDPR, entitled ‘Joint controllers’, provides in particular:

“1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the

controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. *The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.*

3. *Irrespective of the terms of the arrangement referred to in paragraph 1, **the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.***” (emphasis added)

According to the definition given in Article 26(1) GDPR, ‘joint controllers’ are therefore two distinct persons who share some decision-making power as to the purposes and the means of the processing. By way of example, in *Wirtschaftsakademie*,⁷⁴⁵ the CJEU has ruled that the administrator of a ‘fan page’ on Facebook is jointly responsible with Facebook for the processing of the personal data of the users visiting that fan page. It was indeed found by the CJEU that administrators of fan pages on Facebook could obtain anonymous statistical data on visitors to the fan pages via a function called ‘Facebook Insights’, which Facebook makes available to them free of charge under non-negotiable conditions of use.⁷⁴⁶ In this context, the administrator determines the purpose for which these statistical data will be used (for example, to put in place marketing strategies for different target groups). For such processing to take place, however, Facebook must first gather and share with the administrator the necessary data, thereby becoming a joint controller. In this particular case, the CJEU itself pointed out that the notion of ‘joint controllership’ aims to ensure a more complete protection of the rights of the data subjects by allowing them to indiscriminately address or file a complaint against one joint controller or the other, without the need to predetermine the role and respective share of responsibility of each of them.⁷⁴⁷

In the opinion of the author, this provision – also when read in combination with Article 82 GDPR, discussed below – undeniably participates to the functionality of EU data protection law for two main reasons: first, it prevents the dilution of the responsibility of the joint controllers by making them jointly liable, regardless of the respective share of responsibility of each joint-controller with respect to a violation; second, it allows data subjects to strategically decide which controller to contact, or against which controller a complaint should be filed. A data subject could, for example, decide to bring a complaint against a joint controller in their country of residence, or the one which appears to have more resources, and this even if, *prima*

⁷⁴⁵ CJEU, Case C-210/16 *Wirtschaftsakademie*, Judgment of 5 June 2018.

⁷⁴⁶ *Ibid.*, para. 15.

⁷⁴⁷ *Ibid.*, para. 42.

facie, the violation has been committed by the other joint controller, which may be located abroad, or appears to have less resources. In the opinion of the author, this renders the exercise of the rights of the data subjects more convenient, and thus the entire framework more functional for them.

(c) The regulation of controller-to-processor and processor-to-sub-processor relations as a third safeguard against the dilution of responsibilities

If the GDPR had not strictly regulated the relations between controllers and their processors, or processors and sub-processors, it would have probably been too easy for them to dilute their responsibility by creating complex chains of processing activities. Different provisions in the GDPR, however, regulate such relations to ensure that controllers remain accountable in the event of a breach, as further discussed below.

First and foremost, Article 26 of the Regulation states that the controller holds the main responsibility for ensuring compliance under data protection law. The controller remains thus “*the main point of reference*” for ensuring that data subjects are guaranteed an effective protection for any violation of data protection law.⁷⁴⁸ As a consequence, data subjects can exercise their rights vis-à-vis a controller, regardless of whether the processing activity at stake is undertaken by a processor or a sub-processor, or if the breach originates from their negligence. The controller, for its part, may not redirect the data subjects towards another co-controller, a processor or a sub-processor – i.e., legally, indeed, each controller is jointly liable with its co-controllers, and liable for its processors or sub-processors, as further explained below.

Article 28(1) GDPR further requires controllers to only select processors “*providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*” Some authors have interpreted this provision as requiring controllers to conduct some sort of due diligence before engaging any processor.⁷⁴⁹ Such due diligence could include, for example, assessing the expert knowledge, reliability and resources of the processor,⁷⁵⁰ including by checking the privacy and security policies of the processor, ensuring that no major data breaches have occurred in the past, or asking whether the processor has obtained a recognised international certification for data security, such as the ISO 27000 series.⁷⁵¹ According to the EDPB, the obligation to only use

⁷⁴⁸ Cimina, V. (2020). The data protection concepts of ‘controller’, ‘processor’ and ‘joint controllership’ under Regulation (EU) 2018/1725. ERA-Forum, 21(4), 639-654.

⁷⁴⁹ Ibid., p. 644.

⁷⁵⁰ Recital 81 of the GDPR.

⁷⁵¹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020, p. 29.

processors “*providing sufficient guarantees*” is a continuous obligation which does not end with the selection of the processor; rather, the controller should, at appropriate intervals, verify the processor’s guarantees through audits and inspections where appropriate.⁷⁵²

Moreover, Article 28(2) GDPR provides that processors themselves may not engage other processors (i.e., so called, ‘sub-processors’) without the prior written authorisation of the controller. Such authorisation may either be specific or general.⁷⁵³ In the case of general written authorisation, the processor must however inform the controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving the controller the opportunity to object to such changes. In practice, this means that processors must establish a list, table or any other written document, referring to any actual or intended delegation of the processing operations to one or more sub-processors and require the prior approval of the controller before making any modification to this list. This written document thus prevents the responsibility of the controller from being diluted over time, as the latter must be systematically informed about – and approve – the addition of any sub-processor to the chain of processing.

Last but not least, Article 28(3) GDPR requires any relation between a controller and a processor to be governed by a formal agreement comprising no less than eight mandatory clauses (usually referred to as a ‘processing agreement’). Such processing agreements – because they are mandatory – render the chain of processing more transparent, both for data subjects and DPAs. One of the mandatory clauses of such agreements is that the processor can only process the personal data “*on documented instructions from the controller*”.⁷⁵⁴ Hence, the tasks of the processors must be clearly defined beforehand. This, in turn, brings a level of transparency which may later facilitate the allocation of responsibilities between the controller and its processor in the event of a breach by the latter of the processing agreement, as the case may be. Another mandatory clause which must necessarily be included in any processing agreement is that the processor must delete or return all the personal data collected or otherwise processed on behalf of the controller after the end of the provision of the agreed services and delete any existing copies.⁷⁵⁵ This provision is important to put a *factual* end to any link in the chain of processing, rather than a purely formal one. Under Article 28(4) GDPR, the same obligation applies towards processors and their sub-processors, in the sense that they must also conclude a formal agreement containing these mandatory clauses (usually referred to as ‘sub-processing agreement’). Article 28(4) GDPR specifies in this respect that sub-processing agreements must contain the same data protection obligations as set out in the original processing agreement between the controller

⁷⁵² EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020, p. 30.

⁷⁵³ Article 28(2) GDPR.

⁷⁵⁴ Article 28(3)(a) GDPR.

⁷⁵⁵ Article 28(3)(g) GDPR.

and the processor, thereby ensuring that the same level of obligations applies at the beginning and at the end of any processing chain.

In the opinion of the author, the requirements of transparency and the requirement to maintain the same level of obligations throughout the processing chain, especially when read in conjunction with Article 82 GDPR discussed below, participate to the functionality of EU data protection law by preventing the dilution of the responsibility of the original controller throughout the processing chain. By knowing who, when and to what extent different parties are involved in the processing, data subjects and DPAs can have a better picture of the situation, accurately trace back the source of the processing to the original controller, and or strategically held the latter accountable in the event of a violation.

(d) A functional liability regime facilitating the exercise of the right to compensation

In the event a violation of EU data protection law by a controller or a processor has given rise to a damage, Article 24, 26 and 26 GDPR should be read in conjunction with Article 84 GDPR, on the right to compensation and liability of controllers and processors.

Article 82(1) GDPR starts with the logical premise that any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered. As one can notice, not only data subjects are concerned by this provision, but any person in general (including legal persons, as the case may be).

Article 82(4) GDPR then confirms the unitary approach to the concept of controller and processor, joint-controllership and chain of processing, by establishing a joint liability regime among parties involved in the same processing activities. In particular, Article 82(4) GDPR provides that when more than one controller or processor, or both a controller and a processor, are involved in the same processing having given rise to a damage, each controller or processor shall – in the first phase – be held liable for the *entire* damage in order to ensure effective compensation of the data subject concerned. The data subjects, therefore, do not have to file a claim for compensation against all (joint) controllers or processors involved, but may limit the scope of their claim to one of them. In a situation, for example, where a private hospital (i.e., the controller) which forms part of a larger consortium of medical institutions managed by the same commission (i.e., the joint controller) has delegated the back-up and storage of its patient files to an IT service provider (i.e., the processor), and that an employee of this processor has disclosed, out of negligence, sensitive personal data to the public, thereby causing a data breach giving rise to substantial damages, the data subjects concerned – or any other

person having suffered a damage following this breach – can strategically decide to sue either the IT service provider, the hospital, or the commission, depending, *inter alia*, on the location or resources of each party. It is only in a second phase that the controller or processor which has been condemned to pay the full compensation is entitled to claim back from the other processor(s) or controller(s) the part of the compensation corresponding to their wrongdoing or negligence.⁷⁵⁶

Article 84 GDPR can thus be considered as a functional clause which supports the unitary approach to the concept of controllers and processors, as well as the regulation of joint-controllerships and of controller-to-processor and processor-to-sub-processor relations, to the benefit of the effective protection of the rights and freedoms of data subjects. The enforcement of EU data protection law would in general be more difficult to achieve without a third important category of actors under the GDPR; the DPAs. The below section will briefly introduce their role. Since the actual supervisory and enforcement powers of the DPA can however be considered as a separate pillar of the functionality of EU data protection law, which is not intrinsically linked to the personal scope of the GDPR itself, such powers will be discussed separately in Section 3.3 of this study, below.

3.1.3.3. Supervisory authorities as enforcers – “data are being processed, therefore we are competent”

Article 51 GDPR introduces a third important category of actors under the GDPR, officially referred to as ‘supervisory authorities’, and more commonly called ‘data protection authorities’ or, in abbreviated form, ‘DPAs’. In particular, Article 51 of the GDPR states:

*“Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to **protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union** (‘supervisory authority’)” (emphasis added).*

The role of DPAs is furthermore highlighted in Article 16(2) TFEU and in Article 8(3) of the Charter, where it is stated that compliance with EU data protection rules must be subject to the control of independent authorities. The supervisory control exercised by DPAs as well as their independence can thus be considered as fundamental elements of the right to personal data protection as enshrined in the Charter.⁷⁵⁷

⁷⁵⁶ Article 84(5) GDPR.

⁷⁵⁷ Szydło, M. (2013). Principles Underlying Independence of National Data Protection Authorities: Commission v. Austria. *Common Market Law Review*, 50(6): 1809-826.

In accordance with Article 51(1) GDPR, DPAs have a dual role, which reflects the dual objective of the GDPR itself: (1) to protect the fundamental rights and freedoms of data subjects, on the one hand, and (2) to facilitate the free flow of personal data, on the other hand. It is therefore the duty of DPAs to interpret and apply EU data protection law in a manner which may reconcile these sometimes-diverging objectives. Prior to the adoption of the GDPR, most Member States had already established one or several DPAs within their territory, either under the regime of the 1995 Data Protection Directive, or even under a pre-existing data protection law. In France, for example, the *Commission Nationale Informatique et Libertés* or 'CNIL' had already been established in 1978.⁷⁵⁸ Similarly, in Germany, the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, or 'BfDI') was also established in 1978 through the adoption of the *Bundesdatenschutzgesetz*.⁷⁵⁹ Along these years, the tasks, competences and powers of these DPAs have been broadened to reflect the evolution of data processing practices, including through the adoption of EU data protection law. Today, the role of national DPAs has been almost fully harmonised by the GDPR.⁷⁶⁰

As stated in Article 51 GDPR and as confirmed in Recital 117 of the GDPR, Member States can establish more than one supervisory authority within their territory, to reflect their constitutional, organisational or administrative structure. From a constitutional point of view, for example, Germany has established one federal DPA, the *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* or 'BfDI', as well as several state DPAs, i.e., one for each *Land*. From an administrative and organisational point of view, a distinction can sometimes further be drawn between the DPA in charge of supervising the processing of personal data in the public or private sector. In the German state of Bavaria, for example, two state DPAs coexist: the *Bayerisches Landesamt für Datenschutzaufsicht* or 'BayLDA',⁷⁶¹ in charge of enforcing the GDPR in the private sector, and the *Bayerischer Landesbeauftragter für den Datenschutz* or 'BayLfD', in charge of enforcing the GDPR in the public sector.⁷⁶² Unlike Germany, other federal states have opted for a more unitary approach by establishing one DPA for the entire country, such as Belgium with its centralised *Autorité de la Protection des Données / Gegevensbeschermingsautoriteit* (APD/GBA).

Due to the cross-border nature of most data processing activities, national DPAs are under the duty to cooperate with and mutually assist each other.⁷⁶³ Furthermore, to ensure the consistent and uniform interpretation and application of data protection law throughout the EU, the EDPB can adopt opinions or binding decisions, aimed to

⁷⁵⁸ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁷⁵⁹ BDSG 1977. Bundesgesetzblatt, Teil 1, Nr. 7 of 1 February 1977.

⁷⁶⁰ See Chapter VI of the GDPR, Articles 51 to 76.

⁷⁶¹ Official website: <https://www.lda.bayern.de/de/index.html>

⁷⁶² Official website: <https://www.datenschutz-bayern.de/>.

⁷⁶³ See Articles 60 to 63 GDPR.

prevent or resolve diverging views among DPAs.⁷⁶⁴ It must also be noted that the EU itself has established and is thus subject to the supervision of its own DPA, i.e., the EDPS.⁷⁶⁵

Almost needless to say, DPAs fulfil an essential role when it comes to ensuring the effective enforcement of the GDPR for the defence of data subjects' rights and freedoms. They are the first watchdog towards which data subjects can turn in the event a controller or processor is breaching data protection law, before or instead of resorting to national courts. Their intervention can be triggered by lodging a simple complaint with them, free of charge.⁷⁶⁶ Every week, DPAs across the EU render together dozens of decisions in various cases involving the processing of personal data by controllers and processors, sometimes accompanied by corrective measures or administrative sanctions. Since the GDPR became applicable until January 2022, DPAs have imposed together fines for a total amount close to 300 million.⁷⁶⁷

As already mentioned above, the enforcement powers of the DPA can be considered as a separate pillar of the functionality of the GDPR. Each of these powers, and the way in which they may facilitate the protection of data subject's fundamental rights and freedoms, will therefore not be discussed in this section but in Chapter 3.3, below. At this stage, it is relevant to highlight however that the GDPR does not restrict the intervention of DPAs with respect to any specific type of processing activities, as long as it falls within the material and territorial scope of the GDPR. The fact that DPAs are allowed to intervene as soon as personal data are being processed, without their competences being subject to any *de minimis* rule, can thus be considered as an important internal factor of the functionality of the GDPR with respect to its FRO. This is because any processing activity that may potentially harm of the fundamental rights and freedoms of data subjects will necessarily fall under the supervisory powers of DPAs, which may investigate the matter, issue a warning or even a ban on the litigious processing activity, and decide to impose an administrative fine on the infringer, as the case may be.

⁷⁶⁴ Article 64 and 65 GDPR.

⁷⁶⁵ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

⁷⁶⁶ Article 57(3) GDPR.

⁷⁶⁷ In January 2021, this number was around €272 million. (See €272.5m in fines imposed by European regulators under GDPR, Survey by international law firm DLA Piper, published on 19 January 2021 and available at <https://www.dlapiper.com/en/uk/news/2021/01/fines-imposed-by-european-regulators-under-gdpr-survey/>). Since then, the Greek DPA has inflicted an additional fine of €25 millions against Clearview AI (see HDPA, Decision n° 35/2022 of 13 July 2022) and the French DPA a €1 million fine against Total Energies (See CNIL, Délibération SAN-2022-011 of 23 June 2022).

3.1.4. The dialogue between EU secondary and primary law and its effect on the overall scope of EU data protection law

Next to the GDPR, three other important acts regulate the processing of personal data in the EU: (i) the e-Privacy directive (ii) the Regulation on Personal Data Processing by EU Institutions and (iii) the Law Enforcement Directive (LED). Each of these acts have a limited material, personal and territorial scope that complement each other. Beyond this complementary scope, data subjects are logically deprived from any of the functional tools available under these acts, and may thus not invoke EU data protection law as a way to ensure the respect of their fundamental rights or freedoms. It is however unclear whether Article 8 of the Charter would suffer from the same limitations as EU secondary legislation in the field of data protection. One could imagine, for example, that Article 8 of the Charter could be invoked by a data subject who has been subject to online bullying or social media bashing, even if the insults or harassing comments were exchanged on a closed account, such as a private Facebook group with a limited number of members. In that specific case indeed, the GDPR would admittedly not apply against the harassers because the processing activities would fall within the so-called ‘*household exemption*’.⁷⁶⁸ Yet, the question remains whether Article 8 of the Charter is also subject to this exemption, or not. The same question applies for other exemptions or limits with respect to the personal, material or territorial scope of EU secondary law in the field of data protection.⁷⁶⁹

In order to answer those questions, it is first necessary however to take into account the scope of the Charter *itself*. Indeed, Article 51 of the Charter – unequivocally entitled ‘Scope’ – determines when the Charter applies and to whom.⁷⁷⁰ More specifically, the first paragraph of this Article provides that “*the provisions of the Charter are addressed to the [EU] institutions (...) and to the Member States only when they are implementing Union law*”⁷⁷¹ (emphasis added). Two duty bearers are therefore clearly identified: the EU institutions on the one side (as well as EU bodies, offices and agencies), and the Member States on the other side (including their central, regional or local bodies and public organisations).⁷⁷² As far as Member States are concerned however, the application of the Charter is limited to situations where they are “*implementing EU law*”.⁷⁷³ This concept of implementation of EU law is quite elusive and has not facilitated the understanding of the scope of Charter vis-à-vis the

⁷⁶⁸ The GDPR indeed excludes from its material scope the processing of personal data by *natural persons* in the course of a ‘*purely personal or household activity*’. This exemption thus only covers activities conducted by an individual in the context of his/her private or family life (see Article 2(2)(c) of the GDPR, Recital 18 of the GDPR).

⁷⁶⁹ This specific aspect of the scope of Article 8 of the Charter will be further discussed in Chapter 3 of this study, as part of the recommendations for enhancing the multi-functionality of personal data protection.

⁷⁷⁰ Explanations to the Charter – Explanation on Article 51 – Field of application. The Explanations to the Charter therefore seem to consider the words “scope” and “field of application” as synonyms.

⁷⁷¹ Article 51(1) of the Charter of Fundamental Rights.

⁷⁷² Explanations to the Charter – Explanation on Article 51 – Field of application.

⁷⁷³ Article 51(1) of the Charter of Fundamental Rights.

Member States.⁷⁷⁴ What is certain, however, is that this limitation echoes the principle of conferral, and in particular the consideration of Article 6(1) TEU, according to which the provisions of the Charter should not extend in any way the competences of the EU as defined in the Treaties. During the drafting process of the Charter indeed, some Member States raised the concern that the CJEU would rely on the Charter as a ‘competence creep’ at the service of European integration.⁷⁷⁵ In search of a compromise, the field of application of the Charter was thus limited to situations where EU law would already apply. In accordance with Article 51(1) of the Charter, if a legal situation does not come within the scope of EU law, the CJEU does not have jurisdiction to rule on it, and invoking a potential breach of the Charter by a Member State cannot, in itself, form the basis for such a jurisdiction.⁷⁷⁶ Article 51 of the Charter can thus be seen as the “*keystone which guarantees that the principle of conferral is complied with*”.⁷⁷⁷

This keystone is however far from being clear. During the last decade, both national and EU case-law has indeed demonstrated that assessing whether or not a domestic measure engages EU law is “*far from a perfect science*.”⁷⁷⁸ It is generally agreed that there is no fixed formula to determine which measure or (failure to) act by a Member State must be considered as “*implementing EU law*”; this will differ depending on the context, provision and subject-matter under review.⁷⁷⁹ As a consequence, the scope of the Charter is variable. The Explanations to the Charter, which were published in the Official Journal in December 2007, shed additional (yet limited) light on the meaning of “*implementing Union law*” by providing that it is binding on the Member States when “*they act in the scope of Union law*”.⁷⁸⁰ The notion of acting “*in the scope of EU law*” sounds *prima facie* less restrictive than the notion of “*implementing EU law*”. As if to justify such a generous interpretation of Article 51(1) of the Charter, the Explanations refer to the relevant case-law of the CJEU, i.e., Wachauf, ERT, Annibaldi and Karlsson. Having regard to this case-law, it appears indeed that the CJEU has distinguished at least three situations where Member States are “*implementing EU law*” or – as stated by the Explanations – where they “*act in the scope of EU law*”. Among these situations, one may point out in particular: (1) situations where national authorities have taken steps to *apply* or *implement* EU law (the so-called ‘agency situation’)⁷⁸¹, (2) situations where a national measure *restricts* EU law (the so-called ‘derogation situation’)⁷⁸² and (3)

⁷⁷⁴ Fontanelli F. (2014). The Implementation of European Union Law by Member States under Article 51(1) of the Charter of Fundamental Rights. *Columbia Journal of European Law*, 20, 193-307.

⁷⁷⁵ Lenaerts, K. (2012), *op. cit.*, 376.

⁷⁷⁶ CJEU, Case C-466/11 *Currà and Others*, Order of 12 July 2012, para. 26.

⁷⁷⁷ Lenaerts, K. (2012). Exploring the Limits of the EU Charter of Fundamental Rights. 8(3), 377.

⁷⁷⁸ Fontanelli F. (2014), *op. cit.*, p. 196.

⁷⁷⁹ Walkila, S. (2016). *Horizontal effect of fundamental rights in EU Law*. Europa Law Publishing, p. 104.

⁷⁸⁰ Explanation on Article 51 of the Charter – Field of application, second paragraph.

⁷⁸¹ Also referred to sometimes as the “Wachauf situation” in reference to the Wachauf case (CJEU, Case 5/88, *Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft*, Judgment of 13 July 1989). See, on this topic,

⁷⁸² Also referred to sometimes as the “ERT situation”, in reference to the ERT case (CJEU, Case C-260/89, *ERT*, Judgment of 18 June 1991).

situations where a sanction is imposed by a Member State to *penalise an infringement to EU law* (the ‘enforcement situation’).⁷⁸³

Regardless of the situation at stake, the applicability of the Charter will always depend on the applicability of EU law itself. Or, conversely, the applicability of EU law will entail the applicability of the Charter and of the fundamental rights that it guarantees.⁷⁸⁴ Quite logically, when determining whether the Charter applies, the CJEU will thus need to take into account the scope *ratione territoriae, temporis, personae* and *materiae* of the norms of EU law which could potentially regulate the situation under scrutiny.⁷⁸⁵ In the opinion of the author, this sort of “*mise en abîme*” implies a constant dialogue between, on the one hand, the Charter and, on the other hand, EU (primary and secondary) law, taking into account all the relevant factual circumstances at hand.

Keeping the wording of Article 51 of the Charter in mind, one could thus be tempted to conclude that the scope of Article 8 of the Charter is ultimately dependent on the scope of application of EU data protection law itself. Yet, that would only be *partially* correct. In the opinion of the author indeed, there could be two specific case-scenarios where Article 8 of the Charter could potentially be applied *instead* of the GDPR (or any other secondary EU data protection law), while respecting the principle of conferral embedded in Article 51(1) of the Charter:

- First, at the national level, national courts would in principle remain free to interpret any situation in light of the fundamental right to personal data protection as guaranteed by their own legal order *and* the Charter, even in situations where the GDPR does not apply because of the household exemption. As mentioned above indeed, national courts remain free to broaden or extend the level of protection of fundamental rights internally, and thus to disregard the self-imposed limitations on the scope of the Charter as expressed in Article 51(1) of the Charter;
- Second, at the EU level, it could be argued that, even in a situation where EU secondary law in the field of data protection law would not apply because of a clear limit or exemption, the CJEU could still refer to the obligations of a Member State to guarantee the respect of Article 8 of the Charter where *another* instrument of EU law is applicable. For example, the CJEU could be invited to determine whether a Member State’s (in)action with respect to the

⁷⁸³ Also referred sometimes as the “Åkerberg Fransson” situation. CJEU, Case C-617/10 *Åkerberg Fransson*, Judgment of 26 February 2013, paras. 25-28.

⁷⁸⁴ *Ibid.*, para. 21.

⁷⁸⁵ Walkila, S. (2016). *op. cit.*, p. 104-105.

processing of personal data in the field of copyright law⁷⁸⁶ or anti-discrimination laws⁷⁸⁷ infringes Article 8 of the Charter.

On this basis, it can be concluded that the inapplicability of the EU secondary law in the field of data protection would not always preclude the application of Article 8 of the Charter, which could then act as a ‘gap filler’.

Keeping these considerations into mind, the author of this study would like to highlight the beneficial impact that the dialogue between the Charter, on the one side, and EU secondary law in the field of data protection, on the side, could have the material scope of EU data protection law as a whole. Indeed, the case-law of the CJEU in the field of data protection law shows that Article 8 of the Charter can be used as an interpretative prism, in the sense that the CJEU often has often interpreted provisions of the 1995 Data protection Directive, of the GDPR, of the LED or of other legislation pertaining to the processing of personal data *in light of* the fundamental right to personal data protection. In most cases (cf. Section 2.3), this light has been beneficial for the fulfillment of the FRO of EU data protection law, in the sense that the CJEU has often reinforced the scope of EU data protection law. In the case *Jehovan todistajat*, for example, the CJEU restrictively interpreted the household exemption, in light of the Charter. Similarly, in *Schrems II*, the CJEU restrictively interpreted the ‘scope of EU law’ limitation in light of the Charter.⁷⁸⁸ Therefore, the dialogue between EU primary and secondary law in the field of data protection, and more specifically between Article 8 of the Charter on the one hand, and the GDPR, on the other hand, does not only make these two sources of law complementary with regard to their respective scope, but also tends to reinforce the overall scope of these instruments.

For this reason, it can be argued that preserving the substance of Article 8 of the Charter is particularly important for allowing this fruitful dialogue to continue. Yet, the substance of Article 8 of the Charter seems at risk of being diluted within the right to privacy, if both are not clearly distinguished in the relevant case-law. This, in turn, could have an extension-reducing effect on the scope of EU data protection law as a whole, as further discussed below.

The risk of a merger of the fundamental right to personal data protection finds its origin in the quest for consistency between the EU Charter on the one side, and the European Convention on Human Rights on the other side. For reasons of consistency

⁷⁸⁶ A field of law which has been partially harmonized by the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *OJ L 130*, 17.5.2019, p. 92–125.

⁷⁸⁷ A field of law which has been harmonized by several directives: Directive 2000/43/EC against discrimination on grounds of race and ethnic origin; Directive 2000/78/EC against discrimination at work on grounds of religion or belief, disability, age or sexual orientation; Directive 2006/54/EC equal treatment for men and women in matters of employment and occupation; and Directive 2004/113/EC equal treatment for men and women in the access to and supply of goods and services.

⁷⁸⁸

between those two instruments, the Charter itself indeed provides that the fundamental rights it contains must be regarded as having *at least* the same “*meaning and scope*”⁷⁸⁹ as their equivalent under the ECHR. The ECHR therefore establishes a *minimum* level of protection for fundamental rights protection in the EU. The Charter must always guarantee that minimum level of protection and can eventually exceed it. Therefore, Article 7 of the Charter on the right to privacy must have *at least* the same scope and meaning as its equivalent under the ECHR. In practice, this implies that each time the scope of Article 8 of the ECHR is extended at the level of the Council of Europe, the scope of Article 7 of the Charter grows accordingly. By contrast, the right to personal data protection as enshrined in the Charter has no clear equivalent under the ECHR,⁷⁹⁰ and is thus not subject to this mirroring effect *per se*.

The issue however is that, over the years, the ECtHR has been confronted to several cases involving the processing of personal data (hereafter, “ECtHR Data Processing Cases”), in which applicants claimed that their right to privacy had been violated. The factual backgrounds of these cases are diverse; it includes, *inter alia*, mass surveillance by the State,⁷⁹¹ the use of medical data in courts’ proceedings,⁷⁹² the compilation and use of individual files by the police,⁷⁹³ or the collection and storage of traffic data (including IP address) with a view of detecting and prosecuting criminal behaviours.⁷⁹⁴ When ruling on these ECtHR Data Processing Cases, the ECtHR first determines whether the processing activity at stake amounts to an interference with the right to privacy of the persons concerned. If the answer is in the affirmative, the ECtHR then decides whether such an interference is justified by assessing whether it is (i) provided by law and (ii) necessary in a democratic society. When assessing whether these two conditions are fulfilled, it is interesting to note that the ECtHR often refers (sometimes implicitly, sometimes explicitly⁷⁹⁵) to data protection rules, rights and principles as enshrined in Convention 108, the 1995 Data Protection Directive, and other relevant data protection law.⁷⁹⁶ In other words, the existence of an unlawful interference with the right to privacy has been progressively interpreted by the ECtHR in light of data protection-related rights and principles.

As an illustration, one may mention the following cases in particular:

⁷⁸⁹ Article 52(3) of the EU Charter.

⁷⁹⁰ A fact stressed by the CJEU itself (see CJEU, *Tele2 Sverige*, Judgment of 21 December 2016, para. 129).

⁷⁹¹ See, *inter alia*, ECtHR, *Klass and Others v. Germany*, Judgment of 6 September 1978; *Weber and Saravia v. Germany*, Decision on the admissibility of 29 June 2006; *Liberty and others v. United Kingdom*, Judgment of 1 July 2008; *Kennedy v. UK*, Judgment of 18 May 2010; *M. M. v. UK*, Judgment of 29 April 2013; *Roman Zakharov v. Russia*, Judgment of 4 December 2015; *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016.

⁷⁹² ECtHR, *K. H. and others v Slovakia*, Judgment of 6 November 2009; ECtHR, *Z. v Finland*, Judgment of 25 February 1997.

⁷⁹³ See, *inter alia*, ECtHR, *Amann v. Switzerland*, Judgment of 16 February 2000; ECtHR, *Rotaru v. Romania*, Judgment of 4 May 2000; ECtHR, *S. and Marper v. UK*, Judgment of 4 December 2008; ECtHR, *Catt v. UK*, Judgment of 24 April 2019.

⁷⁹⁴ ECtHR, *Benedik v. Slovenia*, Judgment of 24 July 2018.

⁷⁹⁵ ECtHR, *S. and Marper v. UK*, Judgment of 4 December 2008; ECtHR, *Catt v. UK*, Judgment of 24 April 2019.

⁷⁹⁶ Lynskey, O. (2014), p. 586.

- In the *Amann*⁷⁹⁷ and *Rotaru*⁷⁹⁸ cases, the ECtHR has ruled that both the storing by a public authority of information relating to an individual's private life, the use of that information, and the refusal to allow an opportunity for it to be refuted, amounted to interference with the right to respect for private life secured in Article 8 of the ECHR. When analysing whether such an interference could be considered “*in accordance with the law*”, the ECtHR emphasized that the mere existence of a legal basis was not sufficient, but that the law should be accessible to the person concerned and foreseeable as to its effects. Regarding the foreseeability of the law, the ECtHR stressed that the domestic law should lay down with sufficient precision the circumstances in which the State would be allowed to store and make use of information relating to the private life of individuals, the kind of information that may be collected, the categories of persons concerned, or the retention period of the personal data.⁷⁹⁹ From the perspective of data protection law, these criteria reflect the principles of fairness, lawfulness, transparency and storage limitation, as provided in Convention 108 and the 1995 Data Protection Directive;
- In the *Liberty*⁸⁰⁰ and *M. M.* cases,⁸⁰¹ the ECtHR ruled on the compatibility of surveillance measures by the United Kingdom with Article 8 of the ECHR. In each of these cases, the ECtHR recalled that the use and storage of intercepted communications constituted an interference with the right to privacy of the individuals concerned.⁸⁰² When assessing whether such an interference was “*in accordance with the law*”,⁸⁰³ the ECtHR stated that the mere existence of a legal basis was not sufficient; the legal basis also needs to be qualitative enough, in the sense that it must be accessible and its consequences foreseeable to the persons concerned.⁸⁰⁴ A key requirement for a sufficient legal basis is thus the foreseeability of the interference, including the safeguards to be applied at the various stage of the processing of the personal data, in order to prevent abuse or disproportionate measures.⁸⁰⁵ In particular, the ECtHR considered that the domestic law should have clear, detailed rules governing the scope and application of the surveillance measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction. From the perspective of data protection law, this echoes the principles of

⁷⁹⁷ ECtHR, *Amann v. Switzerland*, Judgment of 16 February 2000.

⁷⁹⁸ ECtHR, *Rotaru v. Romania*, Judgment of 4 May 2000.

⁷⁹⁹ See in particular the judgment in *Rotaru v. Romania*, para. 57.

⁸⁰⁰ ECtHR, *Liberty and others v. United Kingdom*, Judgment of 1 July 2008.

⁸⁰¹ ECtHR, *M. M. v. UK*, Judgment of 29 April 2013

⁸⁰² ECtHR, *Liberty and others v. UK*, Judgment of 1 October 2008, para. 57.

⁸⁰³ *Ibid.*, para. 58.

⁸⁰⁴ *Ibid.*, para. 59.

⁸⁰⁵ Kokott, J., & Sobotta, C. (2013), p. 224.

transparency, purpose limitation, storage limitation, and security of the data, as provided in Convention 108 and the 1995 Data Protection Directive;

- In the *S. and Marper* and (more recent) *Catt* cases, the ECtHR recalled that the storage of personal information amounts to an interference with the right to respect for private life of the individuals concerned. When assessing whether such interference is “*necessary in a democratic society*”, the ECtHR stated that several elements must be taken into account, and in particular the existence of effective procedural safeguards. Regarding the procedural safeguards, the ECtHR reiterated in the *S. and Marper* case that the domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (referring, *inter alia*, to Article 5 of Convention 108), efficiently protected from misuse and abuse (referring to Article 7 of Convention 108). Regarding the nature of the data, the ECtHR considered significant that the personal data at stake were sensitive data (i.e., data revealing ethnic origin or political opinion), and recalled that those type of data should benefit from a higher level of protection (referring to Article 6 of Convention 108);
- In *Z. v. Finland*,⁸⁰⁶ *I. v. Finland*⁸⁰⁷ and *K.H. and others v. Slovakia*⁸⁰⁸ the ECtHR stressed the importance to guarantee the security and confidentiality of medical data. In particular, it stated that the protection of medical data is of fundamental importance to a person’s enjoyment of their right to respect for private and family life as guaranteed by Article 8 of the ECtHR, and that respecting the confidentiality of health data is a vital principle.⁸⁰⁹ In the *K. H. and Others* judgment, the ECtHR specifically stated that the right to privacy as guaranteed by Article 8 of the ECHR must be practical and effective and may therefore impose positive obligations on the State, such as guaranteeing to the data subject the right to receive a copy of their data files.⁸¹⁰ This echoes the principle of data security and confidentiality, as well as the right of the data subject to have access to their personal data, as guaranteed by Convention 108 and the 1995 Data Protection Directive.
- More recently, in the *Satamedia* case,⁸¹¹ a turning point was reached when the ECtHR expressly stated that “[t]he protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the [ECHR].” The

⁸⁰⁶ ECtHR, *Z v. Finland*, Judgment of 25 February 1997.

⁸⁰⁷ ECtHR, *I. v. Finland*, Judgement of 17 July 2008.

⁸⁰⁸ ECtHR, *K.H. and others v. Slovakia*, Judgment of 6 November 2009.

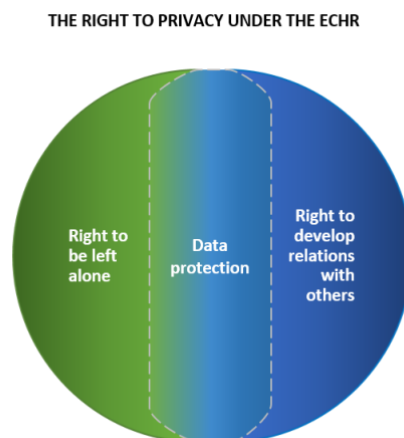
⁸⁰⁹ See judgment in *Z. v. Finland*, para. 95, in *I. v. Finland*, para. 38 and in *K.H. and others*, para. 55.

⁸¹⁰ See judgment in *K. H. and others*, para. 58

⁸¹¹ ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Judgment of 27 June 2017, para. 137.

ECtHR, after recalling that domestic law must afford appropriate safeguards to prevent the unlawful use of personal data, concluded: “Article 8 of the [ECHR] thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged” (emphasis added).⁸¹² In line with the relevant German doctrine, the right to informational self-determination can be considered as a synonym of the right to data protection. In that sense, the statement of the ECtHR in the *Satamedia* case could also be interpreted as meaning that Article 8 of the ECHR is encompassing the right to personal data protection.

The above-mentioned ECtHR Data Processing Cases illustrate how the ECtHR has progressively included data protection-related rights and principles *within* the scope of the right to privacy.⁸¹³ Taking into account that case-law, the right to privacy under the ECHR would thus have three different facets: (i) the right to be left alone, (ii) the right to develop relationships with the outside world, and (iii) the right for individuals to have control over their personal information. As such, this approach appears to be valid and has not been subject to many criticisms among scholars. Rather, it has shed a new light on the concept of privacy and allowed for novel reflexions on the content of that right. Hildebrandt, for example, highlights the interdependence of these three facets by observing that “control over personal information is preconditional for negotiating the membrane that separate us from or link us to the [outside world]”.⁸¹⁴



⁸¹² *Ibid.*, para. 137.

⁸¹³ In 1967 already, Westin had defined privacy as the claim of individuals “to determine for themselves when, how and to what extent information about them is communicated to others.” It seems that the ECtHR has embraced this approach (see Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum. p. 7.).

⁸¹⁴ Hildebrandt, M. (2013). Balance or Trade-off? Online Security Technologies and Fundamental Rights. *Philosophy & Technology*, 26(4), p. 367.

As said above, the fundamental rights guaranteed under the Charter are supposed to correspond in scope and content to the rights guaranteed under the ECHR. As a consequence, by extending the scope and meaning and the right to privacy under the ECHR, the ECtHR has also indirectly extended the scope of Article 7 of the Charter, so as to encompass (almost) all data-protection rights and principles. Ultimately, Article 7 of the Charter could thus completely ‘acquire’ the content of Article 8 of the Charter. Such a takeover is likely to deepen the confusion that already exists regarding the respective scope of each right under the Charter. Most seriously, it could limit the application of Article 8 of the Charter only to situations where an interference exists with the private life of an individual, thereby restraining the material scope of that right, and preventing its autonomous content to be explored. In the opinion of the author, the merger of the right to personal data protection within the right to privacy would be detrimental to data subjects, as it would reduce the overall level of protection that they could obtain under the Charter. Gurthwith and De Gert similarly argue that those two rights should remain sharply distinguished in order to design accurate and effective privacy and data protection policies.⁸¹⁵ The risk pertaining to the entanglement of privacy and data protection therefore resides in the potential full merger of those two rights due to the quest for consistency between the Charter and the ECHR.

A potential solution to avoid such a takeover would be to clarify that Article 8 of the ECHR has not *one* but *two* equivalent articles under the Charter: Article 7 *and* Article 8.⁸¹⁶ When referring to the case-law of Article 8 of the ECHR, the CJEU could then make a clear distinction between, on the one hand, rights relating to the protection of private and family life (whose scope and meaning would correspond to Article 7 under the Charter) and, on the other hand, rights relating to informational self-determination in the context of the processing of personal data (whose scope and meaning would correspond to Article 8 of the Charter).⁸¹⁷ If this system is applied, the mirroring effect between the ECHR and the Charter would allow both Article 7 and Article 8 of the Charter to grow autonomously. This could in turn guarantee the long-term co-existence of the right to privacy and data protection under both instruments.

⁸¹⁵ De Hert P. & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. E. Claes, A. Duff & S. Gutwirth (eds). *Privacy and the criminal law*. Antwerp/Oxford, Intersentia, pp. 61–104.

⁸¹⁶ The European Union Agency for Fundamental Rights (the “FRA”) seems to also be of the opinion that the right to privacy under the ECHR corresponds to both Article 7 and Article 8 under the Charter (see FRA Handbook (2018), “Applying the Charter of Fundamental Rights of the European Union in law and policymaking at the national level”, p. 83, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_en.pdf).

⁸¹⁷ The position of the EU legislator on the question does not contravene this possibility. The 2018 Regulation on Personal Data Processing by EU Institutions indeed provides in its Preamble: “[t]he protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the [Charter] provide[s] that everyone has the right to the protection of personal data concerning him or her. **This right is also guaranteed under Article 8 of the [ECHR]**” (emphasis added). See First recital of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, *OJ L 295, 21.11.2018, p. 39–98*.

Ensuring that both Article 7 and Article 8 of the Charter can grow autonomously might have at least two beneficial consequences at the EU level. First, from a legalistic and linguistic perspective, it might help ending the confusion between the scope and content of each right, and reduce the legal and terminological jumble that sometimes ensues from it.⁸¹⁸ Second, from the perspective of the scope of data protection law, allowing those rights to grow independently might maximize their respective scope, thereby allowing individuals to gain more ‘sub-rights’ in the long-run.⁸¹⁹ In particular, the fruitful dialogue between Article 8 of the Charter and EU secondary law on the processing of personal data could continue. This would of course not prevent the combination of Articles 7 and 8 of the Charter in instances where both the right to privacy and the right to personal data protection would suffer from a common limitation or interference. However, it would also allow courts and tribunals across the EU to envisage these rights independently, instead of having to identify a breach of privacy to be able to rely on Article 8 of Charter as well. Although these two beneficial consequences cannot be guaranteed, the mere possibility of such developments should encourage the CJEU as well as the EU legislator to establish that Article 8 of the ECHR has not one but *two* distinct equivalents under the Charter.

3.1.5. Concluding remarks: the broad material, territorial and personal scope of the GDPR as structural factors of functionality for the defence of data subjects’ rights and freedoms

The above sections have discussed the material, territorial and personal scope of the GDPR from the perspective of their functionality. It has been shown in particular that the broad scope of the GDPR allows data subjects and DPAs to rely on these rules in a wide range of situations, regardless for example of the technology at use, the location of the processing, or whether the controller is a multinational company or a single natural person. Furthermore, the generous interpretation given to the notion of ‘personal data’ and ‘processing’ could also mean that, if the Negroponte shift continues to move forward exponentially, the GDPR could soon turn into the law of *almost* everything, everywhere and everyone. Both the advantages and the risks related to this broadening of the scope of the GDPR have been discussed above. In the opinion of the author, however, the main risk associated with the Negroponte shift – i.e., the fact that the GDPR may no longer be ‘workable’ – is mitigated by the

⁸¹⁸ Today, it is still common to see these two terms being used as if they were interchangeable. As an example, EU scholars and legal experts often refer to “privacy laws” as an umbrella term encompassing both privacy and data protection legislation. On the internet, most websites refer their users to their “privacy policy”, although the information contained in those documents reflect the mandatory information that must be provided to the data subject under Article 12-14 of the GDPR. Similarly, until 25 May 2018, the Belgian data protection authority was called the Privacy Commission (*Commission Vie Privée / Privacycommissie*). Following the adoption of the GDPR, the name was changed to the Data Protection Authority (*Autorité de Protection des Données / Gegevensbeschermingsautoriteit*) by the *Loi du 3 décembre 2017 portant création de l’Autorité de protection des données*, M.B. 10 January 2018, in force on 25 May 2018.

⁸¹⁹ ‘Sub-rights’ or ‘micro-rights’ must be understood as rights deriving from a (main) fundamental right. For example, the right to access one’s personal data or the right to correct one’s personal data may be considered as two sub-rights of the fundamental right to personal data protection.

dual objective of the GDPR and the interests and forces which opposed each other in that context. Moreover, the important role of the various actors involved in the interpretation and application of the GDPR, guided by this dual objective and opposing forces, should enable to avoid the pitfall of interpretative deviations and contribute to the long-term coherence of the framework.

With respect to the research question of this study, it has been concluded that the following elements can be considered as structural factors of the functionality of EU data protection law, in the sense that they facilitate the use of such a framework for the defence of data subjects' fundamental rights and freedoms against potentially harmful data processing practices:

- The material scope of the GDPR is not limited to 'privacy matters'; rather, the GDPR applies when personal data are being processed. Since the notion of 'personal data' and 'processing' have been interpreted unrestrictedly, data subjects may invoke these rules in a wide range of situations where any of their fundamental rights or freedoms have been affected, including DFR;
- The material scope of the GDPR depends on objective and factual elements; i.e., the 'processing' of 'personal data'. There is no need for any subjective (pre-)assessment as to the impact of such processing on the rights, freedoms, or interests of the data subjects. Hence, data subjects can rely on these rules quite conveniently simply by pointing out to the fact that their personal data have been processed;
- The material scope of the GDPR is not limited to a particular type of technology, and no *de minimis* rule applies with respect to amount of data or the extent of the processing operations. Hence, data subjects are protected regardless of the technology at use, and regardless of the extent of the processing itself;
- The material scope of the GDPR does not extend to processing of personal data in the context of purely personal or household activities. Yet, in case of mixed processing, where part of the processing is directed outwards from the private setting of an individual, the GDPR continues applying, for the benefit of the rights and freedoms of the data subjects;
- The territorial scope of the GDPR is not limited to the EU but is construed around the borderless effects that processing activities can have on the rights and freedoms of data subjects, regardless of where this processing is taking place. Hence, the GDPR has a wide territorial reach which also protects the rights and freedoms of data subjects located *outside* of the EU when their data are being processed by an EU-controller, and data subjects located in

the EU when their personal data are processed by a non-EU controller for monitoring purposes, or for the purpose of providing them with goods or services;

- The integrity of the territorial scope of the GDPR is protected by several safeguards to ensure that the level of protection of the rights and freedoms of data subjects do not diminish once their personal data are being transferred abroad. These special safeguards include the obligation for non-EU controllers to establish a representative in the EU, the obligation to abide to specific transfer mechanisms, and international cooperation mechanisms;
- The personal scope of the GDPR is grounded in the notion of ‘personal data’, and does not require the fulfilment by right holders of any additional condition to be recognised as such (no condition of citizenship, nationality, age or *compos mentis*). Hence, individuals simply have to point to the fact that their personal data have been processed to become a right holder under the GDPR;
- The personal scope of the GDPR is also broad as far as duty bearers are concerned, in the sense that any person processing personal data will necessarily be either a controller or a processor, regardless of whether that person is a natural or a legal person, or whether it is acting in a private or public capacity; furthermore, no *de minimis* rule applies in this respect, thereby ensuring that data subjects remain protected even when the processing of their personal data is limited to a single processing operation on a limited amount of data;
- As far as duty bearers are concerned, the personal scope of the GDPR is particularly functional for data subjects seeking to assert their rights, in the sense that it embraces a unitary approach to the notion of ‘controller and ‘processor’, including when multiple controllers, processors and sub-processors are involved in shared processing activities. This unitary approach facilitates the exercise of data protection rights by data subjects, and in particular the possibility to hold the responsible parties accountable.
- The scope of the GDPR is complemented by other instruments of EU secondary law, such as the LED or the Regulation on Personal Data Processing by EU Institutions. The scope of EU secondary law in the field of data protection has been gradually broadened in the case-law of the CJEU when interpreted in light of Article 8 of the Charter. The fruitful dialogue between EU primary and secondary law in the field of data protection law is also a factor that contributes to the fulfilment of the FRO of these rules.

All in all, the GDPR is generally characterized by a broad scope, grounded in the objective notion of ‘personal data’ and ‘processing’, whose borders are flexible enough to include old and new types of data processing practices, including those relying on novel DDTs. Theoretically, the GDPR also applies when a processing activity does not put at risk the right to privacy or data protection *per se*, but may put at risk another fundamental right or freedom. Hence, the scope of the GDPR can be considered *prima facie* as a structural factor of its functionality when it comes to ensuring the protection of the fundamental rights of the data subjects in the context of the processing of their personal data. Whether this theoretical functionality is confirmed in practice will further be explored in the following Chapter of this study. Before putting the scope of the GDPR to the test, however, the author of this study will discuss the second pillar of functionality of the GDPR; its substance, composed of a set of general principles, individual rights and specific obligations.

3.2. SECOND PILLAR OF THE FUNCTIONALITY OF THE GDPR: ITS SET OF PRINCIPLES, RIGHTS AND OBLIGATIONS

The broad scope of the GDPR is doubtlessly a factor which participates to the effectiveness and ultimately to the functionality of EU data protection law for data subjects seeking to ensure the respect of their rights and freedoms. Yet, a wide scope alone is not sufficient to ensure the functionality of a legal framework. Concrete tools must also be available to both data subjects and competent authorities to combat harmful data processing practices. A reading of the GDPR allows to distinguish three types of tools in particular: (1) the Principles of data processing (Article 5 GDPR), (2) the Rights of the data subjects (Articles 12 to 22 GDPR), and (3) the Obligations of controllers and processors (Articles 23 to 46 GDPR).

These three types of tools form together the substance of the GDPR. This substance has already been analysed by many scholars in the form of articles,⁸²⁰ books⁸²¹ or commentaries.⁸²² The purpose of this Section is not to repeat the work of these scholars. Conducting a detailed analysis of the content of the GDPR would indeed go beyond the scope of this study. Rather, this section will focus on the interplay between these three types of tools, and how it participates to the functionality of EU data protection law for achieving its FRO. In particular, in the below Chapter, the author of this study will highlight the synergies deriving from the combinations

⁸²⁰ Hoofnagle, C. J., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019). *op. cit.*; Laurer, M. & Seidl, T. (2021). Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation. *Policy and Internet*, 13(2): 257-77.

⁸²¹ Theodorakis, N. & Dhont, J. (2019). *General Data Protection Regulation: For Practitioners*. Cambridge: Intersentia; Voigt, P. & Von Dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer; Besemer, L. (2020). *Privacy and Data Protection Based on the GDPR: Understanding the General Data Protection Regulation*. Van Haren Publishing.

⁸²² Kuner, C., Bygrave, L. & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press; Bensoussan, A., Henrotte, J.-F., Gallardo, M., Fanti, S. & Falque-Pierrotin, I. (2018). *General Data Protection Regulation: Texts, Commentaries and Practical Guidelines*. Mechelen: Wolters Kluwer Belgium.

which can be made of these different Principles, Rights and Obligations – metaphorically called the ‘PRO triptych’.

The metaphor of the triptych stems from the idea that the substance of the GDPR is composed of three panels which, once read together, create a stronger legal narrative. After briefly presenting each panel within that triptych, the author will assess its robustness, analyse the sequences that derive from them, and its effects on the functionality of EU data protection law. If, on the one hand, it appears that the provisions of the PRO triptych are only useable or useful for defending the right to privacy or data protection, then, it could be argued that EU data protection law is a bi-functional framework. If, on the other hand, it appears that these tools can also serve other rights and freedoms, such as dignity, integrity, freedom of expression or non-discrimination, then, it could be argued that the GDPR is a multi-functional framework, in the sense that its substance contribute to both its primary and secondary functionality.

3.2.1. First Panel of the PRO Triptych: the key-principles of personal data processing

Under Article 5 of the GDPR, data processing must respect seven key-principles. A general overview of these principles is provided in the below table. After briefly presenting each of these principles, particular attention will be paid to the interpretative flexibility that they offer, as well as to the practical implications of the principle of accountability, and how such flexibility and practical implications participate to the functionality of EU data protection law for the fulfilment of its FRO.

3.2.1.1. General overview of the key-principles of data processing

TABLE 3

This table lists and reproduces verbatim the principles of data processing as enshrined in Article 5 of the GDPR.

Principle	Provision
Lawfulness, fairness and transparency	Article 5(1)(a) GDPR: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Article 5(1)(b) GDPR: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the

	initial purposes.
Data minimisation	Article 5(1)(c) GDPR: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Article 5(1)(d) GDPR: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Storage limitation	Article 5(1)(e) GDPR: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
Integrity and confidentiality	Article 5(1)(f) GDPR: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
Accountability	Article 5(2) GDPR: The controller shall be responsible for, and be able to demonstrate compliance with [these data processing principles].

First, the principle of lawfulness, fairness and transparency requires that personal data be processed lawfully, fairly and in a transparent manner in relation to the data subject.⁸²³ This principle thus includes three distinct components. The first of these components, i.e., *lawfulness*, implies that personal data can only be processed by a controller or a processor when a valid legal basis exists for such a processing.⁸²⁴ These valid legal bases are restrictively listed in the GDPR in Articles 6, 9 and 10, respectively. Such legal bases include, for example, the consent of the data subjects,⁸²⁵ the performance of a contract to which the data subject is a party,⁸²⁶ or the existence of a legal obligation to which the controller is subject by virtue of EU or Member States law.⁸²⁷ The second of these components, i.e., *fairness*, implies that personal data must be processed in good faith, in the sense that the relation between the data subject and the controller should be characterized by honesty and

⁸²³ Article 5(1)(a) GDPR.

⁸²⁴ Recital 40 of the GDPR.

⁸²⁵ Article 6(1)(a) GDPR ; Article 9(2)(a) GDPR.

⁸²⁶ Article 6(1)(b) GDPR.

⁸²⁷ Article 6(1)(c) and 6(3) GDPR.

openness.⁸²⁸ In particular, for processing to be fair, personal data cannot be processed in a way that is unexpected, unjustifiably detrimental, discriminatory or misleading for the data subjects.⁸²⁹ This implies, for example, that data subjects should not be 'tricked' into a processing operation through the use of dark patterns.⁸³⁰ The third of these components, i.e., *transparency*, goes hand in hand with the lawfulness and fairness requirement. It implies that data subjects must be made aware of and properly informed about the processing of their personal data, including the applicable legal basis. The GDPR further requires that such information be easily accessible and easy to understand for data subjects. For that purpose, controllers should use clear, concise and plain language.⁸³¹ The transparency requirement – similar to the lawfulness requirement – is further detailed in several articles of the GDPR, and in particular in Articles 12 to 14 of the GDPR on the right to information of data subjects, as discussed in the next Section of this study.

Second, the principle of purpose limitation requires that personal data be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.⁸³² This principle is further reinforced by the obligation of controllers to clearly inform data subjects, at the latest at the time when personal data are obtained, about the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing.⁸³³ Controllers must therefore pre-determine and inform data subjects about a limited number of specific purposes for which their personal data will be used, and cannot spontaneously decide to change or expand the nature or scope of these purposes afterwards, unless they are compatible with the original purposes. As an illustration, if a data subject has ordered a good online, and that her home address and email address are processed by the company for the purpose of billing and delivery, the latter cannot later decide to also share these personal data with a data broker for the (unrelated) purpose of increasing its own revenues. By contrast, sending an email to the customer to inform her about a delay in the delivery of the good, or to attract her attention on similar products sold by the same company, can be considered as compatible with the original purpose, since customer relationship management "*is a usual activity resulting from the customer relationship.*"⁸³⁴ Article 5(1)(b) GDPR specifies that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes must be considered compatible with the initial purposes. Hence, in the example previously mentioned, the company could for example further process the home address of its

⁸²⁸ Hoofnagle, C., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019). *op. cit.*, p. 77.

⁸²⁹ EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2020 (Version 2.0), pp. 17-18.

⁸³⁰ EDPB Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them.

⁸³¹ Recital 39 GDPR.

⁸³² Article 5(1)(b) GDPR.

⁸³³ Article 13(1)(c) GDPR.

⁸³⁴ Kotschy, W. (2020). *Article 6. Lawfulness of processing*. Kuner, C., Bygrave, L. & Docksey, C. (eds). *op. cit.*, p. 341.

customers for statistical purpose, such as determining the region to which most goods are being delivered. Other compatible purposes may exist, but in order to ascertain such a compatibility, controllers should take several elements into account, such as the existence of a link between the initial purpose and the additional purpose, the context in which the personal data have been collected, the nature of the personal data (and in particular whether sensitive personal data are processed), the possible consequences of the intended further processing for data subjects, and the existence of appropriate safeguards, which may include encryption or pseudonymisation.⁸³⁵ When read together with the fairness principle, the purpose limitation principle therefore rests on the premises that due regard should be paid to the reasonable expectations of the data subjects when their personal data are being used for purposes that were not initially envisaged, or about which the data subjects had not been specifically informed at the time their personal data were obtained.⁸³⁶ This principle thus protects data subjects against the repurposing of their personal data, and also puts clear limitations to the use of some DDTs which are sometimes used for unspecified purposes, such as machine-learning, whose aim is often to “discover patterns not anticipated or even perceivable to people”.⁸³⁷

Third, the data minimisation principle entails that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.⁸³⁸ When ordering an item online, for example, the name, home address and credit card details of a data subject can be considered as data which are adequate and relevant for delivery and payment purpose. Asking the same data subject for additional information such as a passport number, however, should be considered as neither adequate nor relevant, given that such information is not necessary for the purpose of delivery, payment or customer relationship management. When read in combination with the purpose limitation principle, the data minimisation principle thus strikes at the heart of the business model of Big Data by prohibiting the collection of large amounts of data which “could be useful in the future”,⁸³⁹ but are not necessary *per se* for pre-determined and explicit purposes.

Fourth, the accuracy principle requires that personal data be accurate and, where necessary, kept up to date. Article 5(1)(d) GDPR further specifies that “every reasonable step” must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.⁸⁴⁰ The accuracy principle thus aims to ensure the correct representation of the person in diverse contexts and is one of the essential

⁸³⁵ Article 6(4)(e) to (a).

⁸³⁶ Kotschy, W. (2020). *op. cit.*, p. 341.

⁸³⁷ Hoofnagle, C., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019). *op. cit.*, p. 78.

⁸³⁸ Article 5(1)(c) GDPR.

⁸³⁹ Hoofnagle, C., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019). *op. cit.*, p. 78.

⁸⁴⁰ Article 5(1)(d) GDPR.

prerequisites of the right to informational self-determination.⁸⁴¹ Yet, this principle also acknowledges the fact that only data subjects may be in possession of accurate information, which is why it does not require “*full accuracy*” on the part of the controller.⁸⁴² The accuracy principle thus embodies a best-effort requirement rather than a performance requirement. If a customer, for example, inaccurately enters his home address when ordering a good online, the controller may not be held accountable for a breach of the accuracy principle. Once a controller has been made aware of an inaccuracy in the personal data, this best-effort requirement, although not becoming absolute, increases the burden of responsibility of the controller to rectify the data, especially once when read in combination with the right to rectification enshrined in Article 16 GDPR. If a customer having ordered a good online, for example, contacts the company to inform the latter about a mistake in the delivery address and provides the correct one instead, the company would be under the obligation to promptly correct the inaccurate data,⁸⁴³ and could thus be held accountable in the event it did not take “*every reasonable step*” to do so.

Fifth, the storage limitation principle requires personal data to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.⁸⁴⁴ Recital 39 of the GDPR further provides that time limits should be established by the controller for erasure or for a periodic review. The storage limitation principle therefore tightly limits data storage and more specifically requires controllers “*to set, ex ante, time limits for planned erasure.*”⁸⁴⁵ A controller may, instead of erasing the personal data, decide to anonymize them instead. This would indeed also ensure that the data subjects are no longer identifiable, given of course that the anonymization is and remains robust enough over time (on this topic, see Section 3.1.1.2(iii)(b), above). Such a principle is further reinforced by the obligation of controllers to inform data subjects, prior to the processing, about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.⁸⁴⁶ For example, a company could inform its customers that their home address will be stored in their CRM database for a period of 6 months after the delivery of the latest purchased goods, before being automatically deleted. Similarly, a company could inform job applicants who are not hired that their CV and other application documents, including the results of any test that they may have had to take, will be deleted within 2 weeks from the day their application was rejected.

Sixth, the ‘integrity and confidentiality’ principle requires personal data to be processed in a manner that ensures appropriate security of the personal data,

⁸⁴¹ Resta, F. (2018). *Commentario, Article 5 GDPR*. Riccio, Scorza & Belisario (eds). GDPR e Normativa Privacy. Wolters Kluwer, p. 59.

⁸⁴² Hoofnagle, C., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019). *op. cit.*, p. 78.

⁸⁴³ Recital 39 GDPR.

⁸⁴⁴ Article 5(1)(e) GDPR.

⁸⁴⁵ Hoofnagle, C., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019). *op. cit.*, p. 78.

⁸⁴⁶ Article 13(2)(a) GDPR.

including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.⁸⁴⁷ In line with this principle, controllers and processors must implement appropriate technical or organisational measures to ensure the security of the personal data against possible data breaches. The integrity and confidentiality principle is further reinforced by Articles 32 to 34 GDPR on the security of personal data and the notification of potential data breaches. Article 32 GDPR, in particular, requires controllers and processors to assess the risk of data breaches, and to implement appropriate measures to protect data subjects against such breaches, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing (including, for example, whether sensitive data are being processed). Typical organisational and technical measures include, for example, encryption of personal data, securing access to building with locks or badges, having periodic servers' back-up, restricting access to files to staff members who need them, implementing a strict password renewal policy, etc. Although a literal reading of the principle of integrity and confidentiality seems to indicate that the EU legislator was mostly preoccupied with the security of the data themselves, it clearly appears from the FRO of the GDPR that the ultimate aim is to protect the *individuals* to whom these data relate. This is also clearly reflected in Article 32 GDPR, given that controllers must, at the time they decide on these security measures, pay particular attention "*the risk of varying likelihood and severity for the rights and freedoms of natural persons*".⁸⁴⁸ Among the risk for the rights and freedoms of individuals which should be considered, the 75th Recital of the GDPR refers in particular to the risk of discrimination, identity theft, fraud, financial loss, damage to the reputation, or any other significant economic or social disadvantage. The obligation of controllers to conduct regular risk assessments when deciding on appropriate security measures,⁸⁴⁹ or when intending to start a new type of processing operations (especially those relying on a new type of DDT),⁸⁵⁰ has thus the ultimate objective to protect data subjects against violations of their rights or freedoms which could lead to physical, material or non-material damages.⁸⁵¹ Hence, the integrity and confidentiality principle should not be considered as setting standards for the security of data themselves, but rather as setting standards to avoid that data subjects "*(...) be deprived of their rights and freedoms, or prevented from exercising control over their personal data.*"⁸⁵²

Finally, the seventh principle of data processing requires controllers to be able to demonstrate compliance with the above key-data processing principles by documenting the measures adopted for this purpose.⁸⁵³ As further discussed below, this accountability principle participates to the functionality of EU data protection

⁸⁴⁷ Article 5(1)(f) GDPR.

⁸⁴⁸ Article 32(1) GDPR.

⁸⁴⁹ Articles 32 GDPR.

⁸⁵⁰ Article 35 GDPR.

⁸⁵¹ Recital 75, 76 and 83 GDPR.

⁸⁵² Recital 75 GDPR.

⁸⁵³ Article 5(2) GDPR.

law by requiring more transparency from controllers and by removing factual or procedural hindrances that may have prevented data subjects or DPAs to rely on the framework. In particular, this principle ensures that the burden of proof in the event of negligence or a violation of EU data protection law does not primarily lie on data subjects or DPAs, but rather on the controller itself. This, in turn, greatly increases the convenience with which right holders may rely on the GDPR, since they are not required to provide *prima facie* evidence of a violation but may – on the basis of an inconvenient experience or a mere suspicion, compel the controller to demonstrate that the processing is compliant with the GDPR. The easily activable leverages available to the data subject in this respect is further backed up by the fact that failure, on the part of the controller, to demonstrate compliance with the GDPR may already amount to a violation of the GDPR and increase the amount of the fine that may be imposed on them.⁸⁵⁴

3.2.1.2. The factors of functionality of the key-principles of data processing: human-centric approach, interpretative flexibility and reversed burden of proof

In the opinion of the author, the principles of data processing participate to the fulfilment of the FRO of EU data protection law because of three important factors in particular: (i) their human-centric aim, (ii) their interpretative flexibility, and (iii) the reverse burden of proof set by the accountability principle.

Although neutral in appearance,⁸⁵⁵ it is undeniable that the seven key-principles of data processing primarily serve the FRO of EU data protection law. Indeed, their aim is to ensure that personal data are processed in a manner that is lawful, fair, transparent, legitimate and secured. It can therefore be argued that the key-principles of data processing have primarily at heart the protection of the interests, rights and freedoms of the data subjects. By contrast, none of these principles is primarily concerned with the facilitation of data flows among EU Member States. There is, for example, no principle about ‘freedom of data movement’ enshrined in Article 5 GDPR. At best, it could be argued that by establishing a harmonised set of standards with respect to data processing, Article 5 GDPR helps eliminating potential regulatory divergences or obstacles to data flows in the EU, thereby also *indirectly* participating to the fulfilment of the IMO of the GDPR. Another noticeable point with respect to the human-centric nature of these principles is their scope. It appears indeed that their aim is not limited to the respect of the right to privacy or data protection of individuals, but also extend to other rights and freedoms. The principle of data minimisation, for example, may prevent controllers from collecting and

⁸⁵⁴ Many DPAs have rendered binding decisions against controllers in which a violation of Article 5(2) GDPR has been found, precisely because the controller was unable to demonstrate that it was acting in a compliant manner. A selection of these decisions can be found on the GDPRhub via the following link: [https://gdprhub.eu/index.php?title=Category:Article_5\(2\)_GDPR](https://gdprhub.eu/index.php?title=Category:Article_5(2)_GDPR).

⁸⁵⁵ Rather than referring to the data subjects or to controllers and processors, each principle refers to the ‘personal data’ themselves.

processing unnecessary data, including data on gender, religion or sexual orientation, which may both benefit the right to privacy of individuals, as well as their right not to be discriminated on the basis of protected characteristics. Because of their human-centric and broad protective scope, these principles are thus multi-functional in nature. How these principles are interpreted and applied in practice, and whether their human-centred approach really contribute to the (multi-)functionality of EU data protection law for the defence of fundamental rights will further be explored in the next Chapter of this study.

In the opinion of the author, another important factor of functionality of the key-principles of data processing is their flexibility. Each of the above-mentioned principles is indeed spelled out in general terms, thereby offering some room for interpretation to competent authorities when enforcing data protection law. Such interpretative flexibility is undeniably an advantage for combatting a wide range of potentially harmful data processing practices, whose impact or effects might not have been primarily foreseen. One of the issues with interpretative flexibility, however, is that, when pushed to its own limits, it can lead to legal uncertainty. Some authorities could therefore become reluctant to derive from these principles concrete or specific requirements that would be incumbent on controllers, precisely because they would be too general. As already illustrated above, however, each key-principle is complemented by more concrete rights and obligations detailed in the GDPR. The lawfulness principle, for example, is supported by the obligation for controllers and processors to find a valid legal basis for the processing of personal data among the different legal bases exhaustively listed in Articles 6, 9 and 10 GDPR. Similarly, the principle of transparency is complemented by the obligation of controllers to inform data subjects about specific aspects of the processing, as detailed in Articles 12 to 14 of the GDPR. In the opinion of the author, the specificity of these rights and obligations counterbalances the interpretative flexibility offered by Article 5 GDPR, therefore contributing to the solidity of the PRO triptych as a whole. Yet, it must also be kept in mind that the scope of the key-principles of data processing is in no way limited by the specific rules laid down in the rest of the GDPR. In other words, data subjects and DPAs can challenge the legality of a processing practice by invoking these principles either *together with* a more specific rule, or *in the absence of* any specific rule.

A third important factor which contributes to the functionality of EU data protection law is the principle of accountability itself. *Prima facie*, the key-principles of data processing could indeed suffer from one major procedural limitation: the difficulty for any data subject, or even DPAs, to establish the existence of a violation of one (or multiple) of these principles by controllers. Data processing activities often take place behind closed doors and, as already discussed above, are not always perceivable. Consequently, it may be difficult for the concerned parties to become aware or denounce a violation of one of the key principles of data processing. By way of illustration, even major public data breaches can sometimes remain secret if

the controller decides not to reveal it, and if no evidence of this data breach emerges.⁸⁵⁶ The EU legislator has however partially addressed this issue by enshrining a 7th key-principle in Article 5(2) GDPR, i.e., accountability. The accountability principle provides that controllers are responsible for and must be able to demonstrate compliance with all the key-principles of data processing as listed in Article 5(1) GDPR.⁸⁵⁷ In other words, competent authorities and data subjects do not have to gather evidence of a violation but may, on the basis of a simple suspicion, require the controller to prove that its data processing practices are compliant with the GDPR. Accountability is thus, as further discussed below, an important internal factor of the functionality of EU data protection law for data subjects seeking to assert their rights, given that the burden of proof of compliance with EU data protection law is primarily put on its duty bearers. This accountability principle is further reinforced by an array of more specific transparency obligations contained in the GDPR, such as the obligations for controllers to maintain a detailed record of processing activities (Article 30 GDPR), the obligation to document and report data breaches (Articles 33 and 34 GDPR), the obligation to draft a DPIA report where a type of processing is likely to result in a high risk for the rights and freedoms of data subjects (Article 35(1) and (7) GDPR), the obligations to sign processing agreements with joint-controllers, processors and sub-processors (Article 26 and 28 GDPR), or the obligation to document any assessment made before relying on a derogation for data transfers (Article 49(6) GDPR). To comply with these various obligations, controllers and processors must draft, maintain and update different policies, records, reports, notices, or agreements, which indirectly compel them put in place a transparent data governance strategy. The resonance between the principles of data processing and the other two panels of the PRO triptych, as well as the way it can contribute to the functionality of EU data protection law, will further be illustrated and discussed in the subsequent sections of this Chapter.

3.2.2. Second Panel of the PRO Triptych: the obligations incumbent on controllers and processors

Beyond the key-principles of personal data processing which apply horizontally, the GDPR contains an array of vertical obligations aiming at regulating specific behaviours of controllers and processors. These obligations constitute the second panel of the PRO triptych. They both reflect and bring additional fresh to the ‘bone structure’ set by the key-principles of data processing. The below section will show that the combination of a key-principle of data processing with one or more specific

⁸⁵⁶ For example, on 18 November 2020, the CNIL imposed a fine of €2.250.000 on Carrefour France for several violations of the GDPR, including for failing to report a data breach which had occurred in November 2018. See CNIL, decision SAN-2020-008 of 18 November 2020, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756?tab_selection=cnil&searchField=ALL&query=2016%2F679&searchType=ALL&typePagination=DEFAULT&sortBy=DATE_DECISION_DESC&pageSize=10&page=1&tab_selection=cnil#cnil.

⁸⁵⁷ Article 5(2) GDPR.

obligations can create a legal sequence which, in the opinion of the author, further empowers data subjects seeking to enforce their rights and freedoms.

Although analysing in detail all the obligations incumbent on controllers and processors would go beyond the scope of this study, providing a general overview of them remains relevant, especially in view of the case-studies discussed in the following Chapter. The main obligations incumbent on controllers will thus be briefly listed here below in the form of a table (Section 3.2.2.1). This table will further highlight the link between each of these obligations and the key principles of data processing presented above. In line with the overreaching research question of this study, particular emphasis will then be placed on specific obligations which are particularly concerned with the respect of data subjects' rights and freedoms and can contribute to the functionality of EU data protection law with respect to this FRO (Section 3.2.2.2).

3.2.2.1. General overview of the obligations of controllers under the GDPR and of their relation to the key principles of data protection

TABLE 4

This table provides a quick overview of the main obligations of controllers under Article 6 to 49 of the GDPR and indicates how they relate to one or multiple of the above-mentioned key-principles of data processing (Table 3).

Obligation	Principle(s)	Description
Valid legal basis for the processing (Art. 6-10 GDPR)	Lawfulness	Controllers may only process personal data by relying on one of the exhaustive legal bases laid in Article 6, 9 or 10 GDPR. These legal bases include the consent of the data subjects, the necessity to perform a contract to which the data subject is a party, or the existence of a legal obligation to process the data under EU or Member State law. When controllers consider that their legitimate interests consist in the applicable legal basis for the processing, they must balance them against the interests, rights and freedoms of data subjects. If the latter prevail, the processing operation cannot take place.
Informing data subjects about the processing (Art. 12-14 GDPR)	Transparency	Controllers must inform data subjects about all the relevant aspects of the processing, including the identity of the controller, the purpose and legal basis of the processing, the recipients or categories of recipients of the personal data, the retention period of the personal data, the transfers of any personal data outside of the EU, the existence of automated individual decision-making, or the rights of the data subjects.
Data protection by design and by	All principles	Data protection by design means that controllers must implement appropriate measures, such as pseudonymisation, which are <i>designed</i>

default (Art. 25 GDPR)		<p>to implement data-protection principles, so as to meet the requirements of the GDPR and protect the rights of data subjects.</p> <p>Data protection by default means that controllers must implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, and that, by default, data are not made accessible without the individual's intervention to an indefinite number of natural persons.</p>
Establishing a representative in the EU (Art. 27 GDPR)	Accountability	<p>Controllers located outside of the EU whose processing activities fall within the territorial scope of the GDPR must establish a representative in the EU, unless (1) the controller is a public authority or (2) the processing of personal data is occasional, does not include, on a large scale, processing of sensitive data, and is unlikely to result in a risk to the rights and freedoms of natural persons.</p>
Entering into agreements with joint controllers and processors (Art. 26-28 GDPR)	Accountability	<p>Controllers must enter into specific agreements with other controllers when they jointly determine the means and purposes of the processing in order to clearly allocate their joint obligations among themselves ; similarly, when controllers (partly) delegate the processing of personal data to processors, they must enter into detailed processing agreements with these processors in order to prevent the dilution of data protection rules along the processing chain.</p>
Records of processing activities (Art.30 GDPR)	Transparency; Accountability	<p>Controllers and processors must each keep a detailed record of their processing activities, usually in the form of a table clearly identifying, for each processing activity, the purpose(s) of the processing, the categories of data subjects concerned and personal data being processed, the categories of recipients of personal data (if any) and the adopted security measures ; such a document must be provided to DPAs on request to allow them to have a full picture of the undertaken processing activities.</p>
Cooperation with DPA (Art. 31 GDPR)	Accountability	<p>Controllers and processors must cooperate, on request, with the DPAs in the performance of their tasks.</p>
Security of processing (Art. 32 GDPR)	Integrity & confidentiality	<p>Controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of personal data processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk for the rights and freedoms of natural persons. Such security measure may include pseudonymization, back-ups, regular security testing, etc.</p>
Notification of personal data breach	Transparency; Accountability	<p>In the event of a data breach, controllers must document it and alert not later than 72 hours after having become aware of it the competent DPA if it is likely to put at risk the rights and freedoms of data subjects. Controllers must also alert the concerned data subjects when the data</p>

(Art. 33-34 GDPR)		breach is likely to result in a <i>high</i> risk for their rights and freedoms (e.g. identify theft ; discrimination; disclosure of sensitive information, etc.).
DPIA (Art. 35-36 GDPR)	All principles	Where a type of processing in particular using new technologies is likely to result in a high risk to the rights and freedoms of natural persons, the controller must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, and adopt measures to mitigate any risk, including specific safeguards or security measures. If the DPIA shows that the envisaged processing operations is likely to result in a high risk, the controller must consult the competent DPA prior to starting the envisaged processing. The DPA may render a negative opinion and thus prohibit the envisaged processing if it considers that the existing risks have not been sufficiently mitigated.
Designating a DPO (Art. 37-39 GDPR)	All principles	Public authorities and controllers and processors that, as part of their core activities, either process personal data on a large scale to <i>monitor</i> data subjects, or process <i>sensitive</i> data on a large scale, must appoint a DPO having sufficient expertise, and enable the latter to perform multiple tasks, including monitoring compliance of the processing activities of the controllers or processors with the GDPR.
Ensuring the lawfulness of personal data transfers (Art. 42-49 GDPR)	All principles	Controllers cannot transfer personal data outside of the EU/EEA, unless (a) an adequacy decision has been adopted by the Commission; (b) specific safeguards (e.g. entering into standard contractual clauses) are implemented, or (c) a specific derogation applies. These articles aim at ensuring that the rights and freedoms of data subjects remain protected by preventing the dilution of controllers' liability through data transfers.

3.2.2.2. Focus on specific obligations explicitly concerned with the protection of the fundamental rights and freedoms of data subjects

Among the obligations that are incumbent on controllers and processors, some specifically put emphasis on the need to guarantee the protection of the rights and freedoms of natural persons in the context of the processing of their personal data. As a matter of facts, the terms “*rights and freedoms*” appear seventy-seven times in the GDPR, each time echoing the FRO of the GDPR. By contrast, the terms “*free movement of personal data*”, which echoes the IMO of the GDPR, only appears fifteen times in the entire text. This Section will focus on those obligations which put at their centre the need to ensure the protection of the rights and freedoms of data subjects, or which may enhance the protection of these rights and freedoms by compelling controllers to ensure the transparency and lawfulness of the processing. The author will further highlight their significance in the PRO triptych, and how they can contribute to the functionality of EU data protection law with respect to its FRO.

(i) The obligation for controllers to have a valid legal basis for processing personal data: focus on the functional and less functional aspects of consent, contractual necessity and legitimate interests

One of the main safeguards that protects data subjects against the unrestricted processing of personal data in a manner that could harm their interests, rights and freedoms, is that controllers can only process such data on the basis of one of the legal grounds exhaustively listed in Article 6, 9 or 10 of the GDPR. The choice of the limited grounds corresponds to the general rules for lawful limitations on fundamental rights set out in Article 52(1) Charter.⁸⁵⁸ As such, it can therefore be reasonably argued that Article 6 and 9 have been designed to serve the FRO of EU data protection law.

While Article 6 GDPR lists different legal bases for the processing of *non-sensitive* personal data, Article 9 GDPR lists different legal bases for the processing of special categories of personal data. Special categories of data include (i) data revealing racial or ethnic origin, (ii) political opinions, (iii) religious or philosophical beliefs, (iv) trade union membership, (v) genetic or biometric data, (vi) data concerning health, as well as (vii) data concerning a natural person's sex life or sexual orientation (also commonly referred to as ‘**sensitive personal data**’).⁸⁵⁹ Article 10 GDPR, for its part, is

⁸⁵⁸ Kotschy, W. (2020). Article 6 Lawfulness of processing. in Christopher Kuner and others (eds). *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford Academic. Web version.

⁸⁵⁹ Article 9(1) GDPR.

solely concerned with data relating to criminal convictions and offences (hereafter, '**criminal data**').

As far as criminal data is concerned, Article 10 GDPR states that such data can only be processed under the control of an official authority, or when the processing is authorised by Union or Member State law, on the condition that this law provides for appropriate safeguards for the rights and freedoms of the data subjects concerned. The processing of criminal data is thus tightly framed, and must either involve a legal authorisation or be undertaken by a competent authority (e.g. police forces, criminal courts, etc.). In Luxembourg, for example, the Law of 29 March 2013 on the organization of criminal records⁸⁶⁰ set out specific rules about the issuance and sharing of extracts of individual criminal records, including for the purpose of employment. According to the applicable rules, a criminal record issued to a public or private employer for the purpose of concluding an employment contract cannot be kept beyond a period of one month from the conclusion of the employment contract. If the person concerned is not engaged, the extract from the record must be destroyed without delay by the employer.⁸⁶¹ Read together with the GDPR, these provisions therefore allow the processing of a limited amount of criminal data for the purpose of recruitment and employment, together with a strict limitation regarding the storage of such data.

As far as non-sensitive personal and sensitive personal data are concerned, Article 6 and Article 9 GDPR respectively provides for an exhaustive list of potential legal bases for processing each type of data. The legal bases listed under Article 9 GDPR are logically more restrictive than the legal bases that can be invoked under Article 6 GDPR, thereby granting data subjects a higher level of protection when it comes to the processing of sensitive data, with a view of better preventing potential abuses, including discriminatory practices. As an illustration, under Article 6(1)(b) GDPR, controllers are allowed to process *non*-sensitive personal data when it is necessary for the conclusion or performance of a contract to which the data subject is party. By contrast, 'contractual necessity' cannot be found among the available legal bases for the processing of sensitive personal data under Article 9 GDPR. In the same vein, under Article 6(1)(f) GDPR, controllers can process personal data when necessary for the purposes of their legitimate interests or the legitimate interests of a third party, as long as the rights and freedoms of the data subjects do not prevail over these interests. By contrast, this 'legitimate interests' basis does not exist under Article 9 GDPR for the processing of sensitive personal data.

Keeping in mind the research question of this study, this section will focus on the functional and dysfunctional aspects of three legal basis in particular: (a) the

⁸⁶⁰ In French: *Loi du 29 mars 2013 relative à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les états membres de l'union européenne, Mémorial A85.*

⁸⁶¹ Article 8-5 of the Law of 29 March 2013 on the organization of criminal records (consolidated version).

(explicit) consent of the data subject; (b) contractual necessity and (c) the ‘legitimate interests’ of the controller or of a third party.

(a) The safeguards around consent as factors of functionality

Under the GDPR, it is allowed to process both non-sensitive data and sensitive data on the basis of the (explicit) consent of the data subjects. It goes without saying that ‘consent’ as a legal basis could have rendered EU data protection law extremely dysfunctional if envisaged as an absolute waiver, whereby the data subjects could completely surrender their personal data to the will of the controller. Another danger that may come straight into mind is that the consent of the data subject could be robbed, coerced, embezzled or otherwise obtained through deceiving practices, including so-called ‘dark patterns’.⁸⁶²

A dark pattern refers to a user interface that has been designed to trick users into agreeing to something that they would have otherwise not been agreeing to if they had been presented with a clearer choice, such as accepting cookies, or signing up for recurring bills.⁸⁶³ Deceptive cookie banners are often used as examples of dark patterns. Placing cookies on the devices of internet users’ with a view of registering their preferences or tracking their behaviour online is a common practice on the internet. As a matter of facts, it is almost impossible nowadays to browse the internet without being constantly asked to agree to the use of cookies. This request takes the form of so-called ‘cookie banners’, which automatically appear on the screen of internet users, and block (part of) the content or decrease visibility. Although these banners are originally envisaged as a compliance tool, they can also be designed in a way that nudge the users into agreeing to the placement of cookies, instead of providing them with the clear possibility to either accept or reject them. Common strategies among controllers consist into using contrasting fonts, colours or multiple layers of information, where the ‘accept’ button is always clearly visible and is easy to click on, while the ‘reject’ button is hidden or only available on another pop-up page.

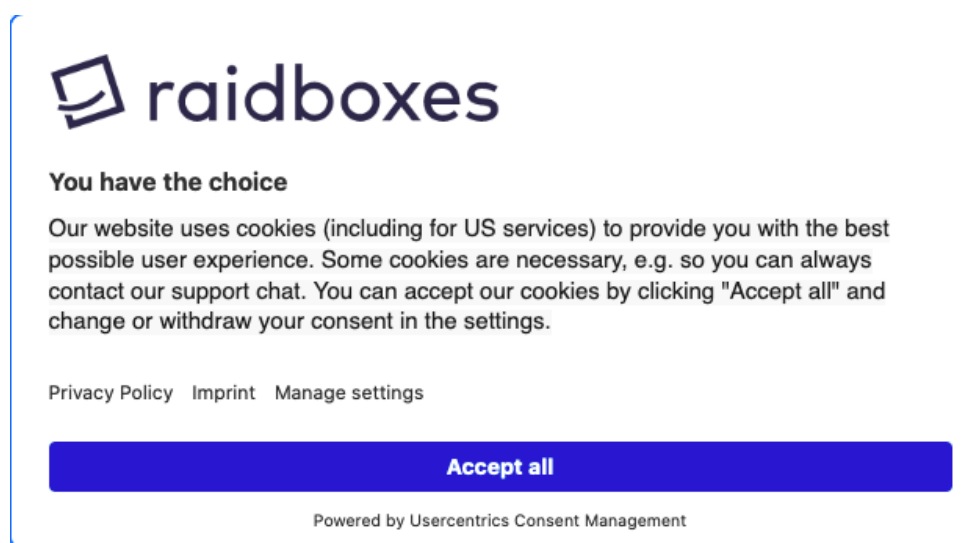
The below image gives an example of a deceptive cookie banner, extracted from the website www.raidboxes.io.⁸⁶⁴ Despite the words “You have the choice” being written in bold, it quickly appears that the user is nudged into clicking on the vivid-blue “Accept all” button, where he or she not only agrees to the placement of cookies on his or her device for so-called ‘functional purpose’ (i.e., selecting a language, etc.),

⁸⁶² EDPB Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them.

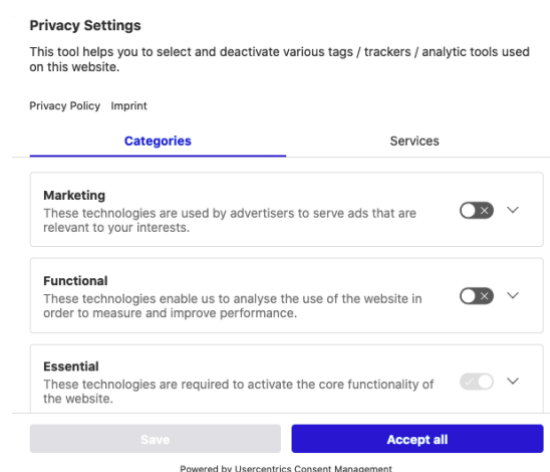
⁸⁶³ See, *inter alia*, Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies* 2016(4): 237-254.

⁸⁶⁴ The author of this study visited the website in October 2022.

but also for marketing purpose (i.e., behaviour tracking and analysis to show targeted ads).



It is only if the user takes the time to read the entire text and clicks on the (noticeably smaller and more discreet) 'Manage settings' option that he or she is redirected towards a second pop-up window (below), allowing him or her to select, among different options, the types of cookies to which he or she agrees. The user is then given the choice to either "Accept all cookies" – an option that is, once again, clearly put in evidence, or to "Save" the preferences that he or she may have selected – an option that is almost not visible because of the light grey and white colours of the button in question. As a result, a fair portion of data subjects will be nudged into accepting the placement of all cookies on their device, instead of rejecting them, which would have been their normal choice if they had been more clearly and equally presented with both options.



Aware of these risks, the EU legislator has established both preventive and corrective safeguards to ensure that data subjects cannot lawfully be nudged or tricked into agreeing to data processing practices that could interfere with their rights or freedoms. **Preventive safeguards** take the form of strict conditions for 'consent' to

be considered as valid under the GDPR at the time the controller seeks to obtain it.⁸⁶⁵ In particular, consent must be *freely given, specific, informed* and *unambiguous*. The adjective '*unambiguous*' implies that the data subject must pose a clear affirmative act, such as clicking on a banner, accepting an information notice, ticking a box or "*any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing*".⁸⁶⁶ By contrast, silence, pre-ticked boxes or inactivity cannot constitute a valid consent under the GDPR.⁸⁶⁷ On top of that, the fact that the consent must be both *specific* and *informed* implies that the data subjects must both be aware and understand the specific purposes of the processing activities to which they are agreeing. The request for consent can thus not be hidden in a long information notice or be requested 'in general' for a wide range of operations that are not clearly defined (i.e., so-called 'blanket consent'). Finally, the fact that the consent must be 'freely given' means that the data subject cannot feel compelled or be coerced into given it, for example by fear of negative consequences or retaliation. Hence, in any relation characterised by an imbalance of powers, such as the employer-employee relationship, the controller can normally not rely on 'consent' as a valid legal basis for processing personal data, unless it can demonstrate that the data subjects were free to accept or refuse the processing activity, without suffering any adverse consequences at all.⁸⁶⁸ **Corrective safeguards** take the form of the right of data subjects to withdraw consent "*at any time*",⁸⁶⁹ as well as the right to request the erasure of the personal data in question once consent has been withdrawn.⁸⁷⁰

As said above, consent can be invoked by a controller or processor as a legal basis for the processing of both non-sensitive personal and sensitive personal data, with the only difference that, in the latter case, the consent of the data subject must also be *explicit*. As explained by the Article 29 Working Party, the term explicit means that, beyond posing a clear affirmative act (such as ticking a box), the data subject must give "*an express statement of consent*". For example, the data subject can be invited to expressly confirm consent in a written statement or by signing a declaration.⁸⁷¹ This additional condition reflects the more serious data protection risk that may emerge where sensitive personal data are being processed, and where a higher level of individual control over personal data is deemed appropriate.

In the opinion of the author, the preventive and corrective safeguards established by the GDPR for 'consent' to be regarded as a valid legal basis were necessary to prevent the framework as a whole to become dysfunctional. If 'consent' could have

⁸⁶⁵ Recital 32 and Article 7 GDPR.

⁸⁶⁶ Recital 32 GDPR.

⁸⁶⁷ Article 29 Working Party. Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018. WP259 rev.0 17/EN.

⁸⁶⁸ *Ibid.*, p. 5-7.

⁸⁶⁹ Article 7(3) GDPR.

⁸⁷⁰ Article 17(1)(b) GDPR.

⁸⁷¹ Article 29 Working Party. Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018. WP259 rev.0 17/EN, p. 18.

been obtained without clear validity requirements, and without the possibility for data subjects to change their mind, there is no doubt indeed that abusive or deceiving processing practices could have proliferated, to the detriment of the FRO of EU data protection law. In particular, data subjects would have been left almost powerless against deceiving or abusive processing practices, where their consent could have been given by mistake, negligence, lack of information or deception.

As far as functionality is concerned, it must also be pointed out that the right for data subjects to withdraw their consent at any time considerably empowers them. This right can also be considered particularly convenient and easy to use, since no formal or substantial requirement is attached to it. Some functional aspects of the right to withdraw consent has already been explored in Section 3.1.1.2(ii) of this study, above, where it was concluded that data subjects who have previously consented to the processing of their sensitive personal data are granted in return a ‘veto power’ in this respect. Indeed, data subjects may – without any prior warning and without having to provide for any legitimate reason – inform the controller that they do no longer consent to the processing of their personal data. In that case, the controller has normally no other choice than to stop the processing practice in question.⁸⁷² This, of course, enables data subjects in certain situations to quickly and effortlessly force the controller to interrupt a processing activity that the data subjects could suspect or consider to be harmful to their rights, freedoms or economic or personal interests. In parallel, this also allows data subjects to strategically point out or create a ‘situation of breach’, where it is apparent that a controller has not obtained a valid consent from them in the first place, or did not take into consideration their withdrawal right, in violation of Article 6, 7 or 9 GDPR, as the case may be.

To illustrate the functional nature of these provisions, one may refer to the 500 complaints lodged by *noyb* in May 2021 with various DPAs across the EU regarding non-compliant cookie banners. To streamline its action, *noyb* developed a software that automatically analyses and flags different types of violations, from the plain absence of a ‘consent request’ to deceptive practices intended to nudge the user into consenting to the use of cookies. Each time the software would discover one or multiple violations on a website, *noyb* would automatically contact the controller in charge of administrating that website via email to provide the latter with (i) an informal draft complaint and (ii) a step-by-step guide on how to change software settings to comply with the GDPR. If the controllers would choose not to change their settings within a month, the complaint would automatically be transferred to the relevant DPA. Since this project has been launched, thousands of website administrator have voluntarily changed their cookie banner so as to comply with the GDPR, while a special task force within the EDPB has been set up to deal with

⁸⁷² Unless, of course, another legal basis under Article 6 or 9 applies.

ongoing complaints.⁸⁷³ Overall, this example shows how *noyb* has been able to rely on the functionality of the GDPR to foster a compliance culture with respect to the placement of cookies in the EU, while enforcing the rights of data subjects against persistent infringers.

In the opinion of the author, the preventive and corrective safeguards surrounding the use of ‘consent’ as a legal basis for data processing have been designed in a particularly convenient way for the benefit of data subjects, which explains why they can now be used as functional tools to fulfil the FRO of EU data protection law. Even if violations have not disappeared altogether (there are indeed still situations where consent is not obtained in a fully transparent and informed manner), the author believes that these violations can be effectively combatted, with the intervention of DPAs where necessary.

(b) Contractual necessity and the danger of ‘self-imposed’ or ‘self-created’ necessity

There exist some processing operations that are factually necessary for the performance of a contract between a controller and a data subject. For example, when a data subject orders a good online, the controller will need to process the name and address of the buyer for the purpose of delivery, as well as their billing information for the purpose of payment. Without that information, the distant sale could not take place. In these situations, acceptance, by the data subjects, of the terms of sale can be assimilated to an acceptance that the relevant personal data be processed for the purpose of performing the contract. Since it would have been unnecessarily burdensome, in these cases, to request in parallel the specific and unambiguous consent of the data subject, the EU legislator has given to controllers the possibility to rely on an alternative legal basis, as foreseen in Article 6(1)(2) of the GDPR: the necessity to process personal data *“for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”*.

As far as the (dys)functionality of the GDPR is concerned, a clear danger that may come straight into mind concerns the notion of ‘necessity’. For example, it could be tempting for a company like Meta to argue that it is *‘contractually necessary’* for them to rely on smart algorithms to flag and erase content that violates their terms of use on Facebook, because of the larger number of Facebook users around the world, and the limited human resources available to Meta. In that case, one may wonder indeed if this apparent situation of ‘necessity’ was not self-imposed or self-created by Meta, rather than truly genuine and/or inherent to the nature of the contract between Meta and the users of Facebook.

⁸⁷³ See *noyb* (2022, March 4). *Many more Cookie Banners to go: Second Wave of Complaints underway*. Available at <https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway>.

As a general rule, the notion of ‘necessity’ must be appreciated together with the purpose of the processing (i.e., necessary for *what* ?) and requires a combined, fact-based assessment of the processing, which must be conducted prior to the commencement of the processing.⁸⁷⁴ In other words, ‘necessity’ cannot be contractually construed or unilaterally imposed by the controllers. The necessity assessment must include, in particular, an analysis of alternative ways to perform the contract that would not require the processing of the personal data in question (if any). As put by the EDPB, “*if there are realistic, less intrusive alternatives, the processing is not ‘necessary’.*”⁸⁷⁵ Furthermore, the notion of ‘necessity’ goes beyond the one of ‘usefulness’ or ‘convenience’. As a result, controllers can normally not justify the processing of personal data for the performance of a contract where it appears that the processing practice in question is merely ‘*useful*’ for other business purposes or renders the performance of the contract ‘*more convenient*’ for the controller, without appropriately considering the rights and freedoms of data subjects.

Based on these considerations, it clearly appears that the notion of ‘necessity’ must be appreciated together with the principle of fairness and purpose limitation.⁸⁷⁶ As argued below, combining the obligation of the controller to have a valid legal basis (such as the performance of a contract) with the key principles of data processing (such as fairness and purpose limitation) create a stronger legal narrative to the benefit of data subjects’ rights and freedoms.⁸⁷⁷

In the opinion of the author of this study, it is important for DPAs and national courts to fully exploit the possibility of combining these various provisions and keep in mind the FRO of EU data protection law when interpreting the notion of ‘contractual necessity’, with a view to challenge the use of that legal ground by a controller when the ‘necessity’ of the processing operations is not genuine. In particular, for this provision not to become dysfunctional, it is important to exclude its use when a controller or a processor would have artificially created a situation of necessity by organising its business operations in a certain way, rather than considering alternative, less impactful or intrusive processing operations for the concerned data subjects.

Restricting the situations in which controllers can rely on ‘contractual necessity’ would logically have the effect of pushing them to envisage the use of another legal basis, such as (i) the consent of the data subject (which, as discussed above, grants them a veto power with respect to the processing), or (ii) the fact that the processing

⁸⁷⁴ EDPB (2019, October 16). Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. 2019A, p. 6.

⁸⁷⁵ *Ibid.*, p. 8.

⁸⁷⁶ Article 29 Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), p. 17.

⁸⁷⁷ See Section 3.2.4 below.

is necessary for pursuing their own *'legitimate interests'*. The functional and less functional aspects of this second legal basis will be discussed here below.

(c) The legitimate interests of the controller against the rights and freedoms of data subjects

Finally, the author of this study wishes to discuss the functional and less functional aspects of a last important legal basis available under Article 6 GDPR: the necessity of the processing for the purposes of the legitimate interests of the controller. This legal basis is spelled out in Article 6(1)(f) GDPR as follow:

*“Processing shall be lawful only if and to the extent that (...) processing is necessary for the purposes of **the legitimate interests pursued by the controller** or by a third party, **except** where such interests are **overridden** by the **interests or fundamental rights and freedoms of the data subject** (...).”*

It quickly appears on first reading that this provision could either be a great ally or a Trojan horse for the fulfilment the FRO of EU data protection law. On the one side, the seemingly dysfunctional aspect of that legal basis stems from the fact that the *'legitimate interests'* of the controller is an extremely broad notion, without any clear limitation, that exclusively depends on the decision-making power of the controller itself. This legal basis could thus become an obvious *'catch-all'*, in the sense that it could be systematically (and therefore potentially abusively) invoked by controllers to justify *any* type of processing. This, in turn, may leave data subjects at the mercy of controllers' will. On the other side, however, Article 6(1)(f) GDPR could also be used as a functional tool by data subjects against controllers, given that it explicitly put emphasis on the fact that controllers *cannot* process personal data for the purpose of their own interests – even if legitimate – where such interests are overthrown by the interests, rights or freedoms of the data subjects themselves. It seems, therefore, that the EU legislator has foreseen the potential abusive recourse to Article 6(1)(f) GDPR in a way that could be detrimental to data subjects' fundamental rights and freedoms, and tried to counterbalance this risk by placing them at the heart of that provision. Article 6(1)(f) GDPR is thus particularly relevant to analyse in the context of this study, given the dual aim it seems to pursue, i.e., on the one side, allowing controllers to process personal data whenever such processing benefits their (legitimate and lawful) interests, while, on the other side, protecting data subjects against the potential harmful effects of such processing.

Before discussing this duality, it seems first necessary however to clarify what the terms *'legitimate interests'* mean. The recitals of the GDPR provide several examples of processing operations which can be considered as *'necessary'* for the *'legitimate interests'* of a controller or of a third-party, such as:

- Fraud prevention: the processing of personal data in the event the controller suspects a fraud can also be regarded as necessary to protect the legitimate economic interests of a controller (e.g. an insurance company that would try to establish whether a claim is real or part of an insurance fraud);⁸⁷⁸
- Network and information security: data processing for network and information security can also be based on Article 6(1)(f) GDPR. Network and information security relate to the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data.⁸⁷⁹ In that context, controllers and processors, including computer emergency response teams (CERTs) or providers of electronic communications networks and services, may legitimately need to process personal data;
- Security via video surveillance: controllers may rely on video surveillance to ensure the security of their property, staff or other third parties (including customers) when there exists a risk of accident, theft, or vandalism. This can include the recording of sounds or images in planes, banks, concert halls, stores, etc;
- Direct marketing: unless provided otherwise into national law,⁸⁸⁰ controllers may process the personal data of *existing* customers for marketing purposes based on their legitimate interests to maintain a relation with them.⁸⁸¹ To counterbalance the intrusive aspects of direct marketing, however, data subjects have in parallel been granted with an absolute right to object to direct marketing;⁸⁸²
- The defence of legal claims: the processing of someone's personal data can be justified when intended for the defence of legal claims (e.g., a company could be processing the personal data of a former employee in the context of a dispute before the courts relating to unpaid wages or an unfair dismissal).⁸⁸³

⁸⁷⁸ Recital 47 of the GDPR.

⁸⁷⁹ Recital 49 of the GDPR.

⁸⁸⁰ Next to the GDPR, the e-Privacy Directive applies to the processing of personal data in the context of electronic communications. Because the e-Privacy Directive is not directly applicable, Member States had to transpose it into national law, and were given some margin of manoeuvre in that respect. Hence, some member States have decided to adopt a less permissive approach regarding direct marketing and have required from controllers to obtain the consent of data subjects before processing their data for marketing purposes. Hence, it is sometimes not legally allowed for controllers to invoke their legitimate interest to keep existing clients informed about their services or products, or otherwise process their personal data for marketing purposes. The rules with respect to direct marketing may thus vary from one Member State to another.

⁸⁸¹ *Ibid.*

⁸⁸² Article 21(2) and (3) GDPR.

⁸⁸³ Article 9(1)(f) GDPR even allows controllers to process *sensitive* personal data where necessary for them to defend (themselves against) a legal claim, whether in the context of a settlement or court procedure.

This, of course, is not an exhaustive list. Hypothetically, controllers could invoke any interest which they would consider legitimate enough to justify the processing of personal data. While some DPAs have already adopted a very restrictive approach of the notion of 'legitimate interests',⁸⁸⁴ the CJEU itself has not (yet)⁸⁸⁵ established any clear limitation as to the scope of these legitimate interests. As mentioned above, Article 6(1)(f) GDPR could thus easily turn into a 'catch-all' provision that would indirectly annihilate the relevance of the other legal bases listed in that Article. Controllers could indeed be tempted to systematically invoke their private interests to justify any type of processing activity without caring too much about whether another legal basis would be more fitted, or whether their interests are truly 'legitimate'.

To limit the instances in which Article 6(1)(f) GDPR can validly be used as a legal basis for processing, additional conditions have been set by the EU legislator: first, the GDPR clarifies that Article 6(1)(f) GDPR cannot be used for processing activities carried out by public authorities in the performance of their tasks.⁸⁸⁶ This greatly reduces the number of potential situations in which this rather loose legal basis may be used. Second, Article 6(1)(f) GDPR itself establishes three conditions that must be fulfilled for that legal basis to be used. In *Rīgas satiksme*, the CJEU confirmed that a three-step test is indeed required prior to relying on that legal basis: first, the controller must demonstrate the pursuit of a *legitimate interest*; second, the controller must demonstrate the *necessity* to process the concerned personal data for the purposes of the pursued legitimate interest; and third, the controller must be able to demonstrate that the fundamental rights and freedoms of the data subjects do not take precedence over this interest.⁸⁸⁷ In line with this third step, controllers must thus conduct an assessment *before* starting to process any personal data. The CJEU has on a number of occasions established that this assessment must comprise a concrete balancing of the legitimate interests of the controller, on the one hand, and the fundamental rights and freedoms of the data subject, on the other hand.⁸⁸⁸ If it appears from this balancing test that the processing activity that they intend to conduct could, for example, disproportionately interfere with the right to privacy of the data subjects, such processing activity should not be started.⁸⁸⁹ The controller would then be forced to abandon the envisaged processing, or would have to rely on

⁸⁸⁴ Most notably, the *Autoriteit Persoengegevens* (the Dutch DPA) has adopted a guidance note in which it considers that a legitimate interest is one designated as a legal interest under law, and must have an "*urgent and specific character*" deriving from a rule or principle of law. According to the Dutch DPA, purely commercial interests do not constitute a legitimate interest under Article 6(1)(f) GDPR. This restrictive position has been contested by the European Commission, but no binding judgment has been rendered by the CJEU yet on this specific question.

⁸⁸⁵ A case is currently pending at the CJEU regarding whether purely commercial interests could be considered as legitimate interests under Article 6(1)(f) GDPR or not (C-621/22 - Koninklijke Nederlandse Lawn Tennisbond).

⁸⁸⁶ Last sentence of Article 6(1) GDPR.

⁸⁸⁷ Article 6(1)(f) GDPR, second part of the sentence.

⁸⁸⁸ CJEU, Judgment of 24 November 2011, *ASNEFF and FECEMD*, Joined cases C-468/10 and C-469/10 ; CJEU, Judgment of 4 May 2017, *Rīgas satiksme*, Case C- 13/16.

⁸⁸⁹ CJEU, *ASNEFF and FECEMD*, Joined cases C-468/10 and C-469/10, para. 38

an alternative legal basis, such as requesting the freely given, informed and specific consent of the individuals concerned.⁸⁹⁰

Recital 47 of the GDPR further clarifies the type of balancing test that must be carried by the controller in the following terms: “(...) *the existence of a legitimate interest would need **careful assessment** including whether a data subject can **reasonably expect** at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects **do not reasonably expect further processing.**” The EU legislator thus put particular emphasis on the reasonable expectations of the data subjects within this balancing test, thereby echoing the principle of lawfulness, fairness and transparency enshrined in Article 5(1)(a) GDPR. Furthermore, it clearly appears from this provision and from recital 47 that the ‘careful assessment’ to be performed puts at its very heart the interests, rights and freedoms of data subjects themselves, thereby echoing the FRO of the GDPR.*

As an illustration, if a car insurance company envisages to prevent insurance fraud by using a new software which calculates the likelihood of a false claim by a client (depending on a variety of personal data such as the age, gender or number of notified accidents of the insured person), this company would first need to envisage the impact that this type of processing could have on the interests, rights and freedoms of the data subjects, including the right to privacy or non-discrimination. Multiple factors would have to be considered as part of this assessment, such as whether the data subjects can reasonably expect such processing to take place based on their relations with the controller,⁸⁹¹ or whether the parameters that will be processed for that purpose could have discriminatory effects (e.g. data on age or gender). In the event this assessment would show – based on all the relevant circumstances of the case,⁸⁹² that the interests of the insurance company are overridden by the rights or freedoms of the data subjects, the insurance company should refrain from processing these personal data.

It may be the case of course that the legitimate interests of the controller do prevail over the conflicting rights of the data subject. In the case *Rīgas satiksme*, for example, the CJEU admitted that a third party could reveal to a person having suffered a damage the identity and address of the person having caused that damage (i.e., the data subject), given that such disclosure was indeed necessary for the injured party to be able to exercise a legal claim against the tortfeasor. According to the CJEU, taking into account this aim and the nature of the processing, the interference with the right to privacy of the data subject could indeed be considered

⁸⁹⁰ Articles 6(1)(a) and 7 GDPR.

⁸⁹¹ Recital 47 of the GDPR.

⁸⁹² CJEU, *ASNEFF and FECEMD*, Joined cases C-468/10 and C-469/10, para. 40; CJEU, *Breyer*, C-582/14, para. 62; and CJEU, *Rīgas satiksme*, Case C- 13/16, para. 31.

(depending on the circumstances) proportionate and thus justifiable under Article 6(1)(f) GDPR.⁸⁹³

Although this balancing test is supposed to protect data subjects against unlawful processing, it cannot be denied that an important pitfall appears to exist in this respect: the fact that this ‘careful assessment’ is primarily left to the discretion of the controllers themselves. It could be expected indeed that, in most situations, controllers would favour the pursuit of their own private interests by minimising any impact that the envisaged processing activity could have on the interests, rights and freedoms of data subjects, including, for example, discriminatory effects, exclusion from a service, loss of a job opportunity, or any other economic or social disadvantage that the data subjects could unfairly endure.⁸⁹⁴ Hence, Article 6(1)(f) GDPR could possibly turn into a Trojan horse for the fulfilment of the FRO of EU data protection law.

Other provisions of the GDPR must however also be considered together with Article 6(1)(f) GDPR when assessing whether this specific provision renders that provision dysfunctional. In the opinion of the author indeed, this Trojan horse can eventually be tamed by relying on other provisions of the PRO triptych, such as: (a) the principle of accountability and the principle of lawfulness, fairness and transparency, which could be considered as violated if the controller is not in a position to demonstrate that it conducted a genuine ‘careful assessment’;⁸⁹⁵ (b) the obligation of controllers to inform data subjects about the envisaged processing, and in particular the nature of the legitimate interests invoked as a legal basis for the processing at stake;⁸⁹⁶ (c) the right of data subjects to object to the processing of personal data if they considered that their own rights prevail over the interests of the controller,⁸⁹⁷ as well as their right to lodge a complaint free of charge with the competent DPA, should a dispute arise on this point between the controller and a data subject.⁸⁹⁸ The DPA would then be able to review the assessment made by the controller, and to issue a warning or impose a ban on the litigious processing practice.⁸⁹⁹ These counterbalancing provisions – each belonging to a different panel of the PRO triptych – can thus effectively be used to prevent abusive use of the ‘legitimate interest’ basis by controllers, as it has already been the case in countless disputes.⁹⁰⁰

The *Lindqvist* case already discussed above provides one of the very first examples of the functional mechanics of the PRO triptych when used to put an end to a

⁸⁹³ CJEU, *Rīgas satiksme*, Case C- 13/16, para. 31-34.

⁸⁹⁴ These risks are explicitly acknowledged in Recital 75 of the GDPR.

⁸⁹⁵ Articles 5(1)(a) and 5(2) GDPR.

⁸⁹⁶ Article 13(1)(d) GDPR and 14(2)(b) GDPR.

⁸⁹⁷ Article 21(1) GDPR.

⁸⁹⁸ Article 77 GDPR.

⁸⁹⁹ Article 58(2)(a) and (f) GDPR.

⁹⁰⁰ Hundreds of decisions rendered by DPAs every year concern this particular topic. For a broad overview of these decisions, please consult the GDPRhub: [https://gdprhub.eu/index.php?title=Category:Article_6\(1\)\(f\)_GDPR](https://gdprhub.eu/index.php?title=Category:Article_6(1)(f)_GDPR).

processing practice that is based on the legitimate interests of the controller. In that case indeed, several colleagues of Mrs Lindqvist had objected to the publication of their personal data on the internet by Mrs Lindqvist. In an attempt to justify the processing of these data, Mrs Lindqvist had invoked her own legitimate interest to write small stories and share them with a larger public within the exercise of her freedom of expression. Even after deleting the concerned pages, she continued arguing that the processing of these data had been fair and lawful because, in her opinion, she had a legitimate interest to exercise her freedom of expression, and this legitimate interest was prevailing over the right to privacy of her colleagues. At the end of the day, however, the Swedish courts did not agree with Mrs Lindqvist's assessment and considered that the processing of her colleagues' personal data had been unlawful under the applicable data protection rules.⁹⁰¹ As a result, Mrs Lindqvist was ultimately condemned to pay a fine.⁹⁰² When the case reached the CJEU, the latter confirmed that the applicable provisions of data protection law allowed each Member States to balance the diverging rights and interests of the parties at stake, without unduly restricting freedom of expression.⁹⁰³

In conclusion, it can be argued that Article 6(1)(f) GDPR, although proven to be a source of conflicts between controllers and data subjects,⁹⁰⁴ does not render the framework dysfunctional *per se*. The above-mentioned principles, rights and obligations can indeed be combined into a legal continuum which provides leverage to data subjects seeking to assert their rights and freedoms against a controller who would unfairly or abusively rely on Article 6(1)(f) GDPR to process personal data. In particular, by establishing human-centric principles for all processing activities, imposing specific obligations on controllers with a view of guaranteeing the rights and freedoms of data subjects, and providing easily actionable rights to these data subjects, the EU legislator has enabled the formation of a solid legal sequence which indubitably increases the overall functionality of the GDPR with respect to the fulfilment of its FRO.

(ii) The obligation to inform the data subjects about the processing of their personal data as a functional empowerment tool

Articles 12 to 14 of the GDPR put controllers under the obligation to provide data subjects, at the latest at the time when personal data are obtained, with specific pieces of information about the processing of their personal data, such as the purposes of the processing and the applicable legal bases,⁹⁰⁵ the storage period

⁹⁰¹ CJEU, *Lindqvist*, paras. 14-17.

⁹⁰² CJEU, *Lindqvist*, para. 90.

⁹⁰³ CJEU, *Lindqvist*, para. 17.

⁹⁰⁴ Many disputes between controllers and processors concern the wrongful use of Article 6(1)(f) GDPR. See, for example, the following decisions from the Belgian DPA (the APD/GBA): 28/2020 ; 42/2020; 74/2020; 03/2021 ; 57/2021 & 125/2021.

⁹⁰⁵ Article 13(1)(c) GDPR.

during which each category of personal data will be kept,⁹⁰⁶ the categories of third-party recipients that will also process these data,⁹⁰⁷ or the existence of data transfers outside the EU/EEA⁹⁰⁸ (among others). Such information must, of course, be provided free of charge.⁹⁰⁹ In that sense, these Articles can be considered as the prolongation of the transparency principle enshrined in Article 5(1)(a) of the GDPR.⁹¹⁰

Information is a prerequisite to allow data subjects to be aware of the processing of their data, understand its implications, assess its fairness and eventually challenge the lawfulness or fairness of the processing practice, if need be.⁹¹¹ The right to rectification, for example, can only be effectively exercised by data subjects if they have first been made aware of the data which are being processed about them, so as to eventually notice that these data are partly inaccurate or incomplete. Similarly, the right to object of data subjects can only be exercised if the latter have been informed about the existence of the processing and of the fact that the controller relies on its own legitimate interests or on an overriding public interest as a legal basis for such processing.⁹¹²

The 39th Recital of the GDPR sheds light on the close relation between the transparency principle enshrined in Article 5(1)(a) GDPR, the obligation of controllers to provide specific pieces of information to data subjects under Article 12 to 14 GDPR, and the exercise of the rights of data subjects under Article 15 to 22, in the following terms:

“(…) It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the

⁹⁰⁶ Article 13(2)(a) GDPR.

⁹⁰⁷ Article 13(1)(e) GDPR.

⁹⁰⁸ Article 13(1)(f) GDPR.

⁹⁰⁹ Article 12(5) GDPR.

⁹¹⁰ Working Party 29, Guidelines on transparency under Regulation 2016/67 adopted on 29 November 2017, WP260 rev.01 17/EN, pp. 4-5.

⁹¹¹ *Ibid.*, p. 4.

⁹¹² The right to object can indeed only be exercised in instances where Article 6(1)(f) or (e) GDPR are used as a legal basis for the processing (i.e., the legitimate interests of the controller, or the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) or Article

processing of personal data and how to exercise their rights in relation to such processing.”

In most instances, information is provided by controllers in the form of a privacy policy or data protection notice available on the website of the controller.⁹¹³ Immediately, an obvious limitation to the functionality of such an obligation may come to the mind of anybody who has been surfing the internet recently, i.e., the difficulty for data subjects to access, read or understand such information. Prior research conducted in the US has shown that only a very small percentage of individuals (less than 1%) actually read the online privacy policies to which they explicitly or implicitly agree while using a website,⁹¹⁴ while a large majority of individuals usually ignore privacy policies because of their length and complexity (on average, understanding a privacy policy requires two years of college education).⁹¹⁵

In an attempt to at least partially solve those issues, the GDPR requires data controllers to provide information to the data subjects in a “*concise, transparent, intelligible and easily accessible form, using clear and plain language*”.⁹¹⁶ These requirements aim at protecting individuals against potential negligence or manoeuvres on the part of controllers with respect to their transparency obligation, including in cases where the information would be incomplete, unintelligible or too difficult to access. The obligation to inform data subjects under Articles 12 to 14 GDPR must thus be interpreted in light of the principle of lawfulness, fairness and transparency. Providing all the mandatory information in a purely legalistic fashion will thus not suffice from a compliance point of view, if it appears that the overall objective of this obligation – i.e., empowering the data subjects in the exercise of their other data protection rights – has not been achieved. This was confirmed by the Working Party 29 in the following terms:

“The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information is as important

⁹¹³ Working Party 29, Guidelines on transparency under Regulation 2016/67 adopted on 29 November 2017, WP260 rev.01 17/EN, p. 8.

⁹¹⁴ Meinert, D. B., Peterson, D. K., Criswell, J. R. & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations*, 4(1):1; Kohavi R. (2001). Mining e-commerce data: The good, the bad, and the ugly. International Conference on Knowledge Discovery and Data Mining. *ACM*, 8:13.

⁹¹⁵ Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*. 25(2):238–249.

⁹¹⁶ Article 12(1) of the GDPR.

as the actual content of the transparency information, which must be provided to data subjects.”⁹¹⁷

In the opinion of the author, this user-centric approach to the information obligation of controllers enhances the functionality of EU data protection law, in the sense that the real objective of this obligation is to provide data subjects with the necessary tools to assert their rights and freedoms. In that sense, it can be argued that the interpretative flexibility offered by the transparency principle is adjustably complementing the specific information requirements provided under Article 12 to 14 GDPR, which are in turn reinforcing the opportunity for data subjects to effectively exercise their rights.

As an example, on 21 January 2019, the French data protection authority (the CNIL) imposed a financial penalty of 50 million euros against the company Google LLC for lack of transparency, inadequate information, as well as lack of valid consent with respect to its tracking practices for advertising purposes.⁹¹⁸ Similarly, the Irish DPA (the DPC) imposed a fine of €225 million on WhatsApp for non-compliance with the principle of transparency under Article 5(1)(a) GDPR and its information obligation under Articles 12 to 15 GDPR, mainly because the information notice provided to WhatsApp users with respect to the processing of their personal data, although including all the mandatory information required under Article 13, remained overall unclear, and did not sufficiently empower data subjects with respect to their other rights.⁹¹⁹ In its decision, the DPC stressed in particular that the provision of information to data subjects *“goes to the very heart of the fundamental right of the individual to protection of his/her personal data which stems from the free will and autonomy of the individual to share his/her personal data in a voluntary situation (...)”*⁹²⁰

Based on the above considerations, it is argued that the functionality of EU data protection law is boosted by the legal sequence which exists between, (a) the principle of transparency under Article 5(1)(a) GDPR, which offers interpretative flexibility, (b) the specific obligation incumbent on controllers to provide detailed information to data subjects prior to the processing under Article 12 to 14 GDPR, which offers interpretative certainty, and (c) the right of data subjects under Article 15 GDPR to require (additional) information on the processing within a period of maximum three months⁹²¹ in case the provided notice appears incomplete or

⁹¹⁷ Working Party 29, Guidelines on transparency under Regulation 2016/67 adopted on 29 November 2017, WP260 rev.01 17/EN, p. 5.

⁹¹⁸ For more details, please refer to the following communication from the CNIL: <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.

⁹¹⁹ Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, available at https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf.

⁹²⁰ *Ibid.*, para. 701.

⁹²¹ Article 12(3) GDPR.

unclear. Of course, this sequence must also be envisaged together with the role that DPAs play in ensuring compliance with this informational PRO triptych. Enforcement is indeed essential to the functionality of the entire framework, as further discussed in Section 3.3 of this Chapter.

(iii) The record of processing activities (Article 30 GDPR) and the designation of a DPO (Article 37 GDPR) as monitoring measures against fundamental rights violations

Under Article 30 GDPR, controllers have the obligation to maintain a record of processing activities. According to Article 30(1) GDPR, this written record must contain a description of all the processing activities, their respective purposes, the categories of data subjects and personal data concerned, the recipients to whom personal data are disclosed, the existence of any transfer of personal data to third country, the applicable storage period, and the organisational and technical measures that have been put in place to ensure the security of processing.⁹²² Processors must also maintain such a record with respect to the processing operations carried out on behalf of a controller, without the need however to re-identify the categories of data subjects or personal data concerned.⁹²³

In the opinion of the author of this study, this obligation can be considered as an extension of the principle of accountability enshrined in Article 5(2) GDPR, since documentation is a key aspect of both transparency and accountability.⁹²⁴ Indeed, for controllers and processors, drafting such a record is a mandatory step that may give them a better overview of their processing operations, raise awareness on previously unidentified issues and thus ultimately increase their overall level of compliance. For DPAs, this record can also become a useful investigative tool, since it must be made available to them upon request, thereby allowing them to carry out compliance checks more easily.⁹²⁵

Self-employed individuals as well as some small and medium enterprises are exempted from this obligation, but only if they fulfil the following four cumulative conditions:⁹²⁶ (i) they employ fewer than 250 persons; (ii) they do not process sensitive data; (iii) the processing they carry out is not likely to result in a risk to the rights and freedoms of the data subject; and (iv) the processing is 'occasional'. Because of this last criterion, in practice, only few controllers will benefit from such

⁹²² Article 30(3) GDPR indeed provides that this record “*shall be in writing, including in electronic form.*”

⁹²³ Article 30(2) GDPR.

⁹²⁴ WP29, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, p. 2.

⁹²⁵ Article 30(4) GDPR.

⁹²⁶ Article 32(5) GDPR.

an exemption,⁹²⁷ thereby increasing the situations where such records should be established, to the benefit of transparency and accountability. Of particular relevance is also the condition relating to the risk that a processing activity may pose to the rights and freedoms of data subject; by establishing such a condition, it can be argued that Article 30(5) GDPR participates to the multi-functionality of EU data protection law with respect to its FRO, in the sense that it does not specifically refer to a risk posed to the right to privacy or data protection, but to *any* right or freedom of data subjects. If such a risk exists, then controllers *must* document all their processing activities.

A record of processing activities is also a central tool for the performance of the tasks of Data Protection Officers (DPOs). DPOs are experts in data protection law whose main task is to monitor the data processing activities of the controller or processor for which they work, with a view of advising the latter on how to (better) achieve compliance with EU data protection law. DPOs can thus be regarded as internal ‘watchdogs’ for compliance. DPOs must be designated by their controller or processor on the basis of their expert knowledge of data protection law and their ability to perform various tasks.⁹²⁸ These tasks include (a) informing and advising the controller, processor and employees on data protection compliance, including when a DPIA needs to be conducted (see sub-section (iv) below) ; (b) monitoring compliance with EU data protection law and with the controller’s internal policies (for example, a data retention policy or a data security policy), including in the context of compliance audits; (c) conducting awareness-raising and training of staff involved in processing operations; (d) cooperating with DPAs, and acting as a contact point for them, on any consultation or issues relating to processing; (e) acting as a contact point for data subjects with regard to all issues related to processing of their personal data and to the exercise of their data protection rights.⁹²⁹

Although any controller or processor may voluntarily decide to hire a DPO or a team of DPOs,⁹³⁰ some controllers or processors are *required* to do so under Article 37 GDPR. More specifically, designating a DPO becomes mandatory when:

- (a) the controller or processor is a “*public authority or body*”⁹³¹ (except for courts or independent judicial authorities);⁹³² and, in the private sector, when;

⁹²⁷ For example, if a person, besides being mainly employed, acts from time to time as an independent consultant for a handful of companies in the field of trademark or data protection law (i.e., no processing of sensitive personal data), that person – although qualifying as a controller when processing personal data in the context of this auxiliary activity – may be exempted from having to maintain a record of processing activity, since the processing of personal data is merely ‘occasional’.

⁹²⁸ Article 37(5) GDPR.

⁹²⁹ Article 38(4) GDPR.

⁹³⁰ Depending on the size of the company and the scope of the processing, only designating one person may not be sufficient, taking into account the fact that the DPO must have enough time and resources to be involved in all data protection issues and actively monitor compliance with the GDPR. Some bigger companies that process large amount of personal data have thus to designate a DPO team of 10 people or more.

⁹³¹ Article 37(3) further provides that a single data protection officer may be designated for several public authorities or bodies, taking account of their organisational structure and size

⁹³² Except for courts and tribunals acting in their judicial capacity (Article 37(1)(a) GDPR).

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require “*regular and systematic monitoring of data subjects on a large scale*”;⁹³³ or when

(c) the core activities of the controller or the processor consist of “*processing on a large scale of [sensitive data]*”.⁹³⁴

If a controller or processor does not have the obligation to hire a DPO but decides to do so on a voluntarily basis, it must then ensure that the person having the title of DPO performs all the tasks foreseen in Article 39 GDPR and has the necessary level of competence, knowledge and independence required under Article 38 GDPR.⁹³⁵ A May 2019 IAPP study revealed that, in the EU, an estimated 500,000 organisations have appointed a DPO or a DPO team – i.e., a fairly large but coherent number, taking into account the overall number of concerned actors on the EU territory.⁹³⁶

In the public sector, typical examples of entities having the obligation to hire a DPO include ministries, social security institutions, tax authorities, or – as far as they are public – hospitals, schools or universities.⁹³⁷ In the private sector, typical examples include insurance companies, security services providers, fund managers or banks, given that they have to conduct large scale monitoring of personal data for incident or fraud prevention, by relying on DDTs such as CCTV cameras or fraud detection software. Also in the private sector, other typical examples include any company or group of companies that process large amount of sensitive data, such as social media companies (cf. sensitive content shared by users), political parties (cf. personal data relating to political opinions), private clinics or medical centres (cf. health data), or dating app service providers (cf. data revealing sexual orientation).⁹³⁸

In light of the research question of this study, it is particularly relevant to note that any controller or processor whose core activities imply a ‘high risk’ for the right to privacy and data protection of individuals – either because of the public nature of the concerned entity or because of the scope and nature of its core activities – must designate a DPO. From the perspective of FRO of EU data protection law, it is also worth stressing that DPOs must necessarily be involved in the event of an incident or

⁹³³ Article 37(1)(b) GDPR.

⁹³⁴ Article 37(1)(c) GDPR.

⁹³⁵ Article 37 of the GDPR obliges controllers or processors to appoint a DPO only if they fall in one of these three scenarios: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of sensitive data.

⁹³⁶ IAPP, *Study: An estimated 500K organizations have registered DPOs across Europe*, available at: <https://iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe/>

⁹³⁷ According to a consistent case-law,

⁹³⁸ WP20, Guidelines on Data Protection Officers (‘DPOs’) adopted on 13 December 2016, WP 243 rev.0.

for any envisaged high-risk processing activity that could negatively impact the fundamental rights and freedoms of data subject. This is reflected in Article 33(3)(b) GDPR – which requires DPO to be timely involved and act as a point of contact between the controller/processor and the DPA in the event of a data breach, as well as Articles 30(1) and 35(2) GDPR – which requires the DPO to verify the lawfulness of any new data processing activity and to help conducting DPIA when required (on the obligation to conduct DPIA, see here below). In other words, the supervisory and advisory role of DPOs is accentuated in all situations where the fundamental rights and freedoms of data subjects could be threatened by a new DDT or processing practice – which, in turn, may provide the DPO with the opportunity to raise a red flag and advise the controller against the implementation of the new DDT or processing practice. Because of the obvious link between, on the one side, high risk processing activities and, on the other side, risk to the fundamental rights and freedoms of data subjects, it can therefore be deducted that DPOs play an important role for the protection of data subject’s rights and freedoms. The question remains, however, whether the role of DPO is truly ‘functional’ for achieving the FRO of EU data protection law. In other words, how easily and effectively can DPOs prevent or put an end to a violation of EU data protection law which can also negatively affect the fundamental rights and freedoms of data subjects?

At first sight, it appears that the role of DPO is open to several pitfalls which could decrease its functionality, the most obvious being a lack of independence on the part of the DPO, a lack of resources to fulfil their task, or even internal muzzling practices, whereby the opinions or advises of DPOs would simply be ignored. In this respect, it is worth mentioning that the GDPR provides for specific safeguards aiming at ensuring that DPOs can effectively fulfil their tasks, and alert decision-makers of compliance issues. These safeguards include, in particular:

- **Effective and timely involvement:** it is required from controllers or processors to ensure that their DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.⁹³⁹ For that purpose, controllers and processors are supposed to draft and implement various procedures and policies ensuring, for example, that the DPO participates to all relevant meetings where activities or projects involving the processing of personal data are being discussed, and regularly attend meetings of senior and middle management where decisions are taken.⁹⁴⁰ As explained by the WP29 indeed, “ensuring that the DPO is informed and consulted at the outset” should be “standard procedure within the organisation’s governance” to promote privacy by design and by default, and to ensure compliance from the outset.⁹⁴¹

⁹³⁹ Article 38(1) GDPR.

⁹⁴⁰ D’Ath, F. (2022). Luxembourg DPA Raises the Bar for Data Protection Officers. *European Data Protection Law Review*. 8(1):121 – 127. See also WP29, Guidelines on DPOs, *op. cit.*, p. 13-14.

⁹⁴¹ WP29, Guidelines on DPOs, *op. cit.*, p. 13.

- **Sufficient resources:** the DPO must be provided with sufficient resources, both in terms of time and material resources. In that respect, it is important to note that a DPO may have another function, or even be a person external to the company (such as a remote consultant or an attorney specialized in data protection law). In all cases, the controller or processor must ensure that its DPO has sufficient time to devote to their tasks. According to the CNPD, this means that DPOs who work for an organization which processes personal data on a large scale must be employed or hired on a full-time basis or full-time equivalent. Furthermore, depending on the size and structure of the organisation, it may be necessary to set up a DPO team. In such cases, the Working Party 29 has specified that the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.⁹⁴²

Beyond time management, sufficient resources also mean that DPOs must be provided with all the financial resources, infrastructure and training which are necessary for the latter to be able to perform their tasks (e.g. a working space, IT equipment, access to external services, etc.). The general wording of the GDPR in this respect allows for a flexible interpretation of what can be considered as “necessary resources”, taking into account the size of the controller, the scope or the complexity of processing activities;

- **Independence:** the GDPR also provides that DPO cannot receive any instructions regarding the exercise of their tasks. Equally importantly, they cannot be dismissed or penalised by the controller or the processor for performing their tasks. This safeguard was of course a prerequisite to ensure that DPO effectively play their role of watchdogs instead of turning into harmless pets;
- **Reporting and accountability:** the fact that DPOs must be able to directly report to the highest management level of their organisation can be regarded as another safeguard. Such direct reporting ensures that senior management, such as the board of directors of a company, is aware of the DPO’s advice and recommendations. General opinions and recommendation may be shared through bi-annual or annual report provided to the highest management level. For urgent issues, however, DPOs should be able to immediately raise their concerns or dissenting opinions to the highest management level and their intervention should be given due weight. In case of disagreement, the

⁹⁴² *Ibid.*, p. 14.

WP29 recommends, as good practice, to document the reasons for not following the DPO's advice,⁹⁴³ in line with the principle of accountability.⁹⁴⁴ Even if this does not guarantee that the said management will always give due weight to the advice of the DPO, it increases the accountability of controllers and processors, in the sense that they cannot pretend afterwards having ignored a compliance issue that the DPO had already raised before them.⁹⁴⁵

It is undeniable that these safeguards protect the role of DPOs, which in turn can boost compliance with EU data protection law, to the benefit of the rights and freedoms of data subjects. Yet, it is difficult to assess to what extent DPOs truly contribute to the fulfilment of the FRO of EU data protection law, given that DPOs are bound by secrecy and confidentiality in the performance of their tasks.⁹⁴⁶ This obligation of secrecy and confidentiality – although understandable from the point of view of controllers and processors, who need to be able to protect their right and interests, including intellectual property rights or trade secrets – may become highly problematic within organisation with a bad compliance culture. Indeed, it may prevent DPOs from bringing a violation to light, even in extreme cases where their advice or recommendations would be systematically rejected or disregarded, including when concerns over serious and systematic interferences with the rights and freedoms of data subjects would have been raised. Against this potential factor of dysfunctionality pertaining to the role of DPOs, it is worth emphasising however that the *“obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority”*.⁹⁴⁷ DPAs may thus be regarded as a ‘safe harbour’ for DPOs who may report some of their concerns directly to DPAs without fearing to breach their professional secrecy obligations or exposing themselves to lawsuits. In some instances, DPOs could even play the role of *‘(quasi-)whistle-blowers’*.⁹⁴⁸ This specific point will further be discussed in Section 3.3.2.2 and in the final Chapter of this study as part of the recommendations spelled out by the author of this study on how to increase the functionality of the GDPR.

Besides the hindering effect that DPO's professional secrecy obligation can have, it is also regrettable to note that the GDPR does not explicitly require DPOs to have at least intermediate knowledge of fundamental right law, so as to ensure that they are

⁹⁴³ *Ibid.*

⁹⁴⁴ Article 5(2) GDPR.

⁹⁴⁵ This can further be considered as an aggravating circumstance by a DPA when deciding on a sanction against a controller.

⁹⁴⁶ Article 38(5) GDPR.

⁹⁴⁷ WP29, Guidelines on DPOs, *op. cit.*, p. 18.

⁹⁴⁸ The term *‘quasi-whistle-blower’* is being used to highlight the role that DPOs can play in bringing violations to light. Whistle-blowers (formally, ‘reporting persons’) is however a specific category of defined in Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (*OJ L 305, 26.11.2019, p. 17–56*). Not all DPOs will qualify as ‘reporting persons’ under that Directive. They will only benefit from the protective regime of that directive if (i) they report or publicly disclose information on breaches of the GDPR acquired in a work-based relationship and (ii) fulfil the conditions laid down in Article 6 of that Directive.

able to quickly spot issues and advise their controller or processor in this respect. Fundamental rights law is a domain which require specific knowledge of some key rights and principles, such as the principle of lawfulness or proportionality, for being able to assess whether a new DDT or processing practice disproportionately interferes with the right to privacy, non-discrimination, integrity or human dignity. Rather, the GDPR non-specifically requires DPO to have professional qualities so as to be able to '*fulfil their tasks*'.⁹⁴⁹ Indirectly, of course, this means that DPO should normally be able to advise their controller or processor on the risk pertaining to the use of novel DDTs or processing practices for the fundament rights or freedoms of data subjects, since several provisions of the GDPR require a balancing test to be performed. Yet, the lack of explicit wording in this respect may lead controllers or processors to hire DPO who are expert in data protection law and can efficiently navigate the GDPR, despite a lack of background knowledge in fundamental rights law. As a consequence, it can be feared that DPOs mainly approach compliance issues from a legalistic perspective, rather than monitoring processing activities and providing insightful advice in light of the FRO of EU data protection law itself.

In general, looking back at both obligations, there is no doubt however that the requirements to keep a record of processing activities and, in some instances, to designate a DPO, increase both preventive compliance as well as the convenience with which potentially harmful data processing practices can be detected or denounced. Of course, an obvious hurdle to the effectiveness of these internal control mechanisms could be the negligence of controllers in complying with these obligations, or – even worst – the fraudulent intent of some controllers not to comply. Controllers and processors could, for example, willingly maintain an incomplete data processing records or appoint a strawman as a DPO. In the end, only a thorough audit on the part of a DPA could shed light on a lack of compliance with these obligations. The negligence or fraudulent intent of controllers – despite the clear requirements of the GDPR with respect to the role of DPO – must however be considered as *external* factors that could negatively affect the effectiveness and functionality of the framework. The provisions of the GDPR themselves do not allow or encourage these types of behaviours. On the contrary, controllers or processors that do not respect the requirements relating to the designation and role of DPO could be exposed to administrative up to 10 million euros or 2% of their worldwide annual turnover.⁹⁵⁰ Given the pivotal role that DPOs play in fostering a culture of compliance, some DPAs have been conducted regular checks. In Luxembourg, for example, the CNPD launched 25 different investigations in the public and private sector focused on the role of the DPO. Each of these investigations led to a decision whereby controllers where sanctioned each time it appeared their DPO was lacking the necessary resources for fulfilling the required tasks, did not have appropriate knowledge, or was not guaranteed to be timely and effectively involved in all data

⁹⁴⁹ Article 37(5) GDPR.

⁹⁵⁰ Article 83(4)(a) GDPR.

protection-related issues.⁹⁵¹ The importance of the investigative and correctives powers of DPAs for guaranteeing the effectiveness and functionality of EU data protection law will further be discussed below (see Section 3.3 on the Third Pillar of Functionality of EU data protection law).

(iv) The obligation to ensure data protection by design and by default (Article 25 GDPR) and to conduct DPIAs (Article 35 GDPR) as prevention tools against fundamental rights violations

Before initiating any processing of personal data, controllers have the obligation to integrate the key-principles of the GDPR into the envisaged operations, from the moment of their conception, both ‘by design’ and ‘by default’ (Article 25 GDPR). Moreover, if it appears that the envisaged data processing operations could pose a risk for the rights and freedoms of data subjects, the controller is obliged to conduct in parallel an impact assessment with a view of addressing and mitigating this risk (Article 35 GDPR). In the opinion of the author, Article 25 and Article 35 GDPR both reflect and give flesh to the general FRO of the GDPR, given that their ultimate aim is to ensure that controllers will not engage in any type of potentially harmful processing practice. These provisions do not simply focus on the right to privacy or data protection of the concerned individuals but are envisaging the consequences that processing could have on data subjects’ rights and freedoms in general, therefore comforting the idea that the GDPR can be used as a multi-functional tool for that purpose. The EDPB has further confirmed that the reference to the rights and freedoms of data subjects in those articles must be interpreted as covering all potentially affected rights and freedoms, such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.⁹⁵² There is thus no doubt as to the fact that these articles may be invoked for the protection of *multiple* fundamental rights. Another common characteristic of the obligation to conduct DPIAs and the obligation to ensure data protection *by design* and *by default* is their preventive nature. Indeed, controllers are required to actively find ways to comply with the GDPR *prior* to the start of the envisaged processing activity. As further discussed below however, while Article 25 GDPR applies horizontally to any type of processing activity, Article 35 GDPR only applies to so-called ‘high risk’ processing, including processing relying on a new type of technology.⁹⁵³ The specificities of each of these obligations as well as their respective contribution to the functionality of the GDPR will further be discussed below.

⁹⁵¹ For a summary of these decisions, please see D’Ath, F. (2022). *op. cit.*

⁹⁵² WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01 (17/EN)), as last revised and adopted on 6 February 2018, p. 6.

⁹⁵³ Article 35(1) and Recitals 89 and 91 GDPR.

Article 25 GDPR, entitled ‘Data protection by design and by default’, requires controllers to ensure that the processing activities that they intend to put in place are designed to embody the key-principles of data protection (i.e., data protection ‘by design’) and, also, that they will respect these principles when all their parameters are neutral (i.e., data protection ‘by default’). Article 25(1) GDPR stresses in particular that controllers should, from the outset, adopt technical or organisational measures that are specifically *designed* to implement the key-principles of processing into the intended processing operations. As an illustration, the article refers to the need to implement the principle of data minimisation by limiting the amount of data which is collected and by having recourse to pseudonymisation where possible. Article 25(2) GDPR further stresses that controllers should adopt and maintain technical and organisational measures which ensure that, by default, data protection principles are complied with. As an illustration, one may refer to the placing of cookies on the devices of internet users; by default, these cookies should be limited to what is strictly necessary for the user to be able to visit and navigate a webpage (so-called ‘functional cookies’), while leaving the opportunity to the user to accept more cookies by clicking on an icon (for example, cookies for personalised content). Another example is the implementation of access restriction policies, whereby access to databases is by default restricted to staff members who need it to perform their job. These types of measures have the preventive aim of guaranteeing the respect of the rights and freedoms of natural persons by limiting, in particular, the scope, duration or frequency of the processing, in accordance with the principle of purpose limitation, data minimisation and storage limitation.

Besides Article 25 GDPR, in the event the envisaged processing is likely to result in a ‘high risk’ to the rights and freedoms of natural persons, the controller is further required to assess and mitigate the impact of the envisaged processing activity. This additional obligation is set in Article 35 GDPR, entitled ‘Data Protection Impact Assessment’ (in short, DPIA). Contrary to Article 25 GDPR, which applies horizontally to any data processing activity, Article 35 GDPR only applies to so-called ‘high risk processing’. In practice, before initiating a new type of processing, controllers are required to take the following steps:

1) Identify any *prima facie* risk that the envisaged processing activity could pose to the rights and freedoms of natural persons, in order to determine whether conducting a DPIA is necessary or not. Controllers must be aware that conducting a DPIA is in any case mandatory when the intended processing activity includes one of the following operations:⁹⁵⁴

- the automated evaluation of personal aspects of a data subject to reach a decision that will produce legal or similarly

⁹⁵⁴ Article 35(3) GDPR.

significant effects on the person (e.g. automated assessment of somebody's creditworthiness, suitability for a job, etc.);

- when the envisaged processing activity includes processing of sensitive data on a large scale (e.g. grouping of different hospital databases);
- a systematic monitoring of a publicly accessible area on a large scale (e.g. installation of CCTV cameras in a school, on the streets, etc.).

2) When the intended processing activity qualifies as a 'high risk processing', the controller must conduct a thorough impact assessment in the form of a written report⁹⁵⁵ (i.e., commonly referred to as a 'DPIA report'). This report must comprise, at least:⁹⁵⁶

- a systematic description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects, including, as the case may be, any risk of discrimination, unlawful exclusion, censorship, movement restriction or invasion of privacy;
- the measures envisaged to address the risks, including specific safeguards, security measures and mechanisms (e.g. exclusion of any data containing protected characteristics or other data which could act as 'proxies' for protected characteristics; systematic human review of some categories of automated decisions; etc).

3) Where the DPIA report concludes that the processing would result in a high risk in the absence of any of mitigating safeguards, security measures or mechanisms, the controller is obliged to consult the competent DPA prior to starting the processing. Within a period of eight weeks, the DPA must then render its opinion on whether the controller has sufficiently or insufficiently identified and mitigated any residual risk. In some instances, the DPA can also provide written advice to the

⁹⁵⁵ Technically, the assessment could also be conducted via other means. In accordance with the principle of accountability, however, written documentation would be required, otherwise the controller would be unable to prove that it did perform a DPIA in accordance with the required standards.

⁹⁵⁶ Article 35(7) GDPR.

controller, or – if the processing appears incompatible with the standards of the GDPR – the DPA can issue a warning, a limitation or even a ban on the intended processing (among others).

According to the EDPB, an example of an unacceptable high residual risk includes instances where the data subjects may encounter significant or even irreversible consequences, which they may not overcome, such as being wrongfully laid off.⁹⁵⁷ The risk of a discrimination leading to the wrongful rejection of an applicant or the termination of an employment relation will be further explored in the following Chapter of this study, given that ‘e-recruitment’ has been selected as one of the test areas for this study (see Chapter 4.2, below).

Once read together, it clearly appears that Articles 25 and 35-36 GDPR aim at preventively and continuously guaranteeing the protection of the fundamental rights and freedoms of data subjects by imposing on controllers the obligation to only initiate and maintain processing operations or practices which are respectful of these rights and freedoms, especially when relying on novel or innovative technologies. Theoretically, strict compliance with Articles 25 and 35-36 GDPR would mean that any processing activity that could be detrimental to the rights and freedoms of data subjects would be nipped in the bud or terminated before any disproportionate interference would occur. Yet, one must admit that leaving these risk-based assessments to the discretion and appreciation of controllers can turn into an obvious pitfall. Negligent or ill-intentioned controllers could indeed perform poor assessments (if any at all), with a view of favouring the pursuit of their own interests over the protection of the rights and freedoms of data subjects. Another obvious pitfall in this respect relates to potential changes into the processing activity *after* the mandatory assessments have been performed and documented, so that the controllers appear compliant ‘*on paper*’ even if the processing activity in question has been modified. The discretion left to controllers in this respect could thus be an important factor of dysfunctionality.

The EU legislator seems however to have foreseen these pitfalls by adopting specific provisions meant to keep the autonomous appreciation of controllers in check. As far as the quality of a DPIA is concerned, for example, controllers must normally seek the advice of their DPO,⁹⁵⁸ where designated. In line with the principle of accountability, the advice of the DPO and the ultimate decisions taken by the controller must be documented within the DPIA itself.⁹⁵⁹ Furthermore, where appropriate, the controller should also seek the views of data subjects or of their

⁹⁵⁷ WP29, Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01 (17/EN)), as last revised and adopted on 4 October 2017, p. 19.

⁹⁵⁸ Article 35(2) GDPR.

⁹⁵⁹ Article 5(2) and 35(7)(d) GDPR.

representatives on the intended processing.⁹⁶⁰ This can function as an additional safeguards, given that data subjects could voice their concerns, challenge the point of view of the controller or even dissuade the latter from implementing the envisaged processing activity. Finally, the GDPR makes clear that once a DPIA has been conducted, the obligation of the controllers in this respect does not come to an end. Article 25 GDPR indeed requires controllers to regularly review the impact of their processing practices, “*especially where a processing operation is dynamic and subject to ongoing change.*”⁹⁶¹ Where a DPO has been appointed, such continuous internal control would furthermore be foreseen and supervised by the DPO, who would act as an independent compliance officer over the entire period of the processing.⁹⁶² Finally, the supervisory control operated by DPAs and the sanctions that they may impose on controllers who would have acted in breach of Article 25 and 35 can also function as a tool of deterrence and compliance. As with most provisions of the GDPR, it therefore appears that the functional nature of Articles 25 and 35-36 GDPR primarily derives from their interactions with other provisions of the PRO-triptych. Besides the above-mentioned provisions, another one should be mentioned in particular: Article 22 GDPR. The synergies between Articles 22, 25 and 35 GDPR, and the way they may ultimately enhance the functionality of the GDPR, will be further discussed here below.

(v) *The additional obligations of controllers relying on AIDM under Article 22 GDPR: a higher threshold of responsibility against a higher risk of fundamental rights violations*

Automated individual decision-making, or AIDM, is a type of processing that is exclusively performed by automated means, and which leads to a decision that has legal effects or similarly significant effects on the data subject. Due to the risks that AIDM pose for the rights and freedoms of data subjects, the EU legislator has specifically regulated this type of automated decisional processing. Before analysing this specific regime, it is first necessary however to understand what AIDM is.

(a) Understanding the notion of AIDM as regulated under Article 22 GDPR

Article 22(1) GDPR – entitled ‘*Automated individual decision making*’ – provides:

“[T]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal

⁹⁶⁰ Article 35(9) GDPR. It is specified however in the same Article that such step should only be taken “*where appropriate*”, and “*without prejudice to the protection of commercial or public interests or the security of processing operations*”, which would *de facto* greatly limit the instances where controllers would actively seek the point of views of data subjects.

⁹⁶¹ WP29, Guidelines on DPIA, *op. cit.*, p. 14.

⁹⁶² Article 39(1)(c).

effects concerning him or her or similarly significantly affects him or her” (emphasis added).

As made clear in Article 22(1) GDPR, AIDM may (but does not have to) involve profiling. Profiling is defined in the GDPR as a form of automated processing where personal data are used to evaluate, predict or analyse certain personal aspects relating to natural persons, such as their performance at work, economic situation, potential health issues or shopping behaviour.⁹⁶³ Profiling on the internet is commonly used nowadays for marketing purposes in almost all sectors. A beverage company, for example, can place cookies on the device of internet users with a view of collecting various personal data about those individuals, such as their age, purchase power or drinking habits, in order to profile and categorize them (for example, ‘high-income / spirits lover’ or ‘low-income / beer lover’), which will in turn enable this company to better target these potential customers by adapting its communications towards them.⁹⁶⁴ Although many people think of marketing as being the most common area for profiling,⁹⁶⁵ other sectors increasingly rely on it in order to improve their services or performances, including in the field of healthcare, employment, education, banking or insurance. Profiling may be used, for example, to find candidates for a specific job, to detect and prevent money laundering, or to make more accurate health predications with respect to a patient.⁹⁶⁶

When reading Article 22 of the GDPR, it can be inferred from its wording that, as a general rule, AIDM should not be performed on data subjects, as they have the right *not* to be subject to such automated decisions. The next paragraph however sets specific exceptions to this general rule by allowing AIDM when, for example, the data subject has explicitly consented to it, or when authorised by EU or Member State law.⁹⁶⁷ Generally speaking, it would thus be wrong to state that DDTs relying on AIDM are prohibited under EU law. Rather, they are tolerated as long as additional obligations and rights are being respected.⁹⁶⁸ Reliance on AIDM will indeed automatically provide the concerned data subjects with additional rights and increase the level of obligations controllers, as further explained below.

To fully understand the implications of AIDM in terms of additional rights and obligations, it is first necessary to clearly define when a data processing practice qualifies as an AIDM under Article 22, and when it does not. According to Article

⁹⁶³ Article 4(4) of the GDPR.

⁹⁶⁴ Art. 4(4) of the GDPR more particularly defines profiling as: “*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*”.

⁹⁶⁵ See literature referenced in the following sections.

⁹⁶⁶ WP29, Guidelines on AIDM, *op. cit.*, p. 19.

⁹⁶⁷ Art. 22(2)(a) and (b) of the GDPR.

⁹⁶⁸ In that sense, the author of this study thus concurs with the opinions of some scholars according to which AIDM is not subject to a general prohibition. See, in particular, *Thouvenin, F., Früh, A. & Henseler, S. (2022). Individual Decision-Making: Prohibition or Data Subject Right? EDPL 2/2022, 8:183-198.*

22(1) GDPR, two requirements must be fulfilled for a set of processing operations to qualify as an AIDM:

- first, the processing must lead to a decision which either produces *legal effects* on the data subject, or which “*similarly significantly affects*” the data subject;
- second, the decision must have been taken “*solely through automated means*”, that is, without any human involvement in the decision-making process.⁹⁶⁹

Regarding the first criteria, the existence of a legal effect suggests “*a processing activity that has an impact on someone’s legal rights,*”⁹⁷⁰ such as the freedom to associate with others, the right to vote, to receive social benefits or to take legal action. Hence, if a software is used to calculate the child support payable to a person, or to determine whether someone is allowed to vote during the next local elections based on a set of data such as level of incomes, residence, or civil status, the automated decision can be considered as producing legal effects on the individual concerned. By contrast, if a bridal shop uses a software to make a pre-selection of wedding dresses for each of their customers based on their average budget, clothing size or personal preferences, without any obligation for them to buy a dress from this shop, such a tool will *not* qualify as an AIDM, since it does not produce any legal effects on the customers.

It must be stressed however that, even if a fully automated decision does not produce any legal effect on the data subject, it could still be regulated under Article 22 GDPR if it “*significantly affects*” the individual concerned in a way that is similar to a legal effect. To be able to appreciate the level of impact of an automated decision on a data subject, such effects should always be appreciated *in concreto*, taking into account all the relevant circumstances of the case. The Preamble of the GDPR provides example of such automated decisions by referring to the automatic refusal of an online credit application and to the use of e-recruiting tools for excluding job candidates.⁹⁷¹ In both cases, the individuals subject to the AIDM are confronted to a decision that is likely to *significantly* affect them, although these decisions are characterized by the *absence* of any legal effects, in the first case because they are denied the possibility to enter into a contract, and in the second case because they may be deprived from the chance to be hired.

Despite their differences, the notions of a decision ‘*producing legal effects on*’ or of a decision ‘*significantly affecting*’ a data subject share the fact that both types of decision must meet a certain threshold of seriousness in order to fall within the

⁹⁶⁹ WP29, Guidelines on AIDM, *op. cit.*, p. 10.

⁹⁷⁰ *Ibid.*, p. 9.

⁹⁷¹ Recital 71 of the GDPR.

scope of Article 22 GDPR. Hence, trivial decisions about an individual – even if fully automated – will not be considered as part of a regulated AIDM process. For example, if a 40-years old manager fills in, out of curiosity, a free online survey entitled ‘*how good of a boss are you?*’, and is characterized as a ‘*mediocre manager*’, this result – even if fully automated – will not be considered as an AIDM in the sense of Article 22 GDPR, since it will not legally or similarly significantly affect him. At most, the result of the survey is likely to slightly influence the mood of that person for the rest of the day, but it will certainly not put into question their position or any advantages that they may receive from their company. By contrast, if the same software is used by a company to test the skills of all its managers for the purpose of calculating their end-of-year bonus, such a software would most probably qualify as an AIDM under Article 22 of the GDPR.

The existence of a legal or similarly significant effect is not the only requirement that a decision must fulfil to qualify as an AIDM under Article 22 GDPR. On top of that, it must also be shown that the decision is *fully* automated. According to this second criteria, a process will thus only qualify as an AIDM if the decision concerning the data subject is taken *solely* on the basis of automated means. This implies that no human is involved in the decision-making process. For example, if an algorithm formulates a recommendation which will then serve as a basis for a human person to take a final decision concerning a data subject, this processing will not qualify as an AIDM under Article 22 GDPR.⁹⁷² Keeping this element in mind, it can be argued that the legally binding decision of a judge relying on the *non*-binding recommendation of a software like ‘COMPAS’⁹⁷³ would not fall under Article 22 GDPR since the final bail or sentencing decision rests with the judge.

An unscrupulous data controller could of course be tempted to circumvent Article 22 of the GDPR by asking a straw man – such as an obedient or unqualified employee – to (pretend to) review the automated decisions, so that they would no longer appear fully automated. The EDPB however made clear in its Guidelines on AIDM that controllers could not fabricate human involvement.⁹⁷⁴ Hence, for the human involvement to be considered as sufficiently meaningful, the human(s) involved in the decision-making should at least have the *authority* and *competence* to review and/or depart from the automated decision.⁹⁷⁵ For example, if someone would “*routinely*”⁹⁷⁶ rely on results generated by automated means to take a decision regarding data subjects, without having the possibility or competence to consider any other factors, such person would have no actual influence on the decision. In that case, the human involvement would thus not be considered meaningful enough, and the decision would qualify as an AIDM regulated under Article 22 GDPR.

⁹⁷² WP20, Guidelines on AIDM, *op. cit.*, p. 9.

⁹⁷³ See Section C, above

⁹⁷⁴ WP20, Guidelines on AIDM, *op. cit.*, p. 10.

⁹⁷⁵ *Ibid.*, p. 10.

⁹⁷⁶ *Ibid.*, p. 21.

(b) Overview of the additional obligations and rights deriving from the existence of AIDM

As mentioned above, AIDM are not strictly prohibited under EU law; rather, reliance on AIDM is subject to stricter rules. In particular, the use of an AIDM will grant additional rights to the concerned data subjects and, conversely, impose additional obligations on the responsible controllers.

As far as the additional obligations of controllers are concerned, they can be divided into two distinct categories: (i) obligations incumbent on the controller *prior* to subjecting an individual to an AIDM (i.e., *ex-ante* obligations); and (ii) obligations incumbent on the controller *after* an automated decision has been taken (i.e., *ex-post* obligations). An overview of these *ex-ante* and *ex-post* obligations is given in the below table.

TABLE 5

This table provides an overview of the ex-ante and ex-post obligations of controllers when the latter rely on AIDM under Articles 13-14 (information to data subjects) and 22 GDPR itself, respectively.

Ex-ante obligations	1.	Obligation to provide the data subject with meaningful information about the <u>logic</u> involved, as well as the <u>envisaged consequences</u> of the AIDM.	Article 13(2)(g) and 14(2)(f) GDPR.
	2.	Obligation to have a <u>valid legal basis</u> for the AIDM among the following three options: the data subject's explicit consent, a legal authorization or contractual necessity.	Article 22(2) GDPR.
Ex-post obligations	1.	Allow each data subject to <u>express their point of view</u> .	Article 22(3) GDPR
	2.	Allow each data subjects to <u>contest and challenge the automated decision</u> .	Article 22(3) GDPR
	3.	Provide <u>human intervention</u> upon request from a data subject.	Article 22(3) GDPR
	4.	Implement <u>any other suitable measures</u> necessary to safeguard the data subject's rights and freedoms and legitimate interests, such as	Article 22(3) and Recital 71

		providing an explanation of the automated decision.	GDPR
--	--	---	------

The obligations of controllers and, conversely, the rights of the data subjects with respect to AIDM are like the two sides of a coin. Quite logically, the fact that controllers have the duty to inform data subjects about the existence, consequences and logics of an AIDM supposes that data subjects have the right to be informed about it, prior to the processing, in accordance with Article 13 and 14 GDPR. Similarly, the fact that a controller should stand ready to provide a human review upon request from a data subject implies that data subjects have the right to be granted such a human intervention. It is also obvious that these additional rights and obligations principally aim at empowering data subjects by allowing them to contest automated decisions impacting them in a significant way. For the sake of clarity, the below section will discuss the functionality of Article 22 GDPR in terms of the obligations of controllers. It must be kept in mind, however, that the same considerations could be made with respect to the corresponding rights of the data subjects when their personal data have been processed in the context of an AIDM.

(c) The ex-ante obligation of controllers to have a valid legal basis prior to any AIDM: a factor of (dys)functionality?

As far as the ex-ante obligation to guarantee the lawfulness of AIDM is concerned, the EU legislator has restrictively listed the valid legal bases which can be invoked for such type of processing. In particular, when an AIDM relies on *non-sensitive* personal data, only three legal bases are available under Article 22(2) GDPR: (i) the controller has obtained the explicit consent of the data subject with respect to such AIDM; (ii) the AIDM is authorised by EU or Member State law (for example, this can be the case for fraud and tax-evasion monitoring and prevention purposes),⁹⁷⁷ on the condition that the law in question lays down suitable safeguards to protect the data subjects' rights, freedoms and legitimate interests; and (iii) the AIDM is necessary for entering into or for the performance of a contract to which the data subject is a party.⁹⁷⁸ If a company, for example, processes information about the spending behaviours of its customers to determine (exclusively through automated means) whether they can be part of a loyalty programme, it can only do so if the data subject has given his/her *explicit* consent, or if such AIDM is objectively necessary for entering into or for the performance of the loyalty programme.

⁹⁷⁷ Recital 71 of the GDPR.

⁹⁷⁸ Article 22(2)(a) to (c).

By contrast, when an AIDM relies on *sensitive* personal data, only two legal bases are available under Article 22(4) GDPR: (i) the explicit consent of the data subject; or (ii) the fact that such processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law, given that such law is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. If the judiciary of a Member State, for example, would like to integrate a special algorithmic process for the calculation of criminal penalties, such AIDM would have to be authorised by national law, and such law should provide sufficient safeguards to protect the rights, freedoms and interests of the data subjects concerned. One may imagine that the law could, among other, limit the use of such an algorithm to minor *financial* penalties only (thereby expressly excluding higher fines or prison sentences), and give to data subjects the right to challenge the automated decision before a specific commission or tribunal.

In theory, this restrictive approach is supposed to protect data subjects against the generalisation of AIDM and their potential harmful effects. Yet, the fact that the explicit consent of the data subjects may suffice for a controller to be able to lawfully rely on AIDM could, in some instances, become a factor of dysfunctionality of EU data protection law for the fulfilment of its FRO. Indeed, it cannot be ignored that the relation between data subjects and controllers is often characterized by an imbalance of powers. In some situations, data subjects may be nudged into giving their consent, or feel like they have no other choice than giving their consent if they want to have access to a product, service or social advantage provided by the controller (i.e., a job opportunity; an insurance; social allowances; etc). Allowing data subjects to consent to an AIDM which would otherwise be deprived of any legal basis could thus jeopardise the protective rules aimed at ensuring the respect of their rights and freedoms. Yet, to assess the extent to which ‘consent’ as a legal basis could become a factor of dysfunctionality, other provisions of the PRO triptych must also be considered. Among these provisions, one should mention, in particular: (i) the principle of lawfulness, fairness and transparency and its interpretative flexibility; (ii) the right of data subjects to withdraw their consent at any time under Article 7(3) GDPR ; and (iii) the specific requirements that exist for the consent of a data subject to be validly obtained under Article 4(11) GDPR, the obligation of controllers to provide meaningful information regarding the AIDM under Article 13(2)(f) and 14(2)(g) GDPR, or the obligation of controllers to implement suitable measures to guarantee the rights and freedoms of data subjects in the event of an AIDM, including providing them with the possibility to contest the automated decision under Article 22(3) GDPR. Once again, the legal continuum formed by the PRO triptych has to be considered in its entirety to appreciate the functionality of the GDPR for the defence of the fundamental rights and freedoms of data subjects.

Similarly, the fact that controllers may rely on an AIDM when they consider it is “*necessary for entering into, or performance of, a contract between the data subject*

and a data controller”⁹⁷⁹ may become a factor of dysfunctionality for the FRO of the GDPR, given that the notion of ‘necessity’ is not strictly defined in the GDPR, and could be broadly interpreted by controllers, which could even in some instances create a situation of contractual necessity to justify the use of an AIDM. To avoid abuses, the EDPB has however already clarified that necessity should not be confused with convenience but requires a strict test.⁹⁸⁰ In particular, the EDPB made clear that:

- the concept of necessity is factual rather than formalistic, in the sense that a contract cannot validly provide that an AIDM is *necessary* for the contract if such a statement is purely artificial;⁹⁸¹
- the AIDM must be *objectively* necessary for a purpose that is ‘integral to the contract’; the controller must thus be able to demonstrate that the main subject-matter of the contract cannot be performed if the AIDM in question does not occur;⁹⁸² and also
- the necessary nature of the AIDM does not only depend on the controller’s perspective (e.g. only economically viable option), but also on the reasonable data subject’s perspective when entering into the contract, and whether the contract can still be considered to be ‘performed’ without the processing in question.⁹⁸³

Furthermore, to assess the extent to which this legal basis could become problematic for the FRO of the GDPR, other provisions of the PRO triptych must be considered. Among these provisions, one should mention, in particular, the principle of lawfulness, fairness and transparency, as well as the principle of accountability. Regarding accountability first, such a principle implies that the burden of proof with respect to the ‘contractual necessity’ of performing an AIDM is primarily placed on the controller. Hence, it would be for the controllers to be able to prove that the AIDM is truly necessary for the contract, rather than for the data subjects to prove that it is not. Second, regarding the fairness principle, the interpretative flexibility offered by that principle may become particularly handy in situations where the overall context of the processing would tend to show that the AIDM is not ‘fair’ to the data subjects. The notion of fairness, although inherently vague in the GDPR, has indeed been interpreted by the EDPB in favour of the rights and freedoms of data subject. In that respect, the EDPB has already provided a non-exhaustive list of

⁹⁷⁹ Article 22(2)(a) GDPR.

⁹⁸⁰ EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019 (version 2.0), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

⁹⁸¹ *Ibid.*, para. 28.

⁹⁸² *Ibid.*, para. 30.

⁹⁸³ *Ibid.*, para. 32.

fairness elements which should always be respected while processing personal data.⁹⁸⁴ From the perspective of protection of data subject's rights and freedoms in the context of AIDM, the following elements are particularly relevant:

- Expectation – Processing should correspond with data subjects' reasonable expectations;
- Non-discrimination – The controller shall not unfairly discriminate against data subjects;
- Non-exploitation – The controller should not exploit the needs or vulnerabilities of data subjects;
- Power balance – Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided;
- Respect rights – The controller must respect the fundamental rights of data subjects and implement appropriate measures and safeguards and not impinge on those rights unless expressly justified by law;
- Ethical – The controller should see the processing's wider impact on individuals' rights and dignity;
- Truthful – The controller must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects;
- Human intervention – The controller must incorporate qualified human intervention that is capable of uncovering biases that machines may create in accordance with the right to not be subject to AIDM;
- Fair algorithms – the controller should regularly assess whether algorithms are functioning in line with the purposes and adjust the algorithms to mitigate uncovered biases and ensure fairness in the processing.

Once again, the legal continuum formed by the PRO triptych has to be considered in its entirety to appreciate the functionality of the GDPR in protecting data subjects' rights and freedoms against unlawful or unfair AIDM. Among this legal continuum, the other additional obligations of controllers in relation to AIDM must also be considered, as further discussed below. This continuum will also be tested in Chapter

⁹⁸⁴ EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2020 (version 2.0), p. 18. See also CJEU, Judgment of 1 October 2015, *Bara*, Case C-201/14.

4 of this study by relying on concrete examples in the sector of e-recruitment (Section 4.2, below).

(d) The ex-ante obligation of controllers to inform data subjects about the ‘logic’ and the ‘envisaged consequences’ of the AIDM as an empowerment tool

As far the obligation to provide information on the AIDM is concerned, the EU legislator requires controllers to be clear about the logic and the envisaged consequences of the AIDM *prior to* the processing itself.⁹⁸⁵ This information obligation is essential to thwart the lack of initial insight or influence that data subjects have on automated decisions in the first place.⁹⁸⁶ Indeed, if data subjects were not made aware of the existence of an AIDM or of its impact, they could not knowingly accept or challenge it.

The purpose of this specific information obligation is thus to give to data subjects the opportunity to better understand the AIDM, which may in turn prompt them to exercise other data protection rights, such as alerting the controller about the fact that some data may be inaccurate,⁹⁸⁷ request additional information on a specific element of the AIDM,⁹⁸⁸ or even to challenge the fairness or lawfulness of the AIDM as a whole.⁹⁸⁹

In accordance with Article 13(2)(g) and 14(2)(f) GDPR, the ‘*meaningful information*’ that controllers must provide to data subjects prior to conducting an AIDM has two main components: (i) the *logic* being the AIDM, and (ii) the *envisaged consequences* of the AIDM. The GDPR does not specify however the degree of details which must be provided to the data subjects with respect to each of these components. If, for example, a bank uses an algorithm which profiles loan applicants in order to predict, in the form of an overall percentage, the likelihood of default of payment on the basis of 20 different parameters (e.g. amount requested ; duration of the loan ; purpose of the loan ; applicant’ net monthly revenues, level of education, family status, etc.), there is no specification codified in the GDPR as to whether it would be enough for the bank to provide general information about the logic behind that algorithm, or if a detailed account of each parameter and of their varying influence on the overall result should be provided. If the second option was chosen, there exists the risk that data subjects would be overwhelmed by the information provided

⁹⁸⁵ According to Article 13(1) and 14(1) GDPR, this information should indeed be provided at the latest “*at the time when personal data are obtained (...)*”.

⁹⁸⁶ Brkan, M. (2019). Do Algorithms Rule the World? Algorithmic Decision-making and Data Protection in the Framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 27(2), p. 97.

⁹⁸⁷ Article 16 GDPR. See also Section 3.2.3 below on the rights of data subjects.

⁹⁸⁸ This is one of the additional ‘*suitable measure*’ that controllers may be requested to implement in accordance with Article 22(3), as exemplified in Recital 71 GDPR.

⁹⁸⁹ Article 22(3) GDPR.

and would not be able to understand the logic of the AIDM because of its high level of complexity. A balance must therefore be found between ‘too much’ and ‘too little’, as well as ‘too complex’ or ‘over-simplified’ information. Less doubtless is the fact that this information obligation requires controllers to be at least *able* to understand the functioning of the algorithms themselves. As explained above, however, this can be difficult to achieve when the algorithm in question is a complex self-learning algorithm. Indeed, self-learning algorithms share the characteristic of continuously changing, refining and/or improving their predictive or other decision-making models over time, usually based on additional input data, without such changes being systematically visible or understandable for the persons who have initially coded such algorithms or who are using them.

Because of this opaqueness, one could question the use of self-learning algorithms overall. The great advantage of self-learning algorithms compared to exclusively human-programmed algorithms is the speediness of their development, as well as the – sometimes inexplicable – accuracy of their predictive models, which often beat even the most trained or experienced human mind. As an illustration, one may refer to two self-learning algorithms of the firm DeepMind⁹⁹⁰: AlphaZero – an algorithm which has beaten the world’s best chess-playing computer program after teaching itself to play chess in under four hours⁹⁹¹ – , and AlphaGo Zero – an algorithm which has learned to master the Japanese game of Go *tabula rasa*.⁹⁹² The main issue concerning smart algorithms is their lack of transparency. When only the input data and the output data can be analysed, but not the in-between process, controllers cannot understand the functioning of the algorithm (cf. the ‘black box’ metaphor). As a result, many scholars⁹⁹³ have interpreted the information obligation of the GDPR as prohibiting or at least restricting the use of ‘smart’ algorithms developed through machine-learning, given that such tools are characterized by their opacity (i.e., the so-called ‘black box’ metaphor).⁹⁹⁴ Simply knowing about the input and output data within the framework of an AIDM would indeed not suffice, since controllers must also be able to inform the data subjects about the *logic* involved, i.e., the in-between process. To achieve the required level of algorithmic transparency, other technological tools may thus be needed, such as algorithms specialised into ‘reading’ smart algorithms and making their underlying logic apparent.⁹⁹⁵

⁹⁹⁰ A subsidiary of the ‘tech giant’ Google Inc.

⁹⁹¹ Gibbs, S. (2017, December 7). AlphaZero AI beats champion chess program after teaching itself in four hours. *The Guardian*. <https://www.theguardian.com/technology/2017/dec/07/alphazero-google-deepmind-ai-beats-champion-program-teaching-itself-to-play-four-hours>.

⁹⁹² Silver, D., Schrittwieser, J., Simonyan, K., Antonoglou, I., Huang, A., Guez, A., Hubert, T., Baker, L., Lai, M., Bolton, A, Chen, Y., Lillicrap, T., Hui, F., Sifre, L., Driessche, G., Graepel, T. & Hassabis, D. (2017). Mastering the game of Go without human knowledge. *Nature*, 550:354-359.

⁹⁹³ Brkan, M. (2019), *op. cit.*, pp. 120-121; Casey, B. Farhangi, A. & Vogl, R. (2019). Rethinking Explainable Machines: The GDPR’s ‘Right to Explanation’ Debate and the Rise of Algorithmic Audits in Enterprise. *Berkeley Technology Law Journal*, 34(1), p. 179.

⁹⁹⁴ On algorithmic opacity, see, *inter alia*, Burrell, J. (2016). How the Machine “thinks”: Understanding Opacity in Machine Learning Algorithms. *Big Data & Society*, 3(1), p. 12.

⁹⁹⁵ Wachter S., Mittelstadt B. & Russell C. (2017). Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289.

Further down the line, it has been argued by some scholars that the right to information on AIDM amounts to a *right to explanation*, in the sense that the controller should be able to explain to the data subjects how the AIDM functions.⁹⁹⁶ The debate on the existence of this so-called '*right to explanation*' has caused a lot of ink to flow in the literature.⁹⁹⁷ In the opinion of the author, these debates have not always been the most fruitful from the perspective of the FRO of EU data protection law. Explanation, indeed, does not necessarily lead to understanding; one may receive a detailed explanation on a specific algorithm without however being able to grasp its logic because of a lack of knowledge or time. Hence, even if a right to explanation would indeed exist under the GDPR, it may not as such empower data subjects in exercising their other data protection rights to assert their other rights or freedoms. Many scholars who have participated in debates on a potential '*right to explanation*' partly or fully acknowledge this issue.⁹⁹⁸

Against this background, of greater relevance is the notion of '*meaningful information*' itself. The adjective '*meaningful*' can first appear quite vague. Yet, when read together with Article 12(1) GDPR on transparency, it becomes clearer that controllers must provide data subjects with information that is both relevant and easy to understand. Under Article 12(1) GDPR indeed, any information provided to data subjects must be "*concise, transparent, [and] intelligible*", with controllers being required to use "*clear and plain language*", so that data subjects can understand the relevant aspects of the processing and be truly empowered by such information. In the context of AIDM, this means that the information must be clear enough so that data subjects are able to understand the reasons for the automated decision and decide whether to accept or contest it.⁹⁹⁹ This reading is supported by the EDPB itself, which acknowledges in its Guidelines on AIDM that "*a data subjects will only be able to challenge a decision or express their view if they **fully understand** how it has been made and on what basis*".¹⁰⁰⁰ The author agrees with this holistic and purposeful approach of Article 13(2)(g) and 14(2)(f) GDPR, in the sense that the ultimate purpose of this '*meaningful information*' obligation should be to allow data subjects to make an informed decision to opt-in, opt-out or challenge the lawfulness or use of the AIDM.¹⁰⁰¹ As stated by Brkan indeed, "*the logic involved into the automated decision is 'meaningful' only if the data subject can understand the factors and considerations on which the decision was based. An abstract*

⁹⁹⁶ Goodman, B. & Flaxman, S. (2017). EU Regulations on Algorithmic Decision-Making and a 'right to Explanation'. *AI Magazine*, 38(3):50-57.

⁹⁹⁷ Seen among others, Brkan M. (2019), *op. cit.*; Burt, A. (2017). Is there a 'right to explanation' for Machine Learning in the GDPR? *iapp: Privacy Tech*; Edwards, L. & Veale, M. (2017). Slave to the Algorithm? Why a 'right to an explanation' is Probably not the Remedy you are Looking For. *Duke Law & Technology Review*, 16(1). Selbst, A. D. & Powles, J. (2017). Meaningful information and the right to explanation. *International Data Privacy Law*, 7(4), p. 237.

⁹⁹⁸ Brkan, M. (2019), *op. cit.*, pp. 112-113; Casey, B., Farhangi, A. & Vogl, R. (2019). Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise. *Berkeley Technology Law Journal* 34(1): 143.

⁹⁹⁹ EDPB, Guidelines on Automated Decision-Making, p. 25.

¹⁰⁰⁰ *Ibid.*, p. 27. Emphasis added.

¹⁰⁰¹ This opinion is also advanced by Burt, A. (2017), *op. cit.*

*understanding of the system or the functioning of an algorithm will not be of much use to the data subject, especially if the decision rejects her request, for example, for a loan or a credit card.”*¹⁰⁰²

Regarding the actual content of this ‘*meaningful information*’, the author is of the opinion that it would vary from one AIDM to another, depending on all relevant circumstances of the case, such as the complexity of the AIDM, the nature of the personal data being processed or the categories of data subjects concerned.¹⁰⁰³ For example, an AIDM used by a bank for granting loans, which would function on ten objective parameters (e.g. loan duration ; requested amount ; applicants’ net revenues; etc.) and would only have two envisaged consequences (i.e., acceptance or rejection of the loan application), would be easier to understand for the concerned data subjects than a highly complex algorithm relying on hundreds of varying criteria. The characteristic of the concerned public should also be taken into consideration and the information should be adapted accordingly, depending on whether it is addressed, for example, to educated adults, elderly persons or young individuals. As an illustration, if the Ministry of Education of a Member State relies on a complex AIDM to allocate undergraduate places to high school students,¹⁰⁰⁴ the provided information should be adapted so that it remains intelligible for young adults, by having recourse, as the case may be, to flow charts, graphics or practical examples.¹⁰⁰⁵

As already mentioned above, providing meaningful information about an AIDM is a prerequisite to allow data subjects to assess and potentially challenge the fairness or lawfulness of automated decision-making process on them. As such, the obligation of controllers to provide such information can therefore be considered as a factor of functionality of EU data protection law. Yet, in the opinion of the author, and as also argued by Casey, Fahrangi and Vogl, the “*true power*”¹⁰⁰⁶ of this obligation primarily derives from the many synergies that it creates with other provisions of the PRO triptych, such as (i) the principle of lawfulness, fairness and transparency; (ii) the obligation of controllers to guarantee data protection by design and by default, and to conduct DPIAs; together with (iii) the right to access of data subjects, as well as their *ex-post* right to challenge the automated decision, express their point of view of the matter, and obtain a human review on their case (discussed here below).

¹⁰⁰² Brkan, M. (2019), *op. cit.*, p. 113.

¹⁰⁰³ This is in line with the purposeful approach that is generally adopted by the CJEU, DPAs and EDPB with respect to information.

¹⁰⁰⁴ Such being the case in France through the controversial application process called “Parcoursup”. See, ‘*Comment fonctionne le nouvel algorithme de Parcoursup (et quelles questions pose-t-il) ?*’, press article written by Sonia Princet, published on 3 April 2019 on www.franceinter.fr, available at <https://www.franceinter.fr/education/comment-fonctionne-le-nouvel-algorithme-de-parcoursup-et-queelles-questions-pose-t-il>. ‘*Parcoursup : "Beaucoup de gamins se découragent et renoncent à la fac"*’, press article written by Marie Piquemal, published 3 March 2018 on Libération.fr, available at https://www.liberation.fr/france/2018/03/15/parcoursup-beaucoup-de-gamins-se-decouragent-et-renoncent-a-la-fac_1636433/.

¹⁰⁰⁵ EDPB, Guidelines on AIDM, *op. cit.*, p. 26.

¹⁰⁰⁶ Casey, B., Fahrangi, A. & Vogl, R. (2019), *op. cit.*, p. 188.

(e) The ex-post obligation of controllers relying on AIDM to implement suitable measures to safeguards the rights and freedoms of data subjects

The ex-post obligations of controllers with respect to AIDM directly reflect and embody the FRO of the GDPR. Indeed, whenever a controller relies on AIDM, Article 22(3) GDPR requires the latter to “*implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests*”. Article 22(3) GDPR further specifies that such measures should “*at least*” include (i) providing data subjects with the right to express their point of view, (ii) allowing data subjects to challenge the decision, and (iii) ensuring a human intervention upon request from the data subject.

Allowing the data subject to contest an automated decision, express his, her or their point of view and obtain human intervention can be regarded as the last defensive barrier against harmful AIDM, as they allow the data subject to potentially reverse or alter the negative consequences that an automated decision already had on them. For these consequences to be reversed or altered, however, the human intervention granted to the data subject must be more than merely symbolical or superficial. A clear potential factor of dysfunctionality in this respect is that the GDPR does not specify the actual role that the human reviewer must play. The EDPB has attempted to fill this gap by interpreting this safeguard as meaning that the after the human reviewer should undertake a “thorough assessment of all the relevant data”, including the point of view and additional elements provided by the data subject, and that the human reviewer must have both the authority and capability to change the decision. Rubberstamping would thus not be considered as a genuine ‘human intervention’ in the sense of Article 22(3) GDPR. In the opinion of the author, this purposeful interpretation provided by the EDPB is more than legitimate. Merely requesting from controllers a purely *symbolical* human review would indeed be pointless from the perspective of protection of data subjects’ interests, rights or freedoms, and would thus be in contradiction with the spirit and objective of the GDPR itself.¹⁰⁰⁷ How this obligation is implemented and respected in practice, however, remains to be seen, as there is currently no case-law on that specific question (yet).

The use of the terms “*at least*” in Article 22(3) GDPR does not leave any doubt as to the mandatory character of the three specific measures contained therein. This list is however non-exhaustive. Controllers therefore remain under the obligation to adopt other ‘*suitable measures*’ whenever necessary to safeguard the rights and freedoms of data subjects. Recital 71 of the GDPR mentions one additional measure in particular, i.e., the provision of an “*explanation of the decision reached **after** such*

¹⁰⁰⁷ Article 1(2) GDPR, read in combination with Recitals 6 and 10 GDPR.

assessment".¹⁰⁰⁸ A data subject could thus request specific information about the decision that was reached for their particular case, on top of the ex-ante 'meaningful information' that the controllers was supposed to already give them. Controllers could of course decline such a request. The wording of Article 22(3) GDPR indeed suggests that the need to implement additional suitable measures, including the provision of an ex-post explanation, is left to the discretion of controllers. Yet, in accordance with the principle of accountability, it could be argued that controllers would ultimately be responsible for demonstrating that the rights and freedoms of the data subject were not put at risk by the processing. Providing an ex-post explanation of the automated decision could thus, in some instances, become a necessary element for compliance, especially if a data subject or a DPA specifically requests it.

As far as the multi-functional nature of Article 22 GDPR is concerned, one can note that the protective scope of this provision is not limited to the fundamental right to privacy or data protection but includes any other right or freedom that could be interfered with because of an AIDM, including human dignity, non-discrimination or freedom of expression, as the case may be. Recital 71 of the GDPR indeed expressly indicates that these measures should aim at preventing, inter alia, "*discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation.*" The multi-functional nature of Article 22 GDPR is also acknowledged by the EDPB in its Guidelines, which states that this Article aims at safeguarding the rights and freedoms of data subjects, including "*but not limited to*" the right to privacy.¹⁰⁰⁹ In the concluding part of these Guidelines, the EDPB further stresses that the obligation of controllers to implement 'suitable safeguards' under Article 22(3) GDPR implies that controllers should carry out frequent assessments on the relevant datasets to prevent undue discrimination through "*any bias [or] prejudicial elements, including any over-reliance on correlations*". The EDPB further adds: "*Systems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making including profiling are other useful measures. Controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies or discrimination on the basis of special category data. These measures should be used on a cyclical basis (...).*"

Against this background, there is no doubt that the ex-post obligations of controllers under Article 22(3) GDPR is meant to play a central role for the fulfilment of the FRO of the GDPR. Yet, whether this provision is truly functional for data subjects seeking to assert their rights and freedoms against potentially unfair and harmful AIDM should be appreciated in practice. The following Chapter of this study will precisely

¹⁰⁰⁸ Emphasis added. This illustrative measure indicates that data subjects should in some instances also be given an ex-post right to information in the form of an explanation, in addition to their ex-ante right to information under Article 12 to 14.

¹⁰⁰⁹ EDPB, Guidelines on AIDM, *op. cit.*, p. 6.

aim at testing the solidity of the PRO triptych in this respect. At this stage, it can already be noted that Article 22 GDPR undeniably puts at its very centre the need to ensure the respect of the rights and freedoms of data subjects, without limiting those rights and freedoms to privacy or data protection. Hence, different fundamental rights could benefit from the Articular, such as non-discrimination or consumer protection.

(f) Interactions between Article 22 GDPR and other provisions of the PRO-triptych

In the opinion of the author, to fully appreciate whether the GDPR regulates AIDM in a manner that is functional for the data subjects, multiples provisions of the PRO-triptych must be read and appreciated together. As already stated above indeed, the author of this study agrees with the opinion of Casey, Fahrangi and Vogl, according to which the “*true power*”¹⁰¹⁰ of Article 22 GDPR primarily derives from the synergies that it creates with other provisions of the PRO triptych.

As far as the obligations of controllers are concerned, the GDPR requires the latter to elaborate, monitor and correct AIDM processes to ensure their soundness and fairness in a preventive fashion, including on the basis of Article 25 GDPR (data protection by design and by default) or Article 35 GDPR (on Data Protection Impact Assessments), both discussed below. As far as the rights of data subjects are concerned, the GDPR gives them additional leverage, including by granting them a right to contest the automated decision and request human intervention (Article 22(2) GDPR). In other words, both controllers and data subjects *must* or *may* take an active part in the making and monitoring of fair AIDM, through a mixture of preventive obligations and reactive rights. This legal continuum is further solidified by the investigative and corrective powers of DPAs, who can play a central role in the creation of a strong compliance culture for the design, prototyping, field testing, and deployment of fair automated data processing systems.¹⁰¹¹

(vi) The obligation to ensure to security of processing and to report of data breaches as prevention and accountability tools

One of the most common risks associated with the processing of personal data is the risk of security breaches, also referred to as ‘personal data breaches’ or more simply ‘data breaches’.¹⁰¹² In recent years, many companies, institutions or authorities have been the victim of such breaches, whether caused by involuntary human errors (i.e.,

¹⁰¹⁰ Casey, B., Fahrangi, A., and Vogl, R. (2019), *op. cit.*, p. 188.

¹⁰¹¹ *Ibid.*, p. 188.

¹⁰¹² According to Article 4(12) GDPR, a personal data breach means ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’.

accidental breaches) or the result of wilful acts (i.e., intentional breaches). As an illustration, in July 2015, a group of hackers stole the personal data of users of the online dating website 'Ashley Madison', which connects married individuals seeking to have an extramarital affair.¹⁰¹³ The group of hackers, whose action was mainly driven by ideological reasons, threatened to release the users' personal data if the company administrating the 'Ashley Madison' website would not immediately shut it down. Because the company refused to do so, more than 60 gigabytes of data, including personal data, were ultimately leaked in August 2015, thereby exposing many users of the website.¹⁰¹⁴ Among the exposed individuals, millions of formerly anonymous members and many public figures were singled out, including politicians, priests, military members, civil servants or celebrities.¹⁰¹⁵ The exposure of these data had a dramatic impact on the life of many users and of their family, from divorce, to losing their job to suicide.¹⁰¹⁶

While intentional breaches are sometimes driven by ideological considerations, as was the case in the 'Ashley Madison' scandal, most cyberattacks are conducted by criminal groups with the intention of obtaining a ransom. In December 2019, for example, Maastricht University transferred 30 bitcoins (at the time worth around 200.000 EUR) to a criminal group who had hacked and blocked access to the university's computer systems, including email and research databases.¹⁰¹⁷ It was later found that the initial breach which had enabled the criminal group to conduct such an attack had resulted from an unidentified staff member clicking on a phishing e-mail.¹⁰¹⁸

Whether intentional or accidental, and regardless of the underlying reason, data breaches are characterized by the (ir)reversible destruction, loss, alteration, unauthorised disclosure or unavailability of personal data.¹⁰¹⁹ Each of this situation can be detrimental to the interests, rights and freedoms of the data subjects whose data have been compromised. Hence, to protect data subjects against the harmful consequences of data breaches, the GDPR impose several obligations on controllers and processors with respect to both the security of processing¹⁰²⁰ and the reporting of incidents.¹⁰²¹ These obligations can be divided into two categories of mandatory

¹⁰¹³ *Ashley Madison hack returns to 'haunt' its victims: 32 millions users now watch and wait*, by Zack Doffman, Forbes, 1 February 2020, <https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/>.

¹⁰¹⁴ *A Timeline of the Ashley Madison Hack*, press article by Nate Lord, Digital Guardian, <https://digitalguardian.com/blog/timeline-ashley-madison-hack>

¹⁰¹⁵ *Life after the Ashley Madison affair*, press article by Tom Lamont, 28 February 2016, the Guardian, <https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked>.

¹⁰¹⁶ *Ibid.* See also, *The Ashley Madison hack ruined my life*, press article written by Jose Pagliery, CNN business, 21 August 2015, <https://money.cnn.com/2015/08/21/technology/ashley-madison-ruined-lives/index.html>.

¹⁰¹⁷ *University of Maastricht says it paid hackers 200,000-euro ransom*, published on 5 February 2020, Reuters, <https://www.reuters.com/article/us-cybercrime-netherlands-university-idUSKBN1ZZ2HH>.

¹⁰¹⁸ *Ibid.* Following a declaration of University Vice President Nick Bos at a Press Conference.

¹⁰¹⁹ Article 4(12) GDPR.

¹⁰²⁰ Articles 24, 25 and 32 GDPR.

¹⁰²¹ Article 33 and 34 GDPR.

actions: preventive actions (i.e., Article 32) and corrective actions (i.e., Articles 33-34 GDPR), as further discussed below.

With a view of *preventing* data breaches, Article 32 of the GDPR requires controllers to implement various security measures. Article 32 GDPR can thus be seen as the continuation of the principle of integrity and confidentiality enshrined in Article 5(1)(f) GDPR. These technical and organisational measures must be chosen and implemented to ensure a level of security “*appropriate to the risk*”, taking into account all relevant elements, such as the nature or scope of the processing, but also to which extent “*the rights and freedoms of natural persons*” could be harmed in the event of a breach. Hence, Article 32 GDPR puts at its heart the need to protect the rights and freedoms of data subjects, including (but not limited to) their right to privacy. Among the measures that controllers can adopt, the GDPR mentions, *inter alia*, pseudonymisation, encryption, the ability to restore the availability of the data in the event of a technical incident (e.g. back-up system), or the adoption of internal policies to test, assess or improve these security measures.¹⁰²² Aware of the fast space at which technology is evolving, the GDPR does not codify the specific IT measures that must be implemented, nor any ISO standard which should be adopted by controllers to be considered as compliant. Rather, it is specified that controllers and processors should take as a reference point the ‘state of the art’.¹⁰²³ This, of course, can be seen as a positive element for the GDPR to be able to stand the test of time, but also for DPAs and other competent authorities who will be in charge of assessing whether controllers have sufficiently complied with that obligation.

While Article 32 GDPR is concerned with preventive security, Articles 33 and 34 GDPR, for their part, are concerned with the documentation and reporting of data breaches in the aftermath of such incidents. The ground rule in that respect is that controllers must keep a complete record of all data breaches and of the measures adopted to mitigate such incidents. In case the potential harmful consequences of a data breach cannot be fully mitigated, controllers must report the breach to the competent DPA as soon as possible, and in any case not later than 72 hours after having become aware of it.¹⁰²⁴ In the event the breach could significantly harm the interests, rights or freedoms of the data subjects, the latter also have to be alerted without undue delay.¹⁰²⁵ Articles 33 and 34 GDPR can therefore be considered as a prolongation of the principles of transparency and accountability enshrined in Article 5 GDPR.

The main element to be taken into consideration by controllers when determining whether a data breach must be reported is the risk that the breach in question represents for to the rights and freedoms of natural persons. In particular, Article

¹⁰²² Recitals 78 and 83 of the GDPR. Article 32(1)(a) to (c) of the GDPR.

¹⁰²³ Recitals 78 and 83 of the GDPR. Articles 25 and 32 of the GDPR.

¹⁰²⁴ Article 33(1) GDPR.

¹⁰²⁵ Article 34(1) GDPR.

33(1) GDPR provides that it is required to report a data breach to the competent DPA when the breach represents a *risk* to the rights and freedoms of natural persons. Similarly, Article 34(1) GDPR provides that it is required to communicate the data breach to the concerned data subjects when the breach is likely to result in a *high risk* to the rights and freedoms of natural persons. By contrast, in situations where the risk associated with a data breach has been fully mitigated (e.g. successful recall of an email sent to a wrong recipient; recovery of a database through a back-up system; etc.), the controller does not have to report the breach *per se*, but must document it internally in a special record comprising the facts relating to the personal data breach, its effects and the remedial action taken.¹⁰²⁶

Yet, it cannot be denied that an obvious caveat exists in this respect: the fact that the risk assessment referred to in Articles 33(1) and 34(1) GDPR is left to the discretion of controllers. It can be feared indeed that controllers would generally be reluctant to admit to and report data breaches, especially when they result from their own negligence, or if their long-term consequences can be dissimulated. In the recent years, the media have reported countless cases of data breaches that controllers had first attempted to conceal, as was the case for Uber, Warwick University or the Finnish firm Vastaamo.¹⁰²⁷ The robustness of the PRO triptych against such behaviours should however be assessed by taking into account other provisions of the GDPR. One may cite, *inter alia*, the principle of integrity and accountability, as well as the right of data subjects to lodge a complaint with a DPA and to obtain an effective judicial remedy. The competent DPA may also request access to the internal data breach record of the controller, investigate the case and impose a fine on any controller which would have failed to report a breach in due time. Such a fine can be up to 10 000 000 EUR or to 2 % of the total worldwide annual turnover of the controller, whichever is higher.¹⁰²⁸ The clarity of these principles, rights and obligations, coupled with the deterrent effect of a potential fine, has encouraged a surge in data breach reporting in the EU since the adoption of the GDPR.¹⁰²⁹ Between the year 2020 and 2021, for example, over 130,000 personal data breaches were notified to the competent DPAs - on average 356 breach notifications per day. By contrast, in the US, where less stringent obligations apply, only around

¹⁰²⁶ Article 33(5) GDPR.

¹⁰²⁷ See, for example, Marton, A. (2020, April 13). Warwick University was hacked and kept breach secret from students and staff. SKY NEWS. <https://news.sky.com/story/warwick-university-was-hacked-and-kept-breach-secret-from-students-and-staff-11978792>; Newcomer, E. (2017, November 21). Uber Paid Hackers to Delete Stolen Data on 57 Million People. *Bloomberg*. <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>.

¹⁰²⁸ Article 83(4)(a) GDPR.

¹⁰²⁹ McKean, R., Kurowska-Tober, E. & Waem, H. (2022, January 18). DLA Piper GDPR fines and data breach survey: January 2022. *DLA Piper*. <https://www.dlapiper.com/fr/france/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/>

1000 data breaches were reported to the authorities for the year 2020, i.e., around only two per day.¹⁰³⁰

Among the risks which may result from a data breach, the GDPR specifically mentions discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy or “*any other significant economic or social disadvantages*” to natural persons.¹⁰³¹ Since data breaches often lead to the disclosure of private details or the loss of control over personal data, the fundamental right to privacy and the right to personal data protection are the most likely to be infringed with in that context. Yet, interferences with other fundamental rights can also be feared depending on the nature of the personal data. As an illustration, one may refer to the Vastaamo data breach in Finland.¹⁰³² The psychotherapy firm Vastaamo had endured two data breaches in November 2018 and March 2019, whereby a hacker had gained unlawful access to thousands of patient records. These records included information about the identity, contact details and mental health issues of the patients concerned, including their name, social security number, email address and the actual written notes that therapists had taken.¹⁰³³ Despite being aware of these breaches at the time they took place, the management of the company first kept them secret and only reported them to the Finnish DPA in late September 2020, i.e., shortly after Vastaamo had started being subject to blackmail by the hacker. The following months, the hacker also tried to obtain monetary advantages from at least 15,000 patients by threatening them to publish their personal records. In the end, 300 records were actually leaked online on the Tor network by the hacker. Besides the clear interference with the right to privacy of the individuals concerned, some of the victims feared to be discriminated in their private or professional life because of the mental issues for which they were treated, and which had been revealed to the public. Taking these risks into account, as well as the fact that Vastaamo had failed to implement appropriate security measures or to report these breaches in due time, the Finnish DPA imposed a fine of €608,000 on the firm for the violations of Article 5, 32, 33 and 34 GDPR.¹⁰³⁴

It appears from the above that both the preventive and corrective obligations of controllers with respect to data breaches exist not only to guarantee the right to privacy and data protection of individuals, but also their other fundamental rights and freedoms, such as the right to integrity, non-discrimination or property. It can

¹⁰³⁰ Annual number of data breaches and exposed records in the United States from 2005 to 2020, published on 3 March 2021, available at <https://www-statista-com.proxy.bnl.lu/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/?pds=1432022140316829255558438394526>.

¹⁰³¹ Recital 75 GDPR.

¹⁰³² Tietosuojavaltuutetun toimisto (Finnish DPA), Decision 1150/161/2021 of 7 December 2021, available at <https://finlex.fi/fi/viranomaiset/tsv/2021/20211183>.

¹⁰³³ Ralston, W. (2021, May 4). They told their therapist everything. Hackers leaked it all. *Wired*. <https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/>.

¹⁰³⁴ *Ibid.*

therefore be argued that these obligations participate to the multi-functionality of EU data protection law with respect to its FRO.

(vii) The obligations relating to joint-controllership, sub-processing and the transfer of personal data outside of the EU/EEA

Finally, it is worth pointing out that the GDPR could have become impractical and therefore dysfunctional if controllers or processors could have easily escaped their responsibility by outsourcing whole or part of their processing activities to another person (i.e., a processor or sub-processor), or by transferring whole or part of their database to a recipient located in a third-country (i.e., a country outside of the EU/EEA). As already discussed above, however, safeguards exist against the dilution of the responsibilities of controllers in instances where multiple parties are involved, whether these third parties are located in or outside the EU/EEA (see, in particular, Section 2.3.2.4 on the rules applicable to data transfers, and Section 3.1.3.2(iii) on the obligation for controllers to adopt joint-controllership agreement or processing agreements every time they jointly process personal data with another controller or delegate (part of) their processing activity to a processor). A purpose-minded reading of these safeguards, which can respectively be found in Articles 26 to 29 GDPR, and in Articles 44 to 49 GDPR, reveals that the aim of the EU legislator was to ensure that the level of protection afforded to data subjects remain equivalent, regardless of the length or complexity of the chain of processing.

With respect to data transfers in particular, the Schrems saga discussed above (Section 2.3.2.4) makes it particularly clear that a central aspect of these rules is to ensure that data subjects can effectively exercise their rights under the GDPR even when these data are being transferred to a recipient located outside of the EU. In other words, these rules put at their heart the need to ensure the respect of the fundamental rights and freedoms of data subjects in the context of data processing, including their right to an effective remedy under Article 47 of the Charter. The clarity and high standards set by EU secondary law, read in light of the Charter, has thus provided the CJEU with the necessary tools to strike down two EU decisions that were running counter to the required level of data protection.¹⁰³⁵

These safeguards against the dilution of the responsibility of controllers can doubtlessly be categorised as factors of functionality of EU data protection law for the fulfilment of its FRO. Indeed, rather than being concerned with the facilitation of the free flows of personal data, they primarily relate to the facilitation of the exercise and enforcement of data subjects' rights in practice, especially when a processing activity could put at risks their interests, rights or freedoms. Overall, they

¹⁰³⁵ Reference is here made to the EU Commission decision on the adequacy of the Safe Harbor regime (2000/520/EC) and to the EU Commission Implementing Decision on the adequacy of the EU-US Privacy Shield regime (Decision 2016/1250).

therefore increase the ease or convenience with which data subjects, DPAs, NGOs or other interested parties can hold controllers and processors accountable for violations of fundamental rights through the prism of data protection law. Hence, although enforcement, whether at home or abroad,¹⁰³⁶ can remain a long and challenging endeavour for data subjects, a comprehensive review of the manner in which these safeguards have been interpreted and applied so far tend to confirm that they can actively contribute to the functionality of the overall framework. The final Chapter of this thesis will further spell out recommendation with respect to how such a functionality can further be increased by addressing certain external factors of dysfunctionality.

3.2.3. The Third Panel of the PRO Triptych: the panoply of rights of the data subjects

The above-mentioned key-principles and obligations are two panels of the triptych of legal tools available under the GDPR to ensure the respect of the fundamental rights and freedoms of individuals in relation to the processing of their personal data. A third important panel must still be discussed; the specific rights granted to data subjects under Articles 15 to 22 of the GDPR, as well as Articles 77 and 78 GDPR. This section will provide an overview of these rights before discussing their role in boosting the overall (multi-)functionality of the PRO-triptych. In particular, it will be argued that while rights confer convenient leverages to data subjects to boost compliance, they would lose their functionality if data subjects would not be able to easily exercise them, or if they would not been backed up by the third pillar of the functionality of the GDPR, i.e., its system of supervisory mechanisms and sanctions (see Chapter 3.3 below).

3.2.3.1. Overview of data subjects' rights under EU data protection law

TABLE 6

This table provides an overview and description of the rights of the data subjects under the GDPR, based on the name or the content of the relevant Articles (i.e., the word "right" must be explicitly mentioned).

1.	Right to information	Articles 13-14 GDPR: data subjects have the right to be informed, prior to the start of the processing, about the identity of the controller, the purpose and legal basis of each processing operation, the categories of recipients of the personal data, the storage period, the existence of any data transfers or AIDM, the data protection rights that they may exercise, and whether providing the data is a legal or contractual obligation. The information should be given in plain and clear language, and be precise, concise, easily accessible, and transparent. Such information is usually
----	----------------------	--

¹⁰³⁶ That is, mainly, due to external factors of dysfunctionality, such as the low budget on which DPAs have to run, discrepancies in national procedural law, language barriers, etc.

		provided in the form of a privacy policy or data protection notice made available to the data subjects online.
2.	Right of access	Article 15 GDPR: data subjects have the right to request any (missing or incomplete) information on the processing of their personal data as foreseen by their right to information, as well as a copy – free of charge – of their personal data undergoing processing on a support that is readable (e.g. electronic or paper copy).
3.	Right to rectification	Article 18 GDPR: data subjects have the right to obtain from the controller the rectification of inaccurate personal data concerning them, and to have incomplete personal data completed, including by means of providing a supplementary statement.
4.	Right to erasure	Article 17 GDPR: data subjects have the right to obtain from the controller the erasure of personal data concerning them in case the processing is no longer necessary or lawful (e.g. all the purposes of the processing have been achieved, the data subject has withdrawn his/her consent to the processing, or the processing was unlawful from the start).
5.	Right to restriction	Article 18 GDPR: data subjects may request controllers to restrict (i.e., temporarily limit or suspend) the processing, pending verification of the accuracy of the data, or the lawfulness of the processing, including when a data subject has objected to the processing because he/she considers that his/her legitimate interests, rights and freedoms override the legitimate grounds for processing of the controller pursuant to Article 6(1)(f) GDPR.
6.	Right to data portability	Article 20 GDPR: When a data subject has provided personal data to a controller, and that the legal basis for the processing is either the consent of the data subject or a contract, the data subject can request to receive those personal data in a structured, commonly used and machine-readable format, with a view of transmitting those data to another controller without hindrance. (e.g. transmission of photos from one cloud service provider to another for storage purpose).
7.	Right to object	Article 21 GDPR: The data subject has the right to object, on grounds relating to their particular situation, to the processing of their personal data when the legal basis is either 'legitimate interest' (Article 6(1)(f) GDPR) or 'public interest' (Article 6(1)(e) GDPR). This right is not absolute, unless the personal data are processed for direct marketing purpose.
8.	Rights in relation to AIDM	Article 22(3) GDPR: When subject to an AIDM, data subjects have <i>at least</i> the right to contest the automated decision, express their point of view and obtain a human intervention on the part of the controller (see section 3.2.2.2(v), above).
9.	Right to withdraw consent	Article 7(3) GDPR: When the processing operation is based on the consent of the data subject, the latter has the right to withdraw such consent at any time, in a manner that must be as easy as when they gave consent. The processing of the data must then be put to an end, unless the controller has another valid legal basis for the processing. The exercise of this right does not affect the lawfulness of the processing <i>prior</i> to the consent withdrawal.

10.	Right to lodge a complaint with a DPA	Article 77 GDPR: in the event of a dispute relating to the processing of personal data, data subjects have the right to lodge a complaint with any DPA free of charge, and in particular with the DPA of their country of residence, place of work or place, or where the alleged infringement took place. The DPA may then adopt a decision, including corrective or punitive measures against the concerned controller(s) or processor(s).
11.	Right to an effective remedy against a DPA	Article 78 GDPR: data subjects (but also controllers or processors) have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, including if the DPA does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint.

3.2.3.2. The non-absolute nature of data protection rights and their relation to other rights and freedoms

This study is meant to assess the degree of functionality of the GDPR in protecting the fundamental rights and freedoms of the data subjects in the context of the processing of their personal data, in particular when an interference with a DFR takes place through the use of modern DDTs. For the sake of practicality and achievability, the author has willingly decided to leave out the question whether the GDPR could also be used as a convenient tool to protect the rights, freedoms of interests of *others*, such as controllers, processors or third parties to the processing. Therefore, the following sections will focus on the various factors that make it easy for *data subjects* to activate and exercise their data protection rights, such as the right to access or the right to erasure, in order to assert their fundamental rights and freedoms. By contrast, the question whether the GDPR can also serve as a basis to defend the rights and interests of controllers, processors or third parties will not be specifically addressed, as it falls outside of the scope of this study.

Before highlighting their functionality, it must first be stressed that neither the fundamental right to personal data protection, nor the specific rights granted to data subjects under EU data protection law are absolute. The 4th Recital of the GDPR explicitly acknowledges this by stating that “*the right to the protection of personal data is **not an absolute right**; it must be considered in relation to **its function in society** and be **balanced** against other fundamental rights, in accordance with the principle of proportionality*” (emphasis added). Hence, controllers and processors may decide to reject a data subject’s request and (not) to rectify, disclose or erase personal data, including if the processing operations at stake pursue an overriding legitimate interest or are necessary to protect the fundamental rights and interests of others. For example, when a data subject requests a copy of their data under Article 15 GDPR, such a request can be rejected if the controller considers that it is manifestly unfounded or excessive.¹⁰³⁷ Similarly, when a data subject exercises their

¹⁰³⁷ Article 12(5) GDPR.

‘right to be forgotten’ by requesting the erasure of their personal data, the controller can reject such a request by demonstrating, for example, that the processing is necessary for compliance with a legal obligation¹⁰³⁸ or for the defence of a legal claim.¹⁰³⁹

Balancing data protection rights against other rights, freedoms or interests can lead to divergence of opinions. This is why, as discussed in the previous Chapter of this study,¹⁰⁴⁰ most of the judgments rendered by the CJEU in the field of data protection relate to an interpretative issue with respect to the balancing of the right to personal data protection with other rights, freedoms or public interests. The very first case – *Rundfunk* – concerned the balancing of the right to personal data protection and privacy of (ex) public servants (who did not want information on their revenues or pensions to be shared with the general public) with the right to a transparent public administration in Austria. The second case – *Lindqvist* – concerned the balancing of the right to privacy and personal data protection of members of the parish of Alseda (who did not want their private information to be published on the internet) and the freedom of expression of Mrs Lindqvist. The third case – *Satamedia* – was centred around the need to find a balance between the right to personal data protection of internet users (who did not want their identity to be revealed to a third party) and the right to intellectual property of record companies (who have an economic interest in fighting illegal music sharing). If, in each of these cases, the right invoked by the concerned data subjects had been absolute, such cases would have never reached the CJEU. In other words, it is mainly the non-absolute character of data protection rights that repetitively prompted national courts to refer cases to the CJEU for clarifying the interpretation to be given to EU data protection law, and in particular how to reconcile the exercise of data protection rights with other rights, freedoms and interests.

Similarly, many decisions rendered by DPAs in the field of data protection are centred around this sometimes-difficult balancing exercise. In 2020, the CNIL alone received 13,585 complaints (i.e., a 62.5% increase since the implementation of the GDPR),¹⁰⁴¹ a substantial portion of which originating from disputes opposing data subjects and controllers on the exercise of data protection rights. National courts must also carry out such a balancing exercise in a fair number of cases to clarify which elements should weigh in the balance. As an illustration, on the very day the author of this study is writing those lines, the German Supreme Court (Bundesgerichtshof issued, ‘BGH’) rendered a decision in which it was recognised that a landlord could validly reject the access request of one of its tenants (i.e., the data subject) pursuant to Article 15 GDPR, when disclosing such information could be detrimental to the right to privacy of another tenant (i.e., the informant), depending

¹⁰³⁸ Article 17(3)(b) GDPR.

¹⁰³⁹ Article 17(3)(e) GDPR.

¹⁰⁴⁰ See in particular Section 2.3, above, on the fulfilment of the FRO of EU data protection law.

¹⁰⁴¹ CNIL 2020 Activity Report, available at https://www.cnil.fr/sites/default/files/atoms/files/cnil_41e_rapport_annuel_-_2020.pdf.

however on the accuracy of the information originally provided by the informant.¹⁰⁴² At the origin of the dispute, the informant had complained to the landlord about strong odours and vermin in the stairwell, which were suspected to originate from the data subject's flat. The landlord therefore carried out an inspection of the data subject's flat and found it in a state of disrepair. The data subject however rejected the allegation according to which he/she was responsible for the strong odours or the vermin in the stairwell. A legal procedure ensued, in the context of which the data subject requested the landlord to disclose the identity of the informant pursuant to Article 15(1)(g) GDPR.¹⁰⁴³ The landlord however refused to grant access to such information, considering that the right to privacy of the informant was prevailing over the right to access of the data subject. Both the Regional Court of Ravensburg and the Higher Regional Court of Stuttgart agreed with the landlord's decision, which they considered in line with the applicable provisions of the GDPR. The German Supreme Court however specified that, when balancing the right to access of the data subject and the right to privacy of the informant, all the relevant circumstances of the case should have been taken into account by the lower judges, including, in particular, whether the information relating to the odour nuisance and the vermin in the staircase was actually accurate, or whether it had been a groundless allegation. The BGH noted that, in the case of a groundless allegation, the disclosure of the informant's identity by the controller could be lawful under Article 6(1)(f) GDPR, and would prevail over the informant's right to privacy, because necessary for the purposes of the legitimate interest pursued by the data subject to establish a legal claim or assert possible rights against the informant, from whom potentially inaccurate data originated, thereby causing damage to the data subject. This case illustrates the non-absolute character of the right to access and of data protection rights in general, as well as the complexity and intricateness of the above-referred 'balancing exercise'.

As an exception to what has just been said, it is worth mentioning that *one* data protection right can be considered as absolute, because prevailing over the legitimate interest pursued by the controller in all circumstances: the right to object to the processing of personal data for marketing purpose.¹⁰⁴⁴ Controllers have thus no choice but to stop processing the name, email address, or any other personal data of a data subject in the context of the marketing of goods, services, or activities, as soon as the latter has objected to such processing. This is the reason why marketing emails should normally always be accompanied by an 'unsubscribe' link at the bottom of the communication, which must allow the data subject to easily and

¹⁰⁴² BGH, VI ZR 14/21 Judgment of 22 February 2022, available at <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=128026&pos=7&anz=853>.

¹⁰⁴³ According to Article 15, data subjects have the right to obtain information about the source of their personal data, whenever the personal data were not directly collected from the data subject himself or herself (i.e., in this case, the source of the data was the informant).

¹⁰⁴⁴ Article 21(2) GDPR.

rapidly opt-out from the mailing list.¹⁰⁴⁵ This right to object to marketing communications is the only data protection right which can be considered as absolute. By contrast, all the other rights listed in the above table must be considered as non-absolute. Keeping this important element in mind, the author will now discuss the functional role that data subjects' rights can play within the PRO-triptych of the GDPR, and further highlight how the synergies between this panel and the other two panels of the PRO-triptych may increase the overall functionality of the framework for the defence of data subjects' fundamental rights and freedoms.

3.2.3.3. The functional role of data subjects' rights within the PRO-triptych of the GDPR

The data protection rights listed in the above table undeniably provide leverages to data subjects seeking to assert their rights and freedoms against potentially harmful data processing practices. Once activated, each of these right triggers a new obligation on the part of the controller or processor concerned: the obligation to respond to the request, without undue delay.¹⁰⁴⁶ This, in turn, may compel the controller or processor to analyse the processing activity concerned and address a potential lack of compliance on their part. Yet, as mentioned above, these rights would not be truly functional if exercising them would be subject to burdensome formal, substantial or procedural requirements. If, for example, data subjects would be required to communicate with the controller via registered letters, to pay a fee, or provide evidence of the unlawfulness of the processing before even being able to submit a request, this could dissuade them from exercising their rights in the first place. Similarly, if controllers could ignore data subjects' requests with impunity or did not have to respect any particular deadline for responding to such requests, these rights could become ineffective and less functional. To avoid this, the EU legislator has introduced several safeguards in the GDPR whose aim is precisely to facilitate the exercise of data subjects' rights. The below section will review those provisions to highlight the intrinsic functionality of data protection rights. Then, the following section will focus on the role of these rights play within the PRO-triptych of the GDPR, and in particular how the synergies between the key-principles of processing, the rights of data subjects and the obligations of controllers participate to the overall functionality of the GDPR.

First and foremost, Article 12(2) GDPR provides that controllers are under the obligation to facilitate the exercise of data subjects' rights under Article 15 to 22 GDPR. This supposes, for example, that the controller must be easily reachable.¹⁰⁴⁷ Furthermore, controllers cannot refuse to act on the request of data subjects exercising their rights under Articles 15 to 22 because some formal requirements

¹⁰⁴⁵ Article 21(4) GDPR. See also Belgian DPA (APD), Recommendation 1/2020 of 17 January 2020, available at <https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf>, pp. 53-54.

¹⁰⁴⁶ Article 12(3) GDPR.

¹⁰⁴⁷ Providing the contact details of the controller or the DPO is in any case a requirement under Article 13(1)(a) and (b) GDPR and 14(1)(a) and (b) GDPR.

would not be fulfilled.¹⁰⁴⁸ For example, controllers may not systematically request the data subjects to provide identification or other documents (such as a birth certificate or proof of residence) before accepting to analyse and respond to a request. Rather, the controller can only ask for the provision of additional information necessary to confirm the identity of the data subject where the controller has “*reasonable doubts*” concerning the identity of the natural person making the request.¹⁰⁴⁹ In that case however, it would be the duty of the controller to demonstrate that it is not in a position to identify the data subject.¹⁰⁵⁰ In practice, this would mean that, if a data subject submits a request to a controller, such as an erasure request, while indirectly confirming their identity (for example, by sending the request through a private account with individualised login details), the controller must respond to such a request without overburdening the data subject with additional formalities. Failure to do so could expose the controller to an administrative fine.¹⁰⁵¹

A second important point in this respect is that data subjects can exercise their rights without having to provide any justification, and without having to be knowledgeable about the applicable law. For example, a data subject can request the erasure of their personal data without having to explain the reason behind that request, and without having to justify it from a legal point of view. It will never be required from data subjects, for example, to use legal jargon or to refer to the applicable GDPR article in which their right is enshrined. If, on the other side, the controller decides to turn down the data subject’s request, it must explain the reason why, including any legal reason, as the case may be.¹⁰⁵² From the perspective of the FRO of the GDPR, this can be considered as an important factor of functionality, in the sense that data subjects can subjectively activate any of their data protection right without having to provide any *prima facie* evidence of an interference with their interests, rights or freedoms. For example, if a data subject suspects that a processing activity, which is based on their consent, could produce discriminatory effects on them, they could alert the controller of their wish to withdraw their consent to the processing, while in parallel submitting an erasure request, without however having to explain their motive. In other words, the existence of an infringement or of a violation is not a prerequisite for data subjects to be able to exercise their rights under the GDPR.

Third, regarding the means of communication between the data subject and the controller, Article 12(3) GDPR, last sentence, provides that where a data subject submits a request by electronic means, the answer from the controller should also be given by electronic means, unless otherwise requested by the data subject.

¹⁰⁴⁸ Article 12(2) GDPR.

¹⁰⁴⁹ Article 12(6) GDPR.

¹⁰⁵⁰ Article 12(2) GDPR.

¹⁰⁵¹ Article 83(5)(b) GDPR.

¹⁰⁵² This derives from the principle of accountability enshrined in Article 5(2) GDPR, as well as Article 12(4) GDPR, which provides: “*If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.*”

Although this provision may appear to contain a mere technical detail, it guarantees the promptness of the communication between the data subject and the controller, which in turn increases the convenience and ease with which data subjects can exercise their rights. This provision can therefore be considered as a factor of functionality of the GDPR for data subjects seeking to assert their rights and freedoms under that framework.

Fourth, Article 12(3) GDPR states that controllers must provide data subjects with information on the action that they will take “*without undue delay*” and in any event “*within one month of receipt of the request*”. If the request is particularly complex or important in scope, the controller is allowed to extend that period by two further months but must inform the data subject of this delay within one month of receipt of the request, together with the reasons for such a delay.¹⁰⁵³ Controllers can therefore not ignore requests from data subjects or postpone their action indefinitely. Controllers may of course decide to reject the data subject’s request if they consider that it is not founded, without merits, or if they believe that their own rights and interests prevail over the one of the data subjects.¹⁰⁵⁴ Yet, they will need to answer the request, which should normally compel them to at least assess the lawfulness of the processing. The one-month deadline inscribed in Article 12(3) GDPR thus increases the functionality of the GDPR by forcing a reaction on the part of the controller – even if it leads to the rejection of the request, and the potential intervention of a DPA, as discussed here below.

Fifth, in the event the controller is of the opinion that it cannot respond positively to the data subject’s request – for example, because it considers that it has a valid ground to refuse the objection, rectification or erasure request of the data subject – the controller must inform the data subject without delay, and at the latest within one month of receipt of the request, of the reasons for not taking action, and also on the possibility of lodging a complaint with a DPA.¹⁰⁵⁵ Data subjects may thus contest the decision of the controller by involving a DPA, without having to seek the advice of a legal professional on the question beforehand.¹⁰⁵⁶ The important role of DPAs in enforcing the rights of data subjects will further be discussed in the next Chapter of this study. At this stage, it is already worth noting that the mandatory mention of the possibility for data subjects to lodge a complaint with a DPA in the event of a negative answer from the controller can act as a supplementary safeguard for the rights of data subjects. Indeed, this mandatory mention guarantees that data subjects are properly informed about the possibility to pursue their claim through the intervention of a DPA, without having to put important additional personal efforts into it. This can be seen as another factor of functionality of the GDPR, given

¹⁰⁵³ Article 12(3) GDPR, second and third sentence.

¹⁰⁵⁴ Unless the request concerns an objection to the processing of personal data for marketing purpose, in which case the controller must always grant it, as discussed above.

¹⁰⁵⁵ Article 12(4) GDPR.

¹⁰⁵⁶ Article 12(4) GDPR.

that investing additional time or money could otherwise deter many individuals from pursuing their claim against the concerned controller.

Last, but not least, Article 12(5) GDPR provides that all communications and any actions taken under Articles 15 to 22 and 34 must be provided “*free of charge*”. As a general rule, data subjects can thus exercise their right to information, access, rectification, erasure, objection, or even their right to a human intervention in the event of an AIDM, without being charged for the associated services. This also increases the functionality of the framework since it allows data subjects to exercise their rights whenever they see fit, without being deterred by the cost this could imply for them. It is only when requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, that the controller may either charge “*a reasonable fee*”, or refuse to act on the request.¹⁰⁵⁷ This provision therefore strikes a balance between the need to guarantee the functionality of data subjects’ rights on the one side, and the economic interests of controllers on the other side, by protecting the latter from abuses of rights.

3.2.4. Concluding remark: the synergies between the PRO-triptych as a horizontal factor of the functionality of the GDPR

In the opinion of the author, the resonance between the principles, rights and obligations set out in the GDPR participate to the overall functionality of EU data protection law. If considered separately, each provision of the GDPR may appear insufficient to effectively protect data subjects against the negative effects of data processing practices on their fundamental rights and freedoms. Yet, one combined together, they can form convenient tools to achieve that end.

Hence, although data subjects’ rights are not absolute, they undeniably complement and reinforce the key-principles of data processing enshrined in Article 5 of the GDPR, as well as the set of obligations incumbent on controllers and processors.¹⁰⁵⁸ For example, the storage limitation principle (Article 5(1)(e) GDPR), as well as the duty to inform data subjects about the period for which the personal data will be stored (Article 13(2)(a) GDPR), is backed up by the rights of the data subject to request further information on the storage period of the personal data, and request their erasure if the data subject considers that they are no longer necessary for the purposes for which they were collected in the first place (Article 15 and 17 GDPR). The combination of this principle and right, combined with the obligation of controller to promptly answer data subject’s request, can be used as a multi-functional tool to achieve another purpose, i.e., put an end to a data processing practice that is negatively impacting the rights and freedoms of the data subject.

¹⁰⁵⁷ Article 12(5)(a) or (b) GDPR.

¹⁰⁵⁸ Limitations to those rights are highlighted in multiple articles of the GDPR. Those limitations derive from many well-known legal concepts such as the prohibition of abuse of rights, as well as the necessity to consider the rights and interests of others to achieve a fair balance.

As a concrete illustration of the synergies of the PRO-triptych, one may refer to the *Google Spain* case, where the data subject – Mr Mario Costeja Gonzales – ultimately obtained the erasure of his personal data from the search engine of the Google group ('Google Search'). The dispute that led to this preliminary ruling found its origin in the fact that, when an internet user would enter Mr Costeja González's name in Google Search, two results would redirect the user to an old newspaper article dating from 1998, mentioning that Mr Costeja González's real estate had been auctioned to reimburse his social security debts.¹⁰⁵⁹ Mr Costeja González kept on suffering from this bad publicity in his professional relations even if it was no longer representative of his situation in 2010, i.e., twelve years after he had reimbursed his debts to society. He had therefore filed a complaint with the Spanish DPA against Google, after the latter had failed to respond to his request for erasure. By ultimately obtaining the erasure of his data, Mr Costeja González did not only put an end to a disproportionate interference with his right to privacy, but also his right to personal data protection, and his right not to be discriminated on the basis of (outdated) information relating to his past financial situation. It must be pointed out, however, that it took Mr González almost a decade to gain back control over his personal data. Furthermore, it may come as an irony that Mr González's name and past financial issues became public knowledge because of the prominence gained by this judgment. One could therefore argue that this case is reflective of the dysfunctionality of EU data protection law rather than of its functionality. Two facts must however be considered in this respect: first, the questions submitted to the CJEU in the *Google Spain* case did not concern the interpretation of the GDPR but of the 1995 Data Protection Directive. Since then, the right to erasure has been explicitly enshrined in Article 17 GDPR; no data subject will thus need to go through the same steps or unwanted notoriety to have their data removed. Second, the CJEU has since then amended its rules of procedure and practices, so as to anonymise the name of the parties in any dispute which gives rise to a preliminary reference, where such anonymity is justified on grounds of privacy or data protection.¹⁰⁶⁰ Hence, although it could be argued that EU law used to be dysfunctional before 2014 as far as the exercise of the right to erasure was concerned, these flaws have since then been largely corrected for the benefit of data subject's right to informational self-determination, as well as any DFR that a data subject may seek to enforce through their erasure request.

Combining different provisions of the PRO-triptych might further contribute to the unwinding of additional rights or obligations, and thus enhance the overall protection of data subjects. As an illustration, one may refer to the principle of

¹⁰⁵⁹ CJEU, Judgment of 13 May 2014, *Google Spain*, Case C-131/12, para. 14.

¹⁰⁶⁰ Articles 95 and 190(3) of the Rules of Procedure of the Court of Justice CJEU of 25 September 2012 (OJ L 265, 29.9.2012), as amended on 18 June 2013 (OJ L 173, 26.6.2013, p. 65), on 19 July 2016 (OJ L 217, 12.8.2016, p. 69), on 9 April 2019 (OJ L 111, 25.4.2019, p. 73) and on 26 November 2019 (OJ L 316, 6.12.2019, p. 103). See also this publication by the CJEU: The protection of personal data in connection with publications relating to judicial proceedings before the Court of Justice, November 2015, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-11/tra-doc-en-div-c-0000-2015-201508723-05_00.pdf.

storage limitation, enshrined in Article 5(1)(e) of the GDPR. This principle prescribes that personal data should not be stored in a form which permits identification of data subjects for longer than what is necessary for the purposes of the processing. If this principle had to be applied alone, it would be difficult to extract from it an obligation for controllers to establish strict data deletion policies. In parallel, however, Article 32 GDPR obliges controllers to adopt technical and organisational measures to ensure the security of processing under Article 32 GDPR. Also, under Article 13(2)(a) and 15, data subjects have the right to be informed about the period during which their personal data will be kept by the concerned controller. Article 12(3) GDPR further specifies that controllers have one month to answer such information request. Once read these different provisions are read together, it quickly appears that, in practice, controllers have no choice but to establish clear internal archiving, deletion or data retention policies, and to constantly monitor the addition and deletion of personal data from their system, also as a way to respect the principle of accountability. Although these duties are not specifically mentioned within the GDPR, they can nonetheless be considered as the indirect consequences of the combination of this storage limitation principle, information right and security obligation.

The case *Google Spain* also illustrates the additional rights that can be derived from the synergies between the different panels of the PRO triptych; before 2014, indeed, the ‘right to be forgotten’ on grounds of informational self-determination did not explicitly exist under EU data protection law. Rather, data subjects only had the right to ask for the erasure of their data under Article 12(b) if these data were ‘*incorrect*’ or ‘*incomplete*’.¹⁰⁶¹ The CJEU, however, took the view that Article 12(b) of the 1995 Data Protection Directive, read in combination with Article 6(1)(c) and (e) of the same Directive (i.e., the principle of data minimisation and storage limitation), as well as Article 7 and 8 of the Charter, should be interpreted as meaning that individuals have a right to request the erasure of their information from the results of search engines, and that, as a rule, such a right overrides not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information when the search is made on the basis of the data subject’s name.¹⁰⁶² This general rule can be tempered by specific circumstances. If, for example, Mr Gonzales would have been an important political figure, it could have been justified to allow Google to still reference these results, given the importance for the public to have access to information relating to political representatives.¹⁰⁶³ Regardless of the facts of that case, however, what remains particularly noteworthy for answering the research question of this study is that the combination of a (still limited) right to erasure with the principle of data minimisation and storage limitation, allowed the CJEU to recognise a broader ‘right

¹⁰⁶¹ Article 12(1)(c) of the 1995 Data Protection Directive.

¹⁰⁶² CJEU, *Google Spain*, para. 99.

¹⁰⁶³ The CJEU more generally refer to “*the role played by the data subject in public life*” as a factor to take into account when assessing whether the erasure is justified or not. See CJEU, *Google Spain*, para. 81 and 97.

to be forgotten’, and in particular the right of data subjects to have their data erased from the results of online search engines, even if these data are factually correct or complete. This case thus illustrates how synergies among the different panels of the PRO-triptych can play a functional role in the fulfilment of the FRO of the GDPR.

The order in which each of the panels of the PRO-triptych have been explored is not coincidental. In the opinion of the author indeed, the legal narrative which emanates from the GDPR starts with the key-principles of processing – which set the scene, and provide an horizontal red line which runs across the two other panels – ; then with the obligations of controllers – who are given a script, and are told *what to do* to be compliant through a myriad of more specific provisions; and finally, the rights of data subjects – who can be considered as the last bastion for compliance, armed with the necessary tools to repel unfair data processing practices. At the end of the sequence, in the event of a distortion or a violation, DPAs may also become involved to restore the narrative of the GDPR, and in particular its objective to protect the rights and freedoms of data subjects in the context of data processing (see Chapter 3.3 below, “*The Third Pillar of Functionality of the GDPR: Supervision and Sanction within a Decentralised Multi-actor System*”).

This triptych of general principles, specific obligations, and activable rights constitute the substance of EU data protection law. How they are applied and interact with each other in the online and offline world, and whether they truly participate to the functionality of EU data protection law when it comes to combat the harmful effects of modern data processing practices on DFR, will further be assessed in the subsequent Chapter of this study. While some elements of this triptych appear to participate to the effectiveness and functionality of EU data protection law, others may indeed suffer from shortages and weaknesses when confronted to modern DDTs. Before exploring the two ‘test areas’ selected for this study however, a third important pillar of the GDPR must still be discussed: its supervision and sanctions system.

3.3. THE THIRD PILLAR OF THE FUNCTIONALITY OF THE GDPR: SUPERVISION AND SANCTION WITHIN A MULTI-ACTOR DECENTRALISED SYSTEM

Sections 3.1 and 3.2 of this study have shown how the scope and substance of the GDPR contribute to the multi-functionality of this legal framework with respect to its FRO. As far as the scope of the GDPR is concerned, it has been shown in particular that the broadness and flexibility of the notions of ‘personal data’ and ‘processing’ allow for the application of the GDPR to almost any type of situations where processing operations could harm the rights and freedoms of data subjects, including DFR. As far as the substance of the GDPR is concerned, it has been shown that the set of principles, rights and obligations laid down in the GDPR, and the synergies that they create, offer a convenient toolbox for preventing or putting an end to processing practices that could harm the fundamental rights and freedoms of data

subjects, without being restricted to concerns over the right to privacy or personal data protection only. Yet, these two pillars of multi-functionality could eventually crumble down under the weight of the overall framework if they were not backed up by a third important pillar: a system of supervision and sanctions.

Supervision and sanction mechanisms fall together under the broader term of 'enforcement'. In the event a controller or a processor does not comply with EU data protection rules, enforcement is what transforms data subjects' rights from theory to practice. In other words, the possibility of enforcing one's rights is central to making these rights a reality.¹⁰⁶⁴ This is also true for EU data protection law and fundamental rights law.

In general, the optimal or sub-optimal nature of enforcement is appreciated from the perspective of *effectiveness*. Indeed, it has already been highlighted in the first Chapter of this study that the effectiveness of any imperative norm is, to a large extent, dependent on enforcement mechanisms (see above, Section 1.1.2). An imperative law deprived from any sort of supervision or sanction mechanism would be like a lion without claws or teeth; alive, but quite harmless and bound to die, eventually. The effectiveness of the GDPR in terms of enforcement is however not the central focus of this study; dwelling on this point or analysing every aspect of it would thus go beyond the scope of the research question under investigation. Yet, since effectiveness and functionality are closely interlinked, it is still relevant to provide an overview of the changes brought by the GDPR that have contributed to the effective enforcement of EU data protection law, and of the main issues that still exist in this respect. As summarized by Wojciech Wiewiórowski, current head of the EDPS, "*[alt]hough enforcement is only a tool for accomplishing this primary objective of the GDPR, the mechanism and means through which it is achieved remain prominently relevant. And what the last four years have shown is that where enforcement lacks, so does an individual's ability to have their rights realized.*"¹⁰⁶⁵

After briefly discussing the GDPR enforcement system from the perspective of its general (*in*)*effectiveness* (Section 3.3.1, below), the author of this study will more specifically focus on the role of each actor within the enforcement system of the GDPR and identify the main factors that seem to contribute or, on the contrary, impede the *functionality* of the GDPR with respect to the fulfilment of its FRO (Section 3.3.2, below).

3.3.1. The effective enforcement of the GDPR: between improvements and disillusionment

¹⁰⁶⁴ European Union Agency for Fundamental Rights (2011). *Report: Access to Justice in Europe: an overview of challenge and opportunities*. https://fra.europa.eu/sites/default/files/fra_uploads/1520-report-access-to-justice_EN.pdf.

¹⁰⁶⁵ Opinion of Wojciech Wiewiórowski, director of the EDPS. Source: Wiewiórowski, W. (2022, June 9). We still need to talk about data protection. *Politico*. <https://www.politico.eu/article/eu-data-protection-gdpr-brussels-regulation-supervision/>.

By broadening the investigative and corrective powers of DPAs, and drastically increasing the fines that can be levied on infringers, the GDPR has undeniably boosted the effective enforcement of data protection rules for the benefit of data subject's rights and freedoms. Section 3.3.1.1 below will highlight these general improvements. Yet, many practical or procedural issues still exist, especially in the context of cross-border enforcement. This has led to a sub-optimal enforcement of the GDPR in practice, and a certain disillusionment among defenders of privacy. Some scholars have even put forward the question whether the GDPR would not be, to some extent, "*deficient by design*" with respect to enforcement,¹⁰⁶⁶ as briefly discussed in Section 3.3.1.2 below.

3.3.1.1. Improvements in enforcement: the impact of the broadening of the investigative and corrective powers of DPAs

Two facets of enforcement can be distinguished in the text of the GDPR: (i) enforcement through supervision mechanisms and (ii) enforcement through corrective measures, including sanctions. While supervision mechanisms allow to detect violations, corrective measures can be imposed to put an end to these violations, punish the infringer, and deter the latter, as well as others, from violating the norm (again).¹⁰⁶⁷ Because the GDPR contains many imperative provisions taking the form of obligations imposed on controllers and processors, it was crucial to accompany these norms with a solid enforcement framework to ensure their effectiveness.

Prior to the adoption of the GDPR, the 1995 Data Protection Directive already put in place some timid supervision and sanction mechanisms.¹⁰⁶⁸ Full discretion was however left to Member States with respect to the investigative and corrective powers of DPAs. And as far as sanctions were concerned, the 1995 Data Protection Directive merely stated that Member States had to adopt "*suitable measures*" to ensure the implementation of data protection law, including by laying down sanctions, the nature or importance of which was neither defined nor even generally outlined by the Directive.¹⁰⁶⁹ This led to the adoption of a fragmented and rather weak enforcement system across the EU, which damaged both the uniformity of EU data protection law and the credibility of DPAs.¹⁰⁷⁰ As a consequence, DPAs were usually regarded as toothless watchdogs¹⁰⁷¹ that one could simply ignore – if one

¹⁰⁶⁶ Gentile, G. & Lynskey, O. (2022). Deficient by design. The transnational enforcement of the GDPR. *International and Comparative Law Quarterly*, 71(4):799-830.

¹⁰⁶⁷ Le Fur, L. (1935), Les caractères essentiels du droit en comparaison avec les autres règles de la vie sociale. *Archives de philosophie du droit*, p. 7 ; in the area of criminal law, see in particular Foucault, M. (1989). *op. cit.*

¹⁰⁶⁸ Including the cumbersome (and pointless) obligation for controllers and processors to notify their DPA of their data processing activities, as provided in Articles 18 and 21 of the 1995 Data Protection Directive. This obligation was abandoned with the adoption of the GDPR.

¹⁰⁶⁹ Article 24 of the 1995 Data Protection Directive.

¹⁰⁷⁰ Giurgiu, A., & Larsen, T. A. (2016). Roles and powers of national data protection authorities. *European Data Protection Law Review*, 2(3), pp. 342-352.

¹⁰⁷¹ Casey, B. & al. (2019), *op. cit.*, p. 150.

was even aware of their existence.¹⁰⁷² Since the adoption of the GDPR, both the tasks and powers of DPAs have been widely expanded, thereby boosting the effectiveness of the overall framework, as further outlined below.

Article 51(1) GDPR provides that each Member State must establish one or more independent public authorities to be responsible for monitoring the application of the GDPR, in order to “*protect the fundamental rights and freedoms of natural persons in relation to processing*” and to “*facilitate the free flow of personal data within the [EU]*”. Seeking the fulfilment of both the FRO and IMO of EU data protection law is thus the main task conferred upon DPAs. This task has been further translated into multiple sub-tasks listed in Article 57 GDPR. Beyond monitoring and enforcing the GDPR, DPAs are required to, among others: “*promote public awareness and understanding*” of the risks, rules and rights attached to processing, especially as far as it concerns children;¹⁰⁷³ “*advise the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms (...)*”;¹⁰⁷⁴ handle complaints lodged by data subjects or associations representing their interests by taking the necessary steps to investigate the subject-matter of the complaint and informing the complainant of both the progress and outcome of the complaint “*within a reasonable period*”¹⁰⁷⁵ ; encourage or approve the drafting of various certification schemes, codes of conduct, or transfer mechanisms in line with the GDPR;¹⁰⁷⁶ contribute to the activities of the EDPB;¹⁰⁷⁷ and, more generally, “*fulfil any other tasks related to the protection of personal data.*”¹⁰⁷⁸

It clearly appears from these provisions that the tasks of DPAs are in no way limited in a way that could be detrimental to the fulfilment of the FRO of EU data protection law; quite the opposite. These tasks are indeed listed in a non-exhaustive way, thereby enabling DPAs to flexibly envisage their actions to monitor and enforce the dual IMO and FRO of EU data protection law. In practice, most of the working time of DPAs is dedicated to handling complaints, either alone or in cooperation with other DPAs.¹⁰⁷⁹

Another important element attached to the role of DPAs which contributes to the effective enforcement of EU data protection law is their independence. Such independence is not only regulated under Article 51 to 54 GDPR but is also enshrined in Article 8(3) of the Charter and Article 16(2) of the TFEU. The CJEU has further safeguarded and specified the required level of independence of DPAs on multiple

¹⁰⁷² When the author of this study was working as an attorney in data protection law, many of her clients admitted that they had no idea DPAs even existed prior to the GDPR.

¹⁰⁷³ Article 57(1)(b) GDPR.

¹⁰⁷⁴ Article 57(1)(c) GDPR.

¹⁰⁷⁵ Article 57(1)(f) GDPR.

¹⁰⁷⁶ Article 57(1)(j), (m), (n), (p), (q), (r) and (s) GDPR.

¹⁰⁷⁷ Article 57(1)(t) GDPR.

¹⁰⁷⁸ Article 57(1)(v) GDPR.

¹⁰⁷⁹ Article 77(2) GDPR.

occasions.¹⁰⁸⁰ As far as the effectiveness of EU data protection law is concerned, this means in particular that each national DPA (i) must remain free from any direct or indirect influence from both the public sector (such as a national governments) or the private sector (such as lobbyists or any powerful private company), (ii) can neither seek nor take instructions from anybody,¹⁰⁸¹ and (iii) must be granted sufficient human, technical and financial resources, as well as the premises and infrastructure necessary for the effective performance of their tasks and powers.¹⁰⁸²

Since the adoption of the GDPR, DPAs were also granted additional investigative powers, including the power to carry out investigations in the form of data protection audits or of ‘daw raids’, with access to the premises of controllers or processors as well as their IT equipment.¹⁰⁸³ As an illustration, in 2020, the CNIL carried out 247 investigations into potentially unlawful data processing practices, including through information requests, analysis of data processing records and data protection audits.¹⁰⁸⁴ Similarly, between 2020 and 2021, the CNPD conducted 25 investigations in the context of a thematic campaign on the role and function of DPOs, targeting both the private and public sector. Many of these investigations enabled the CNPD to establish several shortcomings on the part of the responsible controllers.¹⁰⁸⁵ Beyond these investigative powers, DPAs were also granted additional corrective powers, such as the power to ban a processing activity, or to force a controller to bring processing into compliance through the adoption of specific measures. It is generally admitted that the coercive function of DPAs lies within the exercise of their corrective powers.¹⁰⁸⁶ Yet, granting DPAs a combination of both investigative and corrective powers was essential to allow them to act as the true guardians of the rights of individuals – both preventively and remedially.

For the sake of completeness, an overview of the investigative and corrective powers of DPA is provided in the table below.

TABLE 7

This table provides an overview and description of the powers of DPAs as listed under Article 58 of the GDPR. While the investigative powers of DPAs are highlighted in blue, their corrective powers are highlighted in orange.

¹⁰⁸⁰ For the CJEU case-law on the independence of DPAs, see in particular: Case C-51 8/07 European Commission v Federal Republic of Germany [2010] ECLI:EU:C:2010:125; Case C- 614/10 European Commission v Republic of Austria [2012] ECLI:EU:C:2012:631; Case C-288/12 Commission v Hungary [2014] ECLI:EU:C:2014:237; but also Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650

¹⁰⁸¹ Article 52(2) GDPR.

¹⁰⁸² Article 52(4) GDPR.

¹⁰⁸³ Article 58(1)(f) GDPR.

¹⁰⁸⁴ CNIL 2021 Activity report. The CNIL in a nutshell 2021. https://www.cnil.fr/sites/default/files/atoms/files/the_cnil_in_a_nutshell_2021.pdf.

¹⁰⁸⁵ D’Ath F. (2021). XXX

¹⁰⁸⁶ Giurgiu, A., & Larsen, T. A. (2016). Roles and powers of national data protection authorities. European Data Protection Law Review (EDPL), 2(3), p. 338.

Investigative powers	1.	DPAs may order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks.	Article 58(1)(a) GDPR.
	2.	DPAs may carry out investigations in the form of data protection audits.	Article 58(1)(b) GDPR.
	3.	DPAs may carry out a review on data protection certification mechanisms and on data protection seals and marks, which can be established and issued to a controller or processor for the purpose of demonstrating compliance with the GDPR. ¹⁰⁸⁷	Article 58(1)(c) GDPR.
	4.	DPAs may notify the controller or the processor of an alleged infringement of this Regulation.	Article 58(1)(d) GDPR.
	5.	DPAs may obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks.	Article 58(1)(e) GDPR.
	6.	DPAs may obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	Article 58(1)(f) GDPR.
Corrective powers	1.	DPAs may issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation.	Article 58(2)(a) GDPR.
	2.	DPAs may issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation.	Article 58(2)(b) GDPR.
	3.	DPAs may order the controller or the processor to comply with the requests of data subjects exercising their rights pursuant to this Regulation.	Article 58(2)(c) GDPR.
	4.	DPAs may order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period.	Article 58(2)(d) GDPR.

¹⁰⁸⁷ Article 47 GDPR provides that Member States, the supervisory authorities, the EDPB and the Commission shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks by recognised certification bodies, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.

	5.	DPA's may order the controller to communicate a personal data breach to the data subject.	Article 58(2)(e) GDPR.
	6.	DPA's may impose a temporary or definitive limitation including a ban on processing .	Article 58(2)(f) GDPR.
	7.	DPA's may order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed.	Article 58(2)(g) GDPR.
	8.	DPA's may withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met.	Article 58(2)(h) GDPR.
	9.	DPA's may impose an administrative fine pursuant to Article 83, in addition to, or instead of any other corrective measures.	Article 58(2)(i) GDPR.
	10.	DPA's may order the suspension of data flows to a recipient in a third country or to an international organisation.	Article 58(2)(j) GDPR.

Finally, it cannot be denied that the significant administrative fines that DPAs can now impose on controllers and processors, as set in Article 83 GDPR, have sent a shockwave throughout the EU and beyond. Depending on the violation, such fines may go up to 20 million EUR or 4% of the total worldwide annual turnover of an undertaking.¹⁰⁸⁸ This, of course, led many companies to put “*compliance with the GDPR as one of their key tasks on management level*”.¹⁰⁸⁹

Article 83 GDPR is regularly being actioned by DPAs. Within the first three years of application of the GDPR indeed, DPAs have levied more than 1050 fines for a total of more than €1,610,296,046 EUR,¹⁰⁹⁰ including a single fine of EUR 746,000,000 imposed on Amazon Europe by the CNPD.¹⁰⁹¹ In order to render these numbers more

¹⁰⁸⁸ The numbers of the financial year *preceding* the year of the actual breach are used for that purpose (Article 83(4) and (5) of the GDPR).

¹⁰⁸⁹ Albrecht, J. P. (2016). How the GDPR will change the world. *European Data Protection Law Review*, 3, p. 288.

¹⁰⁹⁰ For an updated overview, please consult <https://www.enforcementtracker.com/?insights>.
















¹⁰⁹¹ The CNPD has so far refused to publish or communicate the decision whereby they imposed that fine, but the amount has been revealed in the annual audit report of the Amazon Group and in the appeal procedure initiated by Amazon before the Administrative Tribunal of Luxembourg.

concrete and vivid, the below table provides an overview of the twenty highest fines inflicted by DPAs until today.¹⁰⁹²

¹⁰⁹² This table has been last updated on October 1st, 2022.

TABLE 8

This table provides an overview of the 20 most important fines imposed on a controller or processor by a DPA for violating the GDPR. While some of the actual decisions behind these fines have not been made available to the public by the concerned DPA, the below information has been collected from various sources by the firm CMS (<https://www.enforcementtracker.com/>). The table shows respectively the concerned jurisdiction, the date of the decision, the amount of the fine, the identity of the controller/processor, the GDPR articles which have been violated, the nature of the main infringement and the source from which this information has been gathered.

	Jurisdiction / DPA	Date	Fine (€)	Controller	GDPR articles	Nature of the main infringement	Source
1.	 LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Article 5 GDPR (other articles unknown)	Non-compliance with general data processing principles	US Securities & Exchange Commission link
2.	 IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	Art. 5(1), 6(1), 12(1), 24, 25 and 35 GDPR.	Non-compliance with general data processing principles	EDPB link
3.	 IRELAND	2021-09-02	225,000,000	WhatsApp Ireland, Ltd.	Art. 5(1)(a) and 12-14 GDPR.	Insufficient fulfilment of information obligations	EDPB link
4.	 FRANCE	2021-12-31	90,000,000	Google LLC	Art. 82 loi Informatique et Libertés (Art. 6 GDPR)	Insufficient legal basis for the processing	CNIL link
5.	 FRANCE	2021-12-31	60,000,000	Facebook Ireland, Ltd.	Art. 82 loi Informatique et Libertés (Art. 6 GDPR)	Insufficient legal basis for data processing	CNIL link
6.	 FRANCE	2021-12-31	60,000,000	Google Ireland, Ltd.	Art. 82 loi Informatique et Libertés (Art. 6 GDPR)	Insufficient legal basis for data processing	CNIL link
7.	 FRANCE	2019-01-21	50,000,000	Google LLC	Art. 5, 6, 13 and 14 GDPR	Insufficient legal basis for data processing; insufficient information.	CNIL link
8.	 GERMANY	2020-10-01	35,258,708	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Art. 5 and 6 GDPR	Insufficient legal basis for data processing	Hamburg DPA link
9.	 ITALY	2020-01-15	27,800,000	TIM (telecommunications operator)	Art. 5, 6, 17, 21 and 32 GDPR	Insufficient legal basis for data processing	Garante link
10.	 ITALY	2021-12-16	26,500,000	Enel Energia S.p.A	Art. 5 (1)(a) and (d), 5 (2), 6(1), 12-13, 21, 24, 25(1), 30 and 31 GDPR	Insufficient legal basis for data processing	Garante link
11.	 UNITED KINGDOM	2020-10-16	22,046,000	British Airways	Art. 5(1)(f) and 32 GDPR	Insufficient technical and organisational measures to ensure information security	ICO annual report 2020 Link
12.	 UNITED KINGDOM	2020-10-30	20,450,000	Marriott International, Inc	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	ICO link
13.	 GREECE	2022-07-13	20,000,000	Clearview AI Inc.	Art. 5 (1) (a), 6, 9, 12, 14-15 and 27 GDPR.	Non-compliance with general data processing principles	Greek DPA link
14.	 ITALY	2022-02-10	20,000,000	Clearview AI Inc.	Art. 5 (1) (a), (b), (e), 6, 9, 12-15, and 27 GDPR	Non-compliance with general data processing principles	Garante link
15.	 IRELAND	2022-03-15	17,000,000	Meta Platforms Ireland Limited	Art. 5(2) and 24(1) GDPR.	Insufficient technical and organisational measures to ensure	DPC link

The investigative and corrective powers of DPAs, as well as their ability to inflict significant administrative fines, have undoubtedly led EU data protection law to evolve from an overlooked or neglected area of law to an important boardroom topic, as well as a matter of interest among the general public.¹⁰⁹³ Yet, despite these noticeable improvements, enforcement can still remain a challenge for data subjects. The last four years have indeed shown that the rules existing on paper are sometimes difficult to enforce in practice, especially in the context of cross-border cases where multiple DPAs have to cooperate.¹⁰⁹⁴ As an illustration, among the 51 individual complaints that the Austrian privacy organisation *noyb* filed between May 2018 and January 2022, only 15% led to the adoption of a binding decision by a competent DPA or court, while *no* decision at all was rendered in any cross-border cases.¹⁰⁹⁵ The below section will briefly discuss the general causes behind this low enforcement rate, and point out to the fact that most issues relating to enforcement seem to find their source in factors that are external to the text of the GDPR itself.

3.3.1.2. Disillusionment: general organisational and procedural issues impeding the effective enforcement of the GDPR

Following the adoption of the GDPR in May 2016, there has been a noticeable surge in the activities of DPAs. Overall, this has led to more enforcement, most of the time for the benefit of data subjects' rights. Yet, scholars, practitioners or the concerned authorities themselves have also identified a long list of issues with respect to enforcement. Among these issues, one may refer to the insufficient budget allocated to DPAs, the difficulty in finding staff with expert knowledge or more generally the poor organisation, communication and cooperation practices of DPAs.¹⁰⁹⁶ As a result, the GDPR still suffers from "*a sub-optimal enforcement leading to a disconnect between the law on the books and its impact in practice*".¹⁰⁹⁷

¹⁰⁹³ Google search traffic peaked to an all-time high for terms such as "privacy" or "data protection" in the month preceding and after the application date of the GDPR on 25 May 2018. Source: Google trends.

¹⁰⁹⁴ See, inter alia, Balboni, P., Taborda Barata, M., Botsi, A. & Francis, K. (2019). Accountability and Enforcement Aspects of the EU General Data Protection Regulation: Methodology for the Creation of an Effective Compliance Framework and a Review of Recent Case Law. *The Indian Journal of Law and Technology*, 15(1): 103-254; *noyb* (2022, January 23). Data Protection Day: 41 Years of "Compliance on Paper"? <https://noyb.eu/en/data-protection-day-41-years-compliance-paper>.

¹⁰⁹⁵ Ibid.

¹⁰⁹⁶ Gentile, G. & Lynskey, O. (2022). *op. cit.*, p. 799. Heinrich Böll Stiftung (2021, December 30). Trends in Privacy Enforcement: A Comparative Analysis of post-GDPR Enforcement Styles. <https://tr.boell.org/en/2021/12/30/trends-privacy-enforcement-comparative-analysis-post-gdpr-enforcement-styles>; Access Now (2021). Three years under the GDPR. An implementation progress report. Available at <https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf>; Heine, I. (2021, September 13). 3 Years Later: An Analysis of GDPR Enforcement. *CSIS*. <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement>; Jeenes, R. & al. (2021, 22 November). Divergence, Convergence and Challenges: Trends on GDPR Enforcement Across Europe and the UK. *Slaughter & May*. <https://my.slaughterandmay.com/insights/briefings/divergence-convergence-and-challenges-trends-on-gdpr-enforcement-across-europe-and-the-uk>.

¹⁰⁹⁷ Gentile, G. & Lynskey, O. (2022). *op. cit.*, p. 799; Balboni, P., Taborda Barata, M., Botsi, A. & Francis, K. (2019), *op. cit.*

It cannot be denied, indeed, that DPAs are currently struggling to handle complaints lodged by data subjects while also investigating GDPR breaches of their own volition in an effective and efficient manner. In some jurisdictions, the situation appears worse than in others. As an illustration, in Ireland, while more than 10,000 complaints were filed with the Irish Data Protection Commissioner (the ‘DPC’) in 2020, less than 1% of these complaints led to the adoption of a formal decision within a year.¹⁰⁹⁸ This means that even when a data subject lodges a relatively ‘simple’ complaint with the DPC (for example, because of the absence of response of an Irish controller following an access request), it can take more than a year for the DPC to issue a binding decision and for the individual concerned to finally get the requested data. Although the poor enforcement practice of the DPC may not be representative of the work of DPAs across the EU (many of which have a much better enforcement rate), it shows that the level of effective enforcement of the GDPR may greatly vary from one Member State to another, depending *inter alia* on political, procedural or cultural specificities.¹⁰⁹⁹

These enforcement issues seem further aggravated in the context of the one-stop mechanism, where a lead DPA is designated and must collaborate with other DPAs on files involving cross-border processing of personal data.¹¹⁰⁰ The use of inadequate communications tools, the incompatibility of national procedures, and divergences of opinions on the measures which should be taken (such as a deeper investigation or a higher fine) are examples of procedural hurdles that arise when multiple DPAs must cooperate, thereby sometimes rendering the procedure extremely difficult, lengthy and thus less effective.¹¹⁰¹ On top of that, many big tech companies, such as Google, Meta, Twitter, WhatsApp or Microsoft, have their main establishment in Ireland, thereby making of the DPC the lead DPA in a significant number of cases impacting the rights of individuals across the EU. Given that the DPC is also one of the least performing DPA in the EU, many high-profile cases get stuck when reaching the Irish regulator. To illustrate this issue, it suffices to mention that, between 2018 and May 2021, the DPC had only rendered four final decisions despite having been designated as the lead DPA in two-hundreds cross-border cases.¹¹⁰²

In a recent article, Giulia Gentile and Orla Lynskey have endeavoured to identify whether the sub-optimal enforcement of the GDPR could be explained by the fact

¹⁰⁹⁸ noyb (2021, April 28). Irish DPC ‘handles’ 99,93% of complaints, without decision? <https://noyb.eu/en/irish-dpc-handles-9993-gdpr-complaints-without-decision>.

¹⁰⁹⁹ Gentile, G. & Lynskey, O. (2022). *op. cit.*

¹¹⁰⁰ Articles 60 to 67 GDPR.

¹¹⁰¹ For example, Johannes Caspar, after leading the Hamburg DPA for 12 years, stepped down after expressing frustration with the “one-stop shop” mechanism, calling it “broken”. Source: Ikeada, S. (2021, July 1). Outgoing Privacy Commissioner Calls GDPR “Broken,” Says That Basic Model “Can’t Work”. *CPO Magazine*. <https://www.cpomagazine.com/data-protection/outgoing-privacy-commissioner-calls-gdpr-broken-says-that-basic-model-cant-work/>.

¹¹⁰² Scally, D. (2021, March 17). Irish data regulator sparks row with EU colleagues on Facebook oversight. *The Irish Times*. <https://www.irishtimes.com/business/economy/irish-data-regulator-sparks-row-with-eu-colleagues-on-facebook-oversight-1.4513065>

that the latter would be “*deficient by design*”.¹¹⁰³ After analysing the cooperation mechanisms of the GDPR and their application in practice, the authors identified four general flaws:¹¹⁰⁴

- The tension between, on the one side, the procedural autonomy of national administrative bodies and, on the other side, the need to ensure the consistent and effective enforcement of the GDPR across the EU.
- The sometimes too prominent role of the lead DPA in the context of cross-border cases, at the expense of other DPAs.
- Insufficient procedural fairness guarantees, which translate into limitations on important procedural rights of the complainants or of their representatives, such as the right to be heard, the right to access documents, or more generally the right to an effective remedy of data subjects.
- The divergences in national approaches towards the enforcement of EU data protection law, which create situations where data subjects are treated differently depending on the jurisdiction, in violation of the principle of equality under the law.

Beyond or within these four general flaws, practical issues pertaining to the implementation of the GDPR also impede the optimal enforcement of data protection rules. One may point out, in particular, the lack of financial and human resources of DPAs to handle an ever-increasing number of complaints.

This general issue has been acknowledged by many actors across the board, including (former) members of DPAs themselves.¹¹⁰⁵

Multiple solutions are already being discussed at the national and EU level to tackle these procedural or practical issues, such as developing better rules of procedures or cooperation guidelines between the DPAs and the EDPB (e.g. streamlined criteria regarding the admissibility of complaints, the procedural rights of data subjects,

¹¹⁰³ Gentile, G. & Lynskey, O. (2022). *op. cit.*

¹¹⁰⁴ *Ibid.*, p. 800.

¹¹⁰⁵ See Access Now (2021). Three years under the GDPR. An implementation progress report. Available at <https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf>. Heinrich Böll Stiftung (2021). Trends in Privacy Enforcement: A Comparative Analysis of post-GDPR Enforcement Styles. 30 December 2021. Available via <https://tr.boell.org/en/2021/12/30/trends-privacy-enforcement-comparative-analysis-post-gdpr-enforcement-styles>; Access Now (2021). Three years under the GDPR. An implementation progress report. Available at <https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf>; 3 Years Later: An Analysis of GDPR Enforcement, by Ilse Heine, CSIS, 13 September 2021, available at <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement>; Divergence, Convergence and Challenges: Trends on GDPR Enforcement Across Europe and the UK, by Richard Jeenes et al., Slaughter and May, available at <https://my.slaughterandmay.com/insights/briefings/divergence-convergence-and-challenges-trends-on-gdpr-enforcement-across-europe-and-the-uk>.

etc.), or encouraging governments to adopt various executive measures to facilitate enforcement from a practical point of view (e.g. increasing the human and technical resources allocated to DPAs, implementing new communication tools to share file documents in cross-border cases, etc.).¹¹⁰⁶

To support such efforts, the EDPB has set up a Support Pool of Experts (the **SPE**), whose task will be to provide expertise to and enhance cooperation among national DPAs with a view of supporting investigation and enforcement activities.¹¹⁰⁷ In particular, the SPE will be deployed to provide support to national DPAs by, for example, assisting them in their legal analysis or drafting investigative reports in complex and resource-demanding cases.¹¹⁰⁸ To tackle procedural discrepancies or hurdles in the context of cross-border cases, the EDPS has also suggested to put in place a more centralised enforcement system, where the EDPB itself would take the lead of some investigations and could render binding decisions against controllers or processors.¹¹⁰⁹ This, however, would require amending the GDPR in a way that would further restrict the procedural autonomy of Member States, which can be a political challenge in itself.¹¹¹⁰

Keeping in mind the research question of this study, the question remains however whether the GDPR would truly be '*deficient-by-design*'¹¹¹¹ when it comes to its enforcement. If that would be the case, it could then be argued that the enforcement system of the GDPR is partly dysfunctional because of *internal* factors inherent to the text of the GDPR itself and the enforcement mechanisms that it establishes. In their article, Orla Lynskey and Giulia Gentile seem to conclude however that many of the shortcomings of the cooperation and consistency mechanisms do not stem from the design of the GDPR itself, but rather from the failure of DPAs and the EDPB to implement these mechanisms appropriately. The author of this study agrees with these findings. Indeed, the main practical and legal issues mentioned hereabove do not stem from the text of the GDPR *itself*, but rather from *existing gaps in the text* (which leave room for national divergences), or even sometimes *despite* the explicit requirements set by the text.

As an illustration, the 120th Recital of the GDPR explicitly states that Member States should provide DPAs with the necessary financial and human resources for the effective performance of their tasks, including those related to mutual assistance

¹¹⁰⁶ EDPS, Conference on effective enforcement in the digital world, 16-17 June 2022, Brussels, <https://www.edpsconference2022.eu/en>.

¹¹⁰⁷ EDPB, Terms of Reference of the EDPB Support Pool of Experts, adopted on 15 December 2020, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_document_supportpoolofexpertstor_en.pdf.

¹¹⁰⁸ EDPS, Annual report 2021, p. 140, available at https://edps.europa.eu/system/files/2022-04/2022-04-20-edps_annual_report_2021_en.pdf.

¹¹⁰⁹ EDPS, Conference on effective enforcement in the digital world, 16-17 June 2022, Brussels, <https://www.edpsconference2022.eu/en>.

¹¹¹⁰ Gentile, G. & Lynskey, O. (2022). *op. cit.*

¹¹¹¹ As worded by Giulia Gentile and Orla Lynskey (Gentile, G. & Lynskey, O. (2022). *op. cit.*).

and cooperation with other DPAs in the context of cross-border case.¹¹¹² In practice, however, Member States have often failed to properly allocate such resources to their DPA(s).

Another example relates to the admissibility of complaints lodged by data subjects. According to Recital 141 and Article 57(2) GDPR, DPAs have the explicit duty to facilitate the submissions of complaints by providing an electronic submission form that data subjects can fill in, for example directly on their website. In some jurisdictions, however, these submission forms are only made available if the data subject respects some formal requirements, such as using an e-government email address, an e-government ID-card reader, or another e-government solution.¹¹¹³ In some cases, this can restrict the ability of data subjects or not-for-profit entities to submit a complaint because they are not citizens of the concerned Member States. In other jurisdictions, the complaint of the data subject has to fulfil some substantial requirements to be deemed admissible, such as clearly identifying the breach of the GDPR at stake, filing the complaint before the expiry of a limitation period,¹¹¹⁴ and/or providing evidence that the data subject has first raised the issue with the controller or processor but that no amicable solution could be found.¹¹¹⁵ The EDPB has already condemned some of these practices in several guidelines.¹¹¹⁶ Yet, the guidelines published by the EDPB are non-binding. As a result, some DPAs still impose strict formal or substantial requirements for complaints to be deemed admissible, thereby taking advantage of the gaps left by the GDPR in this respect. Arguing that the GDPR has been purposefully designed to create such discrepancies, however, would not be correct. Rather, it seems that Member States have relied on the principle of national procedural autonomy to design their own national rules, sometimes *in violation of*, or at least *beyond* the standards set by the GDPR, thereby rendering enforcement more challenging for data subjects than it should be.

Yet another example can be given with respect to diligence of DPAs when fulfilling their tasks. Despite the high standards set out by the GDPR in this respect, some DPAs seem simply overwhelmed by the amount of complaints or cases that they

¹¹¹² Recital 120 of the GDPR provides: “Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.” Articles 52 to 54 GDPR further establish strict requirements with respect to the independence, resources, and expertise of DPAs and their members.

¹¹¹³ To this date (October 2022), it is still the case, for example, in Spain and Poland.

¹¹¹⁴ To this date (October 2022), it is still the case, for example, in Austria, Belgium and Slovakia.

¹¹¹⁵ To this date (October 2022), it can be the case, for example, in Belgium, Austria, France. The debate was also on-going in Spain, until the Spanish Supreme Court declared such practice contrary to the GDPR and Spanish data protection law (Spanish Supreme Court, Decision n° 1.039/2022 of 19 July 2022 (STS 3207/2022 - ECLI:ES:TS:2022:3207)).

¹¹¹⁶ See, in particular: EDPB (2021, 2 February). Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements EDPB (2020, 15 December). Available at: https://edpb.europa.eu/our-work-tools/our-documents/internal-documents/internal-edpb-document-022021-sas-duties-relation_en ; Internal EDPB Document 6/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints. Available at: https://edpb.europa.eu/system/files/2022-07/internal_edpb_document_062020_on_admissibility_and_preliminary_vetting_of_complaints_en.pdf

need to handle, which prevent them for properly fulfilling their tasks.¹¹¹⁷ This was once again illustrated by the recent Resolution adopted by the European Parliament calling on the Commission to start infringement proceedings against Ireland, mainly due to the inertia or negligence of the Irish data protection authority in handling complaints from data subjects.¹¹¹⁸

Based on the above, it can thus be argued that, although it is true that the enforcement of the GDPR is still sub-optimal, most of the factors influencing that result do not find their source in the text of the GDPR itself but rather in factors that are *external* to it, such as discrepancies in national procedural rules, or the slow pace of the judicial system of Member States.¹¹¹⁹ The author of this study admits, however, that depending on the situation, some of these factors could also be regarded as *partly internal*, especially when the text of the GDPR remains unclear, leaves gaps or fails at harmonising important procedural aspects of the enforcement system.

This silence of the GDPR should not be regarded as inherently wrongful. As pointed out by Hielke Hijmans, indeed, *“this silence is the logical consequence of the complete independence [of DPAs] as laid down in Article 8 of the Charter and Article 16 [TFEU] and underlined in the case law of the [CJEU] (...). The [CJEU] stated that complete independence is needed in view of the DPAs’ task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data’. Hence, the Court underlines that establishing a balance between the various interests at stake is the essence of DPA independence.”*¹¹²⁰

Since this study primarily aims at identifying the internal factors of multi-functionality of the GDPR, the author of this study will now focus on these internal or semi-internal factors in particular, by discussing the explicit role, rights or duties of the various actors involved in the enforcement of the GDPR, here below.

¹¹¹⁷ See, for example, “All bark no byte? Unease over Irish performance as EU's lead data watchdog”, AFP, 01/11/2020, available at <https://www.france24.com/en/live-news/20201101-all-bark-no-byte-unease-over-irish-performance-as-eu-s-lead-data-watchdog> ; “Belgium’s Data Protection Authority’s independence no longer guaranteed, director warns”, Belga, published by the Brussels Times, 22 February 2021, available at <https://www.brusselstimes.com/news/belgium-all-news/170364/manhunt-day-four-national-park-swept-no-sign-of-fugitive/> ; “Google’s GDPR fine, why was it so low?”, by Michael Baxter, Information Age, 22 January 2019, available at <https://www.information-age.com/google-gdpr-fine-123478411/> ; “European Parliament calls on Commission to open infringement proceedings against Ireland”, NYOB, 21 May 2021, available at <https://noyb.eu/en/european-parliament-calls-commission-open-infringement-proceedings-against-ireland>.

¹¹¹⁸ European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (‘Schrems II’), Case C-311/18 (2020/2789(RSP)).

¹¹¹⁹ Access Now (2022). Three years under the GDPR. An implementation progress report. Available at <https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf>, p. 9.

¹¹²⁰ Hijmans, H. (2018). How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? European Data Protection Law Review, 4(1):80-84.

3.3.2. The multi-actor enforcement system of the GDPR: a double-edged sword for ensuring the respect of the rights and freedoms of data subjects

While effectiveness and functionality are closely related notions, they should not be confused with one another. As explained in the first Chapter of this study, functionality has been conceptualised as relating to the convenience or ease with which various actors may rely on a piece of legislation to achieve its objective. As far as the GDPR is concerned, the latter would thus be functional with respect to its FRO if it provides convenient tools to prevent, detect and/or put an end to potential violations of the fundamental rights and freedoms of data subjects in the context of personal data processing. The below section will precisely discuss specific provisions relating to the enforcement system of the GDPR which, in the opinion of the author, contribute to the overall functionality of this framework, either alone or in combination with other provisions. The main dysfunctionalities of this enforcement system will also be discussed in parallel, with a view of ultimately being able to formulate recommendations on how to improve enforcement for the fulfilment of the FRO of the GDPR.

Before diving into this topic, it is worth noting that a major limitation that could have generally impaired the enforcement of EU data protection law is the fact that data processing practices are not tangible and that violations can thus remain unnoticed. Indeed, beyond the obvious technical barriers that may prevent laymen from uncovering harmful data processing practices, the digital world also gives the possibility to any controllers or processors to swiftly erase, change or transfer any compromising evidence. In the opinion of the author, one of the main ‘counter-factors’ of functionality of the GDPR in this respect is its multi-actor enforcement system. Indeed, DPAs or courts are not the only actors having the possibility to initiate enforcement proceedings; other actors, such as not-for-profit entities, DPOs or data subjects themselves can actively contribute to the respect of the GDPR by shedding light on a violation and putting enforcement into motion. Furthermore, rather than being organised as a pyramid, this enforcement system takes the form of a flexible network,¹¹²¹ where various actors interact and may or must assist one another in preventing, spotting, and putting an end to a violation. There are, in other words, many pairs of eyes directed at controllers and processors, from various angles. Five types of actors can be distinguished in particular: (1) data subjects; (2) DPOs; (3) not-for-profit associations; (4) DPAs; and (5) national courts.

While specific provisions pertaining to the role of each of these actors will be analysed separately, the author of this study is of the opinion that the overall functionality of the GDPR enforcement system principally derives from the

¹¹²¹ Ost, F. (2010). De la pyramide au réseau? Pour une théorie dialectique du droit. *Presses de l'Université Saint-Louis*.

complementarity and synergies between the role played by each of these actors, as foreseen in the text of the GDPR. As further discussed below indeed, their interactions can form various ‘chains of enforcement’ which can generally facilitate the prevention, detection, or prosecution of harmful data processing practices.

3.3.2.1. Data subjects as first-row sentinels: fishing expedition and the facilitation of complaints submission

Data subjects are at the forefront of enforcement in the sense that they can act as first-row sentinels. Through their own experience indeed, they are often the most likely to uncover violations of their rights and freedoms in the context of the processing of their personal data. If, for example, an individual is unduly black-listed as being ‘insolvent’ in a register relating to creditworthiness, which could in turn lead them to be discriminated or unable to exercise their right to property,¹¹²² this individual will be the first one to experience the negative impact of such processing, and may challenge such processing by exercising, for example, their right to rectification or right to object. This section will focus on the provisions of the GDPR that, in the opinion of the author, increase the ease with which data subjects may rely on that framework to enforce their rights and freedoms in the context of data processing, thereby making it more functional.

In that context, some of the data protection rights granted to data subjects can themselves be considered as functional enforcement tools, and in particular their right to information and access to personal data. Indeed, by relying on these legal means, data subjects can initiate small ‘fishing expeditions’ with a view of confirming that a controller is not complying with the GDPR. An obvious element that could have rendered those rights dysfunctional would have been the absence of any leverage left to data subjects in the event a controller or processor would simply ignore their request or answer with incomplete information. Of particular importance in that respect is the fact that, when a controller is unable or unwilling to take actions on the request of a data subject, this may already offer a legal ground for the data subject to lodge a complaint with a DPA, or to seek judicial remedies.¹¹²³ As already mentioned above, DPAs can then use their investigative and corrective powers to obtain the necessary information, and compel the controller to change or put an end to a harmful data processing practice. This bottom-up approach makes from each data subject a potential sentinel for compliance.

Besides these basic data protection rights, several provisions within the GDPR specifically aim at facilitating the use, by data subjects, of the GDPR framework for enforcement purpose. Article 57(2) GDPR in particular provides that each DPA must facilitate the submission of complaints, including by offering to data subjects the

¹¹²² See, for example, CJEU, Case C-398/15, *Manni*, para. 35.

¹¹²³ Article 12(4) GDPR.

possibility to submit a complaint electronically. Most DPAs offer that possibility by providing for an electronic form on their respective website. The way these forms are structured may further guide the data subjects in filing their complaints, thereby facilitating the entire process. The CNPD, for example, offers a multi-steps complaint form on its website, available in English, French and German.¹¹²⁴ Each field within this form is explained in easy and plain language. As an alternative, however, data subjects can also submit a complaint by sending an email to the general address of the CNPD or by sending a letter to their official address. The CNIL in France, the *Autoriteit Persoongegevens* in the Netherlands, the APD in Belgium, and other DPAs across the EU have adopted a similar approach.¹¹²⁵ Article 57(3) GDPR further provides that the services rendered by the DPAs must be free of charge for the data subjects. Given that some data subjects may be deterred from filing a complaint if the procedural costs would be too significant, such a safeguard was essential to guarantee the success of the complaint filing system.

As said above, however, the functional tools provided to data subjects to initiate the enforcement process would not suffice if data subjects were not provided with external support. It cannot be expected from all data subjects, for example, to have a deep knowledge of the applicable data protection rules, to spend time investigating a potential infringement – for example, in the context of complex AIDM with potential discriminatory effects – or to assiduously follow up on a complaint that they may have lodged with a DPA. Hence, the fact that they may entrust a DPA with their case, free of charge, is essential to the functionality of the entire framework. As said above however, DPAs themselves may not always have the necessary resources to properly investigate and follow-up on all complaints, or may be tempted to consider a complaint as unworthy of their attention, especially when the violation appears negligible, or the information provided incomplete. The lack of involvement or diligence of DPA in pursuing infringers may lead to ‘pick and choose’ some cases over others – even if, strictly speaking, this is not allowed under the GDPR.¹¹²⁶ The various factors that may cause a DPA *not* to enforce the GDPR can thus be classified as *external* factors of dysfunctionality.

What is interesting to note is that, in the event a DPA does not properly handle a complaint, for example, by remaining silent for half a year and not investigating the case, the latter may file a complaint and obtain an effective judicial remedy against a DPA based on Article 78 GDPR. Yet, it must be stressed that this possibility will not solve in itself the underlying issue which triggered the need of the data subject to

¹¹²⁴ See CNPD complaint form (online). <https://cnpd.public.lu/en/particuliers/faire-valoir/formulaire-plainte.html>.

¹¹²⁵ See, respectively, for the CNIL: <https://www.cnil.fr/fr/adresser-une-plainte>; for the *Autoriteit Persoongegevens*: <https://autoriteitpersoongegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap> ; and for the APD/GBA: <https://www.autoriteitprotectiondonnees.be/citoyen/agir/introduire-une-plainte>.

¹¹²⁶ According to Article 57(1)(a) GDPR indeed, DPAs “shall (...) monitor and enforce the application of this Regulation”. The use of the term ‘shall’ indicates that DPAs have normally an obligation to enforce the GDPR, regardless of the type or level of seriousness of the infringement.

rely on the GDPR in the first place. Furthermore, in most Member States, judicial proceedings are often costly and lengthy – two characteristics that may further delay the enforcement process. Although relevant to understand the potential weaknesses of any imperative norms, the difficulties that data subjects may experience in holding DPAs accountable for their lack of actions can also be categorised as *external* factors of the dysfunctionality of the GDPR. Consequently, the EU legislator may not alone rectify these elements by amending the GDPR. Rather, it necessitates improvements with respect to access to or the organisation of DPAs or national courts at the national level, so that the work of DPAs meet the actual requirements laid down in the GDPR. For this reason, these elements will not be further discussed within this study. Furthermore, from the perspective of the functionality of the GDPR, it is worth stressing that two other categories of actors with more expertise in the field of data protection may help bridging the enforcement gap between, on the one side, data subjects and, on the other side, DPAs: DPOs and not-for-profit entities.

3.3.2.2. DPOs as compliance insiders and informers: a (dys)functional channel of communication for compliance?

DPOs are described in the GDPR as persons having “*expert knowledge of data protection law*”.¹¹²⁷ As already discussed above (Section 3.2.2.2(iii)), their general task is to monitor the processing activities of the controller or processor for which they work, and advise the latter on how to ensure, maintain or better achieve compliance with EU data protection law. More specific tasks include advising on the conduct of DPIAs,¹¹²⁸ providing information in the event of a data breach,¹¹²⁹ or being a point of contact for data subjects and DPAs when questions or requests arise with respect to compliance.¹¹³⁰ DPOs therefore play a pivotal role for fostering a culture of compliance with the GDPR, both in a preventive and corrective way.

On the one hand, the obligation for controllers to appoint a DPO can be seen in itself as a factor of functionality of the GDPR, in the sense that the concerned controller or processor will be continuously advised on how to comply with the GDPR by an expert in that field, internally. On the other side, an obvious pitfall with respect to the role of DPOs is the fact that the organisation for which they work could simply ignore their recommendations and initiate or maintain a processing activity that disproportionately interferes with the rights and freedoms of data subjects. Being deprived of any coercive powers, DPOs can indeed not force their organisation to put an end to a violation, even if the violation is obvious, such as an e-recruitment procedure which would exclude women without any rational basis, the tracking of company’s cars without informing employees thereof, or an automated decision-

¹¹²⁷ Recital 97 GDPR and Article 37(5) GDPR.

¹¹²⁸ Article 35(2) GDPR.

¹¹²⁹ Article 33(3)(b) GDPR.

¹¹³⁰ Article 39(1)(d) and (e) GDPR.

making process for creditworthiness which is based on incorrect data.¹¹³¹ Furthermore, as already pointed out above, DPOs cannot freely alert the media or the general public about these issues, since DPOs are subject to a strict obligation of professional secrecy and confidentiality.¹¹³²

What DPOs can do however is to alert the relevant DPA of the fact that the controller or processor for which they work systematically ignore their recommendations.¹¹³³ Article 39(1)(e) GDPR indeed provides that DPOs can always consult the competent DPA in the context of a DPIA or on “*any other matter*”. In the opinion of the author of this study, this provision should be interpreted as opening a safe communication channel between DPOs and DPAs with respect to the existence of any persistent violation that a controller or processor refuses or neglects to address despite the warning of its DPO, so that the competent DPA can exercise its coercive power against the controller or processor in question. Indeed, given that members of DPAs are themselves subject to an obligation of secrecy and confidentiality, the information shared by a DPO with a DPA remains protected.¹¹³⁴ Guaranteeing a secure communication channel free from any restriction between DPOs and DPAs is essential for ensuring that DPOs can effectively participate to the enforcement of EU data protection law in their capacity as watchdogs, instead of being muzzled by their hierarchy and turned into harmless pets. It can thus be concluded that, albeit limited, DPOs can still take on the role of compliance informers towards the competent DPA. Furthermore, another element that participates to the functionality of this chain of enforcement is the fact that DPOs cannot be dismissed or penalised by the controller or the processor for performing their role.¹¹³⁵ This protection is of course essential to enable DPOs to fully perform their role as compliance insider without fearing retaliation.

Comparably to data subjects, DPOs may thus also be regarded as sentinels for compliance and enforcement. However, rather than having redundant roles, three major differences between data subjects and DPOs make them complementary within the enforcement chain of the GDPR: the first major difference is that DPOs are working *within* an organisation and – as required by the GDPR – are normally involved in all data protection-related matters *from the outset*. DPOs thus have a complete picture of the situation and should be in a better position to identify potential violations and report them to their controller or processor in both a preventive and corrective manner. A second major difference is that DPOs are required to have expert knowledge of data protection law and practices,¹¹³⁶ and are thus also in a better position to understand when a breach of the applicable rules

¹¹³¹ See for example, noyb. (2021, August 4). Data voodoo: Credit ranking agency CRIF creates creditworthiness out of thin air. <https://noyb.eu/en/data-voodoo-credit-ranking-agency-crif-creates-credit-rating-out-thin-air>.

¹¹³² Article 38(5) GDPR.

¹¹³³ WP29, Guidelines on DPOs, *op. cit.*, p. 18: “(...) *the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority.*”

¹¹³⁴ Article 54(2) GDPR.

¹¹³⁵ Article 38(3) GDPR.

¹¹³⁶ Recital 97 and Article 37(5) GDPR.

can have a potential negative impact on the rights and freedoms of the data subjects. A third major difference is that DPO can directly report to the highest management level of the controller or the processor, and are thus in a better position than data subjects with respect to advising and convincing the organisation for which they work to bring the processing activities into compliance with the GDPR.¹¹³⁷ For that purpose, it is of course essential to guarantee that DPOs have both the resources and the necessary independence to fulfil their tasks – two safeguards that the GDPR has put into place, as discussed above (see Section 3.2.2.2(iii) of this Study).

Besides data subjects and DPOs, a third category of actors belonging to the civil society may actively contribute to the enforcement of EU data protection law. The complementary nature of this third category of actors, as well as the specific role they may play for the protection of data subjects' fundamental and freedoms in particular, will be discussed in the section below.

3.3.2.3. Not-for-profit associations or bodies as strongholds and bridges for data protection enforcement and fundamental rights protection

This section will look into the provisions of the GDPR that increase the ease with which not-for-profit organisations, associations and bodies (hereafter, 'not-for-profit entities') may rely on that framework to defend the rights and freedoms of data subjects in the context of data processing, thereby contributing to the functionality of the enforcement system of the GDPR. Data subjects and DPOs are indeed not the only actors within civil society which may attract the attention of controllers, processors or DPAs on a potential violation of EU data protection law, and therefore participate to the effective protection of the rights and freedoms of data subjects against harmful data processing practices; not-for-profit entities can also do so.

In the EU, many not-for-profit entities active in the field of data protection, privacy, or more generally human rights are relentlessly patrolling the Internet, channelling complaints from data subjects, critically reviewing the activities of DPAs, or assessing the risks that new or future DDTs or data processing practices could pose for human rights. Among these not-for-profit entities, one may refer in particular to NOYB¹¹³⁸, La Quadrature du Net,¹¹³⁹ Privacy International,¹¹⁴⁰ Digital Rights Ireland,¹¹⁴¹ GDD,¹¹⁴² Big

¹¹³⁷ Article 37(5) GDPR.

¹¹³⁸ *noyb* - European Center for Digital Rights is an NGO based in Vienna, Austria. *noyb* is an acronym for '*none of your business*'. *noyb* specialises in GDPR enforcement through strategic litigation all over the EU. Its founder and honorary chairman, Maximilian Schrems, was the initial complainant in the *Schrems I* and *Schrems II* case on data transfers from the EU towards the US. Source: <https://noyb.eu/en/our-detailed-concept>.

¹¹³⁹ *La Quadrature du Net* is based in Paris, France. Their core purpose is to defend fundamental rights and freedoms in the digital sphere, including through strategic litigation. They notably challenged the legality of Directive 2006/24/EC on data retention by electronic communication service providers (see case C-512/18) as well as the targeted advertising practices of Amazon, having given rise to a fine of 746 million euros by the CNPD against Amazon (decision not yet published). Source: <https://www.laquadrature.net/nous/>.

Brother Watch,¹¹⁴³ Privacy First,¹¹⁴⁴ Bits of Freedom,¹¹⁴⁵ Digitalcourage,¹¹⁴⁶ or Access Now,¹¹⁴⁷ among others.¹¹⁴⁸ Some of these not-for-profit entities collaborate together through the Brussels-based European network EDRI.¹¹⁴⁹

From the perspective of the functional role that they play, these not-for-profit entities may not only shed light on potential violations and alert competent DPAs but may also take an active stance on behalf of data subjects by lodging a complaint with a DPA or by seeking judicial remedies on their behalf – with or without having specifically mandated by the data subjects to do so. According to Article 80(1) GDPR indeed, EU-based not-for-profit entities active in the field of the protection of data subjects’ rights and freedoms may be mandated by one or multiple data subjects to lodge a complaint with a DPA. Article 80(2) GDPR further provides that Member States may allow NGOs to exercise the right to a judicial remedy or exercise the right to receive compensation on behalf of data subjects, independently from any mandate from them.¹¹⁵⁰ This representative action can be brought by a not-for-profit entity whenever the latter “*considers*”¹¹⁵¹ that the rights of one or more data subjects provided for in the GDPR have been infringed. Some not-for-profit entities – including NOYB and La Quadrature du Net – have thus specialised in strategic litigation in the field of data protection, by representing (group of) data subjects

¹¹⁴⁰ *Privacy International (PI)* is a registered charity based in London that works at the intersection of modern technologies and rights. They notably challenged the legality of Directive 2006/24/EC on data retention by electronic communications service providers (see case C-623/17). Source= <https://privacyinternational.org/about>.

¹¹⁴¹ Digital Rights Ireland is based in Kilkenny, Ireland. They are dedicated to defending civil rights in the digital age. They notably challenge the legality of Directive 2006/24/EC on data retention by electronic communications service providers (see Cases C-293/12 and C-594/12). Source: <https://www.digitalrights.ie/>

¹¹⁴² The German Association for Data Protection and Data Security (GDD) was founded in 1976 and stands as a non-profit organization for practicable and effective data protection. Source: <https://www.gdd.de/international/english>.

¹¹⁴³ Big Brother Watch is based in London, UK. Their main goal is to defend privacy and defend freedoms against intrusive technologies, including through lobbying and strategic litigation. Source: <https://bigbrotherwatch.org.uk/about/>.

¹¹⁴⁴ Privacy First is based in Amsterdam, The Netherlands. This NGO promotes civil rights and privacy protection in the Netherlands and in Europe. They notably initiated a case against the Dutch government for implementing a discriminatory tax fraud detection system (i.e., the so-called ‘SyRI case’).

¹¹⁴⁵ Bits Of Freedom is based in Amsterdam, The Netherlands. It is an independent Dutch digital rights foundation, which focuses on privacy and communications freedom in the digital age. Source: <https://www.bitsoffreedom.nl/hoef/>

¹¹⁴⁶ Digitalcourage is based in Bielefeld, Germany. Digitalcourage – known until November 2012 as FoeBuD – is a German privacy and digital rights organisation. Source: <https://digitalcourage.de/>

¹¹⁴⁷ The headquarters of Access Now are based in New York, US. The NGO has however been closely following up and drafting reports on the implementation of the GDPR in the EU. See <https://www.accessnow.org/>.

¹¹⁴⁸ ApTI – Association for Technology and Internet, CILD – Coalizione Italiana Libertà e Diritti Civili, D3 – Defesa dos Direitos Digitais, Dataskydd.net, Electronic Frontier Norway, Electronic Frontier Finland, Epicenter.works, Fitus, Homo Digitalis, Panoptykon Foundation, Vrijdschrift, State watch, Initiative für Netzfreiheit, or Homo Digitalis.

¹¹⁴⁹ European Digital Rights (EDRI) is an association regrouping various NGOs in Europe and the US, including NGO active in the field of data protection and privacy, such as La Quadrature du Net, Access Now, Bits of Freedom, Dataskydd.net, or EPIC. Source: <https://edri.org>.

¹¹⁵⁰ Recital 142 of the GDPR.

¹¹⁵¹ Article 81(2) GDPR.

against big tech companies, such as Facebook,¹¹⁵² Amazon,¹¹⁵³ Google,¹¹⁵⁴ Airbnb,¹¹⁵⁵ Grindr,¹¹⁵⁶ or credit scoring agency such as CRIF.¹¹⁵⁷

In the case *Meta v. BVV*, the CJEU further interpreted Article 80(2) GDPR in a non-restrictive way, thereby reinforcing the possibility for those not-for-profit entities to intervene and play an active role for the enforcement of data subject's rights under the GDPR.¹¹⁵⁸ The facts of this case concerned the processing activities of Meta Platforms Ireland (formerly known as Facebook Ireland; hereinafter 'Meta'). More specifically, Meta made available free games designed by gaming companies through the 'App Center' of various websites, including the German website "www.facebook.de". When consulting this App Center, an indication would appear, informing users that access to certain games would enable the gaming companies to collect and process their personal data. Another consequence of that use is that the users would need to accept the terms and conditions of the application, its data protection policy, and also to authorise the gaming company to make publications on their behalf, such as their score and other information.¹¹⁵⁹ In view of these practices, the Federal Union of Consumer Associations in Germany (hereinafter 'BVV') decided to bring an action for an injunction against Meta on the basis of the applicable German law against unfair commercial practices. In the course of this procedure, the German Federal Court of Justice (the 'Bundesgerichtshof') expressed doubts as to the admissibility of BVV's action, given the entry into force of the GDPR on 25 May 2018, and the changes that this regulation had brought with respect to the conditions attached to the locus standi of not-for-profit associations. The Bundesgerichtshof therefore decided to stay the proceedings and referred several questions to the CJEU for a preliminary ruling. The main question before the CJEU concerned the interpretation to be given to Article 80(2) of the GDPR. As noted by the CJEU in this ruling,¹¹⁶⁰ the German legislator did not adopt any specific national provisions to implement Article 80(2) of the GDPR after the entry into force of that regulation. Yet, even prior to the entry into force of the GDPR, German consumer law already allowed consumer associations to take legal action against an alleged infringer of data protection law. As such, there was thus no need for the German legislator to adopt new provisions to implement the representative action

¹¹⁵² See, inter alia, <https://noyb.eu/de/irische-behoerde-schliesst-noyb-aus-laufenden-verfahren-aus-staatsanwaltschaft-informiert>

¹¹⁵³ See, inter alia, <https://noyb.eu/en/black-box-amazon-algorithm-discriminates-customers> ; <https://noyb.eu/en/complaint-filed-help-my-recruiter-algorithm>.

¹¹⁵⁴ See a summary of the case brought by *La Quadrature du Net* against Google: <https://www.laquadrature.net/en/2019/01/21/first-sanction-against-google-following-our-collective-complaints/>

¹¹⁵⁵ See a summary of the complaint filed by *noyb* against Airbnb: <https://noyb.eu/en/gdpr-complaint-airbnb-hosts-mercy-algorithms>

¹¹⁵⁶ See a summary of the case filed by *noyb* against Grindr: <https://noyb.eu/en/gay-dating-app-grindr-be-fined-almost-eu-10-mio>

¹¹⁵⁷ See a summary of the case filed by *noyb* against CRIF: <https://noyb.eu/en/data-vooodoo-credit-ranking-agency-crif-creates-credit-rating-out-thin-air>

¹¹⁵⁸ CJEU, Judgment of 28 April 2022, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.*, Case C-319/20.

¹¹⁵⁹ *Ibid.*, para. 34.

¹¹⁶⁰ *Ibid.*, para. 61.

mechanism provided for in Article 80(2) GDPR. A closer reading of this Article reveals however that this representative action mechanism remains subject to a number of requirements, both in terms of personal and material scope. It is precisely on these requirements that the CJEU has provided clarifications in response to the preliminary questions referred by the Bundesgerichtshof.

As to the personal scope of this representative action mechanism, not-for-profit entities must fulfil three conditions under Article 80(1) GDPR in order to be entitled to bring judicial proceedings against a controller or processor: first, they must have been properly constituted in accordance with the law of a Member State. Second, they must have statutory objectives which are in the public interest (e.g., consumer protection, privacy, gender equality, access to the internet, non-discrimination, freedom of expression on the internet, etc.). Thirdly, these entities must be active, for the purpose of achieving their public interest objective, in the field of the protection of data subjects' rights and freedoms with regard to the processing of their personal data.¹¹⁶¹ On this basis, the CJEU found that a consumer protection association such as the BVV can fall within the personal scope of Article 80 of the GDPR, since its statutory objective is to protect the rights of consumers, including in the context of digital sales where personal data are being processed. Indeed, as the CJEU pointed out in its ruling, the defence of consumers' interests is an objective that is *"likely to be related to the protection of the personal data of those persons"*,¹¹⁶² especially in the context of online services. Meta's commercial practices give an illustration of this likelihood since the provision of online games via the App Center necessarily involved the processing of users' personal data. Based on these considerations, the CJEU therefore concluded in its judgment that nothing prevents a consumer protection association such as the BVV from being entitled to bring judicial proceedings against a controller or processor in the event of an infringement by the latter of the data protection rights of a (group of) consumer(s).¹¹⁶³

As far as the material scope of Article 80(2) GDPR is concerned, the exercise of a representative action by a not-for-profit entity also presupposes that the entity, *"independently of a data subject's mandate, (...) considers that the **rights of a data subject under this Regulation have been infringed as a result of the processing**"* (emphasis added). In its judgment, the CJEU clarified two important points relating to this material scope by looking into whether it would be necessary for a not-for-profit entity to (1) identify one or more individuals whose personal data were processed in breach of the GDPR and/or to (2) prove the existence of a concrete breach of the GDPR and/or actual harm suffered by the concerned data subject(s) because of a violation of their data protection rights. On the basis of a textual analysis of the wording of this provision, the CJEU first noted that not-for-profit entities cannot be

¹¹⁶¹ In other words, it is not required that the not-for-profit entity be exclusively active in the field of data protection but it must at least pursue an objective of public interest with a connection to data protection. See Karg M. (2021), in Wolff/Brink, *BeckOK DatenschutzR*, Article 80 GDPR (C.H. Beck, 36th edition).

¹¹⁶² CJEU, *Meta vs. BVV*, Case C-319/20, para. 61.

¹¹⁶³ *Ibid.*

required to carry out a prior individual identification of the person(s) specifically concerned by the processing operations allegedly contrary to the provisions of the GDPR.¹¹⁶⁴ This interpretation is primarily supported by the fact that the notion of ‘data subject’ as defined in Article 4(1) of the GDPR covers both identified or identifiable natural persons, i.e., people whose identity is not specifically known. In these circumstances, the CJEU thus considered that it is clear that the exercise of the representative action provided for in Article 80(2) of the GDPR is not conditional on the prior identification of complainants or victims. Rather, it is sufficient, according to the CJEU, that the not-for-profit entity designates a “category” or “group” of persons affected by the processing, without having to identify or obtain a mandate from them.¹¹⁶⁵ The CJEU further noted that bringing a representative action is also not subject to the existence of a “specific” infringement of the rights which a person derives from the GDPR.¹¹⁶⁶ Indeed, in view of the wording of this provision, it suffices that the not-for-profit entity “considers” that a data subject’s rights under the GDPR have been infringed to be able to bring judicial proceedings against the alleged infringer. In other words, it is enough if the not-for-profit entity “alleges”¹¹⁶⁷ the existence of a breach affecting data subject’s rights, without it being necessary however “to prove actual harm suffered by the data subject, in a given situation, by the infringement of his or her rights”.¹¹⁶⁸ In the opinion of the CJEU, this interpretation is consistent with Article 16 TFEU, Article 8 of the Charter of Fundamental Rights of the European Union and with the general objective pursued by the GDPR, which consists in ensuring effective protection of the fundamental rights and freedoms of natural persons and, in particular, of ensuring a high level of protection of individuals in the context of the processing of their personal data.¹¹⁶⁹ In other words, the CJEU specifically relied on the FRO of the GDPR to give a non-restrictive interpretation to Article 80(2) GDPR. In particular, the CJEU is of the opinion that the possibility of empowering consumer associations such as the BVV to seek judicial remedy against a controller or processor, without first having to prove the existence of a specific violation of the rights of one or more identified persons, “undoubtedly contributes to strengthening the rights of data subjects and ensuring that they enjoy a high level of protection”.¹¹⁷⁰ Concurring with the opinion of the Advocate General, the CJEU thus confirmed and further reinforced the “preventive function”¹¹⁷¹ of the representative action mechanism provided for in Article 80(2) of the GDPR.

All in all, the CJEU has therefore adopted a non-restrictive interpretation of Article 80(2) GDPR which reinforced the locus standi of not-for-profit entities, to the benefit of the protection of data subjects’ rights. This ruling indeed confirms the proactive

¹¹⁶⁴ *Ibid.*, para. 68.

¹¹⁶⁵ *Ibid.*, para. 69.

¹¹⁶⁶ *Ibid.*, para. 70.

¹¹⁶⁷ *Ibid.*, para. 72.

¹¹⁶⁸ *Ibid.*

¹¹⁶⁹ *Ibid.*, para. 73.

¹¹⁷⁰ *Ibid.*, para. 74.

¹¹⁷¹ *Ibid.*, para. 76.

role those not-for-profit entities can play for the protection of various rights of data subjects, including consumer protection, when the latter correlates with a violation of their data protection rights under the GDPR. Such actions can thus contribute to the fulfilment of the FRO of EU data protection law by enforcing the rights of an indefinite number of (actual or future) data subjects both in a preventive and a remedial way. In the case at hand, for example, the action brought by the BVV against Meta can benefit both present and future users of the App Center of Meta. At the end of the day, however, it must be stressed that Member States still hold the legislative key which can restrict or open the way to such representative actions. Indeed, although the GDPR is a regulation intended to fully harmonise the rules applicable to the processing of personal data in the EU, Article 80(2) of the GDPR constitutes a so-called “*opening clause*”.¹¹⁷² This clause gives Member States the option – but not the obligation – to lay down additional or derogating national rules to facilitate such representative actions. Given that a wide margin of discretion is left to Member States in this respect, it is to be feared that procedural divergences will persist from one Member State to another.

Yet, it cannot be denied that not-for-profits entities can play a double functional role when it comes to GDPR enforcement. First, they may act as a stronghold behind which various individuals suffering from the same (even minor) violation may gather. In particular, a not-for-profits entity may decide to raise awareness on a specific data protection issue and invite the concerned data subjects to mandate them to act, with a view of initiating a collective action before a DPA on behalf of the entire group. In that context, each registration gathered by the not-for-profit entity may be compared to the piece of a puzzle which, once assembled, may give a more compelling picture of the scope and extent of the infringement at stake. This was the case, for example, in the complaint lodged by La Quadrature du Net against Amazon Europe Core S.à r.l. with respect its targeted advertising practices. In total, 10.000 users of Amazon services residing in France had registered as complainants and mandated la Quadrature du Net to represent them before the CNIL.¹¹⁷³ Second, not-for-profits entities may act as a bridge between, on the one side, a data subject with no or little knowledge over data protection rules, and, on the other side, the competent DPA, by assisting the data subject in filing a complaint. This is particularly important for complex cases, including cases involving multiple data controllers, cross-border processing, or untransparent data processing practices. For that reason, it can be argued that Article 80 of the GDPR is particularly functional in the sense that it enables not-for-profit entities to become strongholds for the defence of the fundamental rights and freedoms of data subjects.

For the perspective of the FRO of EU data protection law, the role of not-for-profits entities may also be particularly functional given that many of these entities often

¹¹⁷² *Ibid.*, para. 57.

¹¹⁷³ See the original complaint filed by *La Quadrature du Net* with the CNIL, para. 5, available at <https://gafam.laquadrature.net/wp-content/uploads/sites/9/2018/05/amazon.pdf>.

have as a core purpose the defence of a public interest and/or fundamental rights. Whether specialised in the defence of privacy, freedom of expression, due process, or non-discrimination, they have usually acquired expert knowledge in the field of human rights law. By relying on such expertise, they are thus often in a better position to understand and seize the opportunity to defend fundamental rights through the application of data protection law, when one or more subjective rights of data subjects under the GDPR have also been infringed. In that sense, not-for-profit entities do not only have the role of strongholds for the defence of data subjects' rights and freedoms but can also act as bridges for the effective fulfilment of the FRO of EU data protection law. The notion of 'bridge' echoes the link that these entities may create between data subjects on the one side, and DPAs or courts on the other side with respect to the enforcement of data protection law and the defence of data subjects' fundamental rights and freedoms. Indeed, although the role that not-for-profit entities can play within the enforcement network of the GDPR is particularly relevant for the fulfilment of its FRO, it would have little or no impact without the later intervention of DPAs or national courts. This is because not-for-profit entities, like data subjects or DPOs, lack the necessary coercive powers to force controllers and processors to comply with the GDPR. This is because data subjects, DPOs and not-for-profit entities merely have the role of sentinels, informers or 'bridges', but have no investigative or corrective powers. Hence, in the event a controller or processor does not bring its processing practices into compliance despite their request to do so, these actors will have no other choice but to pass on the torch to an authority having the ability to issue a binding decision. Under EU data protection law, two authorities may come straight to mind: (1) DPAs (with the oversight of the EDPB, as the case may be); and (2) national courts. The functional and *less* functional aspects of the GDPR pertaining to the role of DPAs and courts will be discussed here below.

3.3.2.4. DPAs as key actors for the enforcement of the GDPR: discretionary use of their wide powers as factors of (dys)functionality

DPAs indubitably play a central role within the multi-actor enforcement network of the GDPR. While data subjects or other actors of civil society do not have any coercive powers, DPAs have the ability to prevent or to put an end to any data processing practice by issuing injunctions and imposing fines.¹¹⁷⁴ For that reason, not-for-profit entities and DPAs have been described as "*natural allies when it comes to putting data protection principles to practice, empowering individuals to assert their rights and holding data controllers accountable for their actions.*"¹¹⁷⁵

¹¹⁷⁴ As foreseen by Article 83 GDPR.

¹¹⁷⁵ Wiewiórowski, W. (2018, May 15). Civil society organisations as natural allies of the data protection authorities. EDPS. https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_en.

Because their investigative and corrective powers, DPAs play the role of quasi-judicial authorities within the enforcement network of the GDPR.¹¹⁷⁶ The more DPAs exercise their powers, the more they may contribute to the effective enforcement of the GDPR, which may in turn boost its functionality. The more a law is interpreted and applied indeed, the easier it usually becomes to use it because of repetition, generalization and standardisation.

Yet, the question remains whether the tasks and powers of DPAs are ‘multi-functional’ enough for the FRO of the GDPR, in the sense that they would both allow and encourage DPAs to take an active stance in cases where a data processing activity would be harmful to the fundamental rights and freedoms of data subjects, including DFR.

Under Article 51 GDPR, DPAs are explicitly made responsible for monitoring the application of the GDPR “*in order to protect the fundamental rights and freedoms of natural persons in relation to processing*”,¹¹⁷⁷ without any distinction as to which right or freedom would be primarily concerned. A literal reading of the GDPR thus tends to confirm that DPAs are competent for enforcing data protection rules to ensure the respect of the right to privacy, data protection or any other fundamental right, such as freedom of expression, non-discrimination or the right to property – just to name a few. This perspective is further reinforced by the fact that several provisions of the GDPR put the rights and freedoms of data subjects at the centre of any assessment on the lawfulness of a data processing activity. Among these provisions, one may refer in particular to Article 6(1)(f) GDPR (i.e., need to balance the legitimate interest of the controller to process personal data with the rights and freedoms of the data subject), Article 21(1) GDPR (i.e., possibility for controllers to reject an objection from a data subject if the controller is able to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject), or Article 22(2)(b) GDPR (i.e., possibility for controllers to rely on AIDM when authorised by EU or national law, to the extent that the law in question lays down suitable safeguards to protect the rights and freedoms of the data subjects). Quite logically, when checking whether controllers have complied with these obligations, DPAs must thus normally review the balancing test conducted by controllers and take into consideration any interference that the processing may cause with the rights and freedoms of the concerned data subjects. There is thus no doubt as to the fact that DPAs are generally competent to deal with fundamental rights issues arising from the processing of personal data. Yet, there is no provision in the GDPR whereby DPAs are required to pay specific attention and thoroughly investigate cases where other fundamental rights could suffer from an interference. DPAs therefore enjoy a high degree of discretion in this respect. As a

¹¹⁷⁶ Porcedda, M. G. (2017). Use of the Charter of Fundamental Rights by Data Protection Authorities and the EDPS. Research Project Report. EUI. <https://op.europa.eu/o/opportal-service/download-handler?identifier=c17ffac6-5ae5-11e7-954d-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=>

¹¹⁷⁷ Article 51(1) GDPR.

result, practices may vary from one Member State to another.¹¹⁷⁸ The below section will discuss this issue, in particular.

Keeping the research question of this study into mind, a specific issue which may arise in the context of GDPR enforcement is the reluctance of some DPAs to rule on cases where the fundamental rights and freedoms of a data subject is conflicting with the rights and freedoms of another party, such as the controller. Some DPAs indeed appear to consider that they lack the necessary legitimacy or competence under national law to render a binding decision that would restrict the fundamental right or freedom of another party. To illustrate the different approaches of DPAs to these fundamental rights issues, one may compare decisions from the Icelandic and the Spanish DPA respectively, concerning the publication of pictures or videos on social media.

The first case – which took place in Iceland – concerns the publication, on Facebook, of the pictures of a child by the father.¹¹⁷⁹ The pictures were accompanied by negative comments concerning the mother because of a dispute on the custody of the child. The mother filed a complaint with the Icelandic DPA to have these pictures and comments removed from Facebook. After investigating the case and collecting the point of view of all the parties involved, the Icelandic DPA rendered a decision in which it stated that the household exemption did not apply to the processing at stake, given that the pictures were accessible to an unlimited number of persons.¹¹⁸⁰ As a consequence, the Icelandic DPA considered that the processing was falling within the material scope of the GDPR. The Icelandic DPA then analysed the relation between the freedom of expression of the father, on the one hand, and the right to privacy and data protection of the child and of the mother, on the other hand. The DPA considered in particular that the father had been exercising his freedom of expression by alerting the public about the difficult situation that he was going through with respect to the custody of the child. The Icelandic DPA then pointed out that freedom of expression was not an absolute right but could be restricted where necessary for protecting the rights and interests of others, such as the right to privacy and data protection of the mother and of the child. By further looking into the extent of its competences as laid down in the GDPR and in the applicable Icelandic data protection law,¹¹⁸¹ the Icelandic DPA considered however that it did not have the power to render a binding decision on the limits of freedom of expression as guaranteed by the Icelandic Constitution and the ECHR, but that such disputes should be subject to judicial review instead. As a consequence, the Icelandic

¹¹⁷⁸ Porcedda, M. G. (2017). *op cit*.

¹¹⁷⁹ Persónuvernd, Mál nr. 2020010552, 17 November 2021, <https://www.personuvernd.is/urlausnir/kvortun-yfir-birtingu-ljosmynda-a-samfelagsmidli-visad-fra>.

¹¹⁸⁰ In line with the CJEU judgment in *Lindqvist*, Case C-101/01.

¹¹⁸¹ Act 90/2018 on Data Protection and Processing of Personal Data, entered into force on 15 July 2018. An English version of this Act is made available on the website of the Icelandic DPA https://www.personuvernd.is/media/uncategorized/Act_No_90_2018_on_Data_Protection_and_the_Processing_of_Personal_Data.pdf).

DPA ultimately declared itself incompetent to rule on the case and rejected the complaint.

By contrast, the Spanish DPA (AEDP) usually considers itself competent to rule on cases involving a conflict between different fundamental rights. For example, the AEDP imposed a fine of €2,000 on the owner of a tobacco shop for publishing on Facebook and Instagram several pictures of a couple with comments accusing them of a robbery. The AEDP strictly applied the rules of the GDPR by analysing in particular whether the shop owner had a valid legal basis for processing these data under Article 6 GDPR. In this respect, the AEDP found that the shop owner did not lawfully process the personal data because the consent of the individuals concerned had not been obtained prior to the publication of the video – ‘consent’ being considered by the AEDP as the only acceptable legal basis for taking and disseminating pictures of individuals on social media.¹¹⁸² Contrary to the approach adopted by the Icelandic DPA, the AEDP did not take freedom of expression into consideration when ruling on this case. In yet another case, the AEDP even took a more active stance by starting from its own initiative an inquiry regarding the publication of a video on Twitter picturing gender-based violence.¹¹⁸³ The video had been published by a user of Twitter together with a message aiming to raise awareness about violence perpetrated against women. Following its investigation, the AEDP found that the victim and her child were identifiable on the video and could thus be considered as data subjects under the GDPR. The AEDP further held that the Twitter user in question – i.e., the controller – had published the video in breach of Article 6(1) GDPR, because the consent of the victim and of her child had not been obtained prior to the processing. Once again, the AEDP did not find it necessary to assess whether such interpretation would not unduly restrict the freedom of expression of the Twitter user. Rather, the AEDP simply established the existence of a breach and fined the Twitter user €6,000 for unlawful processing.¹¹⁸⁴

Other DPAs confronted to similar cases adopted an in-between approach; they applied data protection rules to the publication of pictures on social media while carefully balancing the different interests, fundamental rights and freedoms at stake, in line with Article 6(1)(f) GDPR.¹¹⁸⁵ Unlike the AEDP, indeed, many DPAs consider that Article 6(1)(f) GDPR – i.e., the legitimate interest of the controller – can be used as a valid legal basis for the publication of pictures of third parties on social media, to the extent that the rights and freedoms of the data subjects concerned do not

¹¹⁸² AEDP, Expediente N° PS/00433/2021, 17 January 2022, available at <https://www.aepd.es/es/documento/ps-00433-2021.pdf>.

¹¹⁸³ AEDP, Expediente N° PS/00205/2021, 26 June 2021, available at <https://www.aepd.es/es/documento/ps-00205-2021.pdf>.

¹¹⁸⁴ *Ibid.*

¹¹⁸⁵ See, for example, Datatilsynet (Norwegian DPA), Decision n°20/01790, 22 December 2020, available [here](#); APD/GBA (Belgian DPA), Decision n°42/2020, 30 June 2020, available [here](#); ANSPDCP (Romania), Press release of 30 July 2021 regarding a decision fining a natural person for publishing personal data of other individuals on Facebook (no reference number), available [here](#); UOOU (Czech Republic)? Decision n° UOOU-05284/19-47, 28 May 2021, available [here](#); APD/GBA, Decision n°71/2020, 30 October 2020, available [here](#).

prevail over such legitimate interests. In that context, DPAs are bound to review the balancing test that the controller was supposed to conduct, before assessing whether the different rights and interests at stake have properly been considered. Indirectly, this enables them to also balance the legitimate interest of the controller, on the one side, and the rights and freedoms of the concerned data subjects, on the other side, before determining whether Article 6(1)(f) GDPR could indeed be used as a valid legal basis.

By critically comparing these different approaches while keeping the FRO of EU data protection law in mind, it appears that the approach adopted by the Icelandic DPA in its decision n°2020010552 runs contrary to EU data protection law. Indeed, the tasks and competences of DPAs as described in the GDPR clearly indicate that DPAs are in charge of applying and enforcing data protection rules, including rules which call for a balancing test between the interests of controllers and the rights and freedoms of data subjects or of third parties. It can therefore be concluded that the refusal of the Icelandic DPA to render a binding decision in that case – whether in favour of the freedom of expression of the father, or the right to privacy of the mother and of the child – does not find its source in the GDPR itself, but rather in external factors pertaining to the specific organization, practices and legal culture of the Icelandic legal system. The restrictive approach adopted by the AEDP – even if more protective for the data subjects – can also be criticized to some extent, given that nothing in the GDPR indicates that only ‘consent’ can be used as a valid legal basis for the publication of pictures on social media. Once again however, this restrictive approach does not find its source in the text of the GDPR itself, but rather in the interpretation that is made of it by the AEDP in light of national law and practices.¹¹⁸⁶ By contrast, the in-between approach adopted by other DPAs seems more in line with the GDPR. It offers indeed the possibility to protect the rights and freedoms of data subjects, including their right to privacy, while allowing controllers to pursue their legitimate interest, exercise their freedom of expression. It also confirms that the diverging approaches of DPAs in that respect do not find their origin in an internal factor intrinsic to the legal text of the GDPR, but rather in external factors. Yet, it can also be regretted that the GDPR does not contain any specific provision requiring DPAs to thoroughly investigate and rule on cases where one or multiple rights or freedoms of data subjects appear to be infringed, including cases where a balancing of diverging interests, rights and freedoms would be necessary. This, indeed, would prevent DPAs from declaring themselves incompetent, as the Icelandic DPA did. Furthermore, to increase the legitimacy of DPAs when ruling on fundamental rights issues in general, it would have been advisable to explicitly require DPAs to appoint several members with expertise in the field of fundamental rights law, and to require existing members to be trained to that end. These

¹¹⁸⁶ In particular, under Spanish law, more restrictive grounds apply for the processing of personal images. The right to one’s image has been protected for decades in the Spanish constitution and the limits to its commercial exploitation have been regulated by the Spanish Organic Law 1/1982, of May 5, on the Civil Protection of the Right to Honour, Personal Privacy and Self-Image ('the Self-Image Law').

recommendations will be included in the Conclusion of this study, along with other recommendations to boost the functionality of the GDPR with respect to its FRO.

3.3.2.5. National courts as the last bastion for enforcement: focus on GDPR mechanisms facilitating the exercise of the right to an effective judicial remedy

The Schrems saga discussed above illustrates how EU data protection law can be interpreted in a way that is beneficial for the right to an effective judicial remedy of the data subjects. In that case indeed, the CJEU took the view that such right could not be guaranteed once personal data would be transferred towards the US, as it would be too costly or burdensome for data subjects to start legal proceedings in the US against infringers. In particular, the CJEU found that *“legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.”*¹¹⁸⁷ While this case concerned infringements taking place on the US territory, it is important to take one step back and first look at how functional the GDPR really is with respect to its enforcement in the EU by national courts and tribunals.

Article 79 GDPR provides that, *“[w]ithout prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority (...), each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.”* Article 80 GDPR, discussed here above, also gives the possibility for not-for-profit entities to bring judicial proceedings against an infringer when one or more rights of data subjects deriving from the GDPR have been infringed. In parallel, Article 78 GDPR envisages the scenario where a data subject decides to bring judicial proceedings against a DPA, either because the latter has rendered a legally binding (unfavourable) decision concerning them, or because the DPA has not properly handled their complaint (including, for example, when a DPA fails to inform the data subject within three months on the progress or outcome of the procedure). Finally, Article 58 GDPR stipulates that DPAs themselves have the possibility to bring infringements of the GDPR to the attention of the judicial authorities of their Member State, including by initiating legal proceedings against a controller if it appears that the latter is not respecting EU data protection law, or a binding decision that the DPA itself has rendered.¹¹⁸⁸ Read together, these Articles therefore confirm and recall the important role that courts can ultimately play for the enforcement of the GDPR and the protection of data subjects’ rights in general.

¹¹⁸⁷ CJEU, *Schrems I*, Case C-362/14, para. 95.

¹¹⁸⁸ Article 58(5) GDPR.

This section, after highlighting the different chains of enforcement which can be formed with or without the intervention of national courts, will focus on specific provisions within the GDPR which, in the opinion of the author, partly facilitate access to justice for data subjects, and thus indirectly contribute to the fulfilment of the FRO of the GDPR.

As already discussed above, rather than being organised as a pyramid, the enforcement system of the GDPR resembles more a multi-actor network, each with their specific role, powers and competences. Within this network, a data subject or a not-for-profit entity could thus decide to ‘skip’ the possibility to file a complaint with a DPA, and directly refer a case to the national courts.¹¹⁸⁹ Both Article 78 and 79 GDPR indeed stipulate that the data subject’s right to an effective judicial remedy against a controller, a processor or a DPA is “*without prejudice to any available administrative or non-judicial remedy*”. In the event of an alleged infringement of the GDPR by a controller or a processor, data subjects therefore have the choice to either lodge a complaint with a DPA or to bring proceedings before the competent courts, or – if national law allows for it – to pursue both options at the same time. Hypothetically, the same alleged infringement of the GDPR could thus be subject to both administrative and judicial proceedings in parallel to one another.¹¹⁹⁰ While DPAs and courts often support each other within the enforcement network of the GDPR, they may thus also compete with one another and have diverging opinions on a case.

It is important to note in this respect that the GDPR does not foresee any rules on how to handle contradictory decisions by a DPA and a court, and does not discuss the binding effect of a decision rendered by a DPA for a court, or vice versa.¹¹⁹¹ By default, this type of issue therefore needs to be addressed in light of Member State procedural law, in accordance with the principle of procedural autonomy, which stipulates that in the absence of specific provisions of EU law, Member States remain free to establish their own national procedural rules to govern the exercise of EU law.¹¹⁹² In all Member States, judicial courts are considered as bodies of higher instance than DPAs since they can, *inter alia*, overturn DPAs’ decisions. As a result, in the event of contradictory decisions between a DPA and a national court, national courts would ultimately have the final say on the matter, in the sense that their decision can depart and ultimately prevail over the one of the concerned DPA. The GDPR makes it clear indeed that the independence of DPAs should not mean that the latter are not subject to judicial review.¹¹⁹³ Rather, every time a DPA does not properly fulfil its tasks or renders a binding decision, such omission or action usually

¹¹⁸⁹ Article 79 GDPR.

¹¹⁹⁰ Martini M. (2021). Article 79 GDPR, margin number 12. Paal, B. & al. (eds). *Datenschutz Grundverordnung Bundesdatenschutzgesetz*. C.H. Beck.

¹¹⁹¹ Schrems, M. (2018). Article 79 GDPR, margin numbers 25 to 28. Knyrim (ed.). *Der DatKomm online. Praxiskommentar zum Datenschutzrecht – DSGVO und DSG*. MANZ Verlag.

¹¹⁹² *Ibid.*

¹¹⁹³ Recital 118 of the GDPR.

gives rise to judicial review by the courts of the concerned Member State.¹¹⁹⁴ In the event a DPA, for example, fails to handle a complaint in due time or renders a decision finding that no infringement has been committed, the data subject(s) concerned may decide to challenge such inaction or decision by initiating judicial proceedings against the behaviour or decision of the concerned DPA.¹¹⁹⁵ In the same vein, if a decision is rendered by a DPA against a controller, the latter may challenge such a decision, including the coercive measures adopted by the DPA or the amount of the administrative fine that was imposed on it.¹¹⁹⁶

Taking the above into account, national courts and tribunals undeniably play an important role within the enforcement network of the GDPR. They can be considered as the ultimate bastion for enforcement – keeping in check controllers and processors, but also DPAs. And they may of course – as part of their analysis and in their decisions – pay due regard to the impact that any litigious data processing practice can have on the fundamental rights and freedoms of data subjects, as guaranteed by the constitution of their Member State, by the Charter, the ECHR or by any other relevant legislation. Yet, one must admit that access to justice in most Member States is often problematic; the costs associated with judicial proceedings, the length of judicial procedures, the difficulty sometimes to fulfil or adapt to procedural requirements as well as issues relating to applicants’ *locus standi*, jurisdiction or competence are well-known factors that may deter individuals, not-for-profit entities or DPAs from bringing a case to the attention of the courts in the first place. How Member States organise their own judiciary and may improve access to justice in general is however far beyond the intended scope of this study, since these considerations are external to the text of the GDPR itself. In this respect, it must also be noted that the EU has a very limited capacity to impose changes to the organisation of national courts and tribunal in light of the principle of conferral and the principle of procedural autonomy.¹¹⁹⁷ As a result, even if access to justice should be subject to improvement among the EU Member States,¹¹⁹⁸ the EU legislator has little room for manoeuvre in this respect. The question remains, however, how the EU legislator has used its limited room for manoeuvre to make the GDPR as ‘functional’ as possible with respect to access to justice by looking into specific provisions of the GDPR. Hence, this section will focus on specific elements of Article 78 to 82 of the GDPR and discuss to what extent these elements contribute to the functionality of the GDPR for achieving its FRO.

Article 79(1) GDPR stipulates that data subjects have the right to an “effective” judicial remedy. The right to an effective judicial remedy is a fundamental right in

¹¹⁹⁴ Recital 129 GDPR. See also Articles 78 and 79 GDPR.

¹¹⁹⁵ Recital 143 GDPR.

¹¹⁹⁶ Article 58(4) GDPR.

¹¹⁹⁷ CJEU, Judgment of 16 December 1976, *Rewe*, Case C33/76.

¹¹⁹⁸ European Union Agency for Fundamental Rights (2011). Report: Access to Justice in Europe: an overview of challenge and opportunities. https://fra.europa.eu/sites/default/files/fra_uploads/1520-report-access-to-justice_EN.pdf, p. 65.

itself, enshrined in Article 47 of the Charter. This right implies that everyone whose rights under EU have been violated is “*entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal (...)*”. It also implies that the claimant has “*the possibility of being advised, defended and represented*” before that court or tribunal. In light of Article 47 of the Charter, access to courts under Article 79 GDPR must therefore not be disproportionately difficult, for example through excessively strict admissibility requirements.¹¹⁹⁹ It must be noted however that nothing in this Article refers in particular to the fundamental rights and freedoms of individuals that may have been infringed as a result of the processing of their personal data. On the contrary, the material scope of this Article seems limited to situations where the right of a data subject *under the GDPR* has been infringed *as a result* of a non-compliant processing activity. Two conditions therefore seem attached to the exercise by data subjects of their right to an effective judicial remedy under Article 79(1) GDPR: first, a controller or processor must have processed their personal data in a non-compliant way (for example, because consent was required under Article 9 GDPR but never obtained, or because of the non-respect of one of the key principles of data processing under Article 5 GDPR). Second, there must be a causal link between this non-compliant processing operation and the fact that one of the rights of the concerned data subjects under the GDPR has been infringed, such as the right to access, the right to erasure, or the right to object to the processing.¹²⁰⁰ A strict reading of Article 79(1) GDPR could thus limit the situations where data subjects would be entitled to an effective judicial remedy. As an example, if a controller does not answer an access request from a data subject, one could consider that their right to access under Article 15 GDPR has been violated; yet, if the controller actually does not process *any* personal data about that person (but does not inform the latter about it), this absence of processing could defeat the application of Article 79(1) GDPR, which requires an actual processing operation to take place. Similarly, there may be a situation where a controller or processor does not process personal data in compliance with the GDPR (for example, by failing to maintain a record of processing activities up-to-date, or by failing to conduct a DPIA), without such processing resulting *per se* in a direct violation of one of the rights of a data subject under the GDPR. A restrictive reading of Article 79(1) GDPR could thus render this provision dysfunctional for the protection of data subjects’ rights and go against the general objective of the GDPR and of Article 47 of the Charter. In the opinion of most scholars however, with whom the author of this study agrees, Article 79(1) GDPR should be interpreted through teleological approach, whereby any violation of the GDPR which can potentially *affect* data subjects’ rights would trigger its application.¹²⁰¹ This non-restrictive reading is further supported by the

¹¹⁹⁹ Mundil D. (2020). Article 79 GDPR. Wolff & Brink (eds). *BeckOK Datenschutzrecht*. C.H. Beck.

¹²⁰⁰ Kreße B. (2018). Article 79 GDPR, margin number 4. Sydow (ed.). *Europäische Datenschutzverordnung*. Nomos.

¹²⁰¹ Jahnelt D. (2021). Article 79 GDPR, margin number 29. Jahnelt, D. (ed.). *DSGVO*. Jan Sramek; Bergt, M. (2020). Artikel 79 GDPR, margin number 24. Kühling & Buchner (eds). *DS-GVO BDSG*. C.H. Beck; Boehm, F. (2019). Article 79 GDPR, margin number 10. Simitis, Hornung, Spiecker & Döhmann (eds). *Datenschutzrecht*. C.H. Beck.

judgment of the CJEU in the case *Meta v. BVV*, where the CJEU gave a non-restrictive interpretation to Article 80(2) GDPR by confirming that not-for-profit associations could bring proceedings against an infringer on behalf of data subjects, without it being necessary to prove actual harm suffered by a group of data subjects because of the infringement of their rights.¹²⁰² All in all, Article 79(1) GDPR seems to support the overall idea that Member States must ensure the respect of Article 47 of the Charter in the context of data protection litigation. Yet, arguing that this provision contributes to the functionality of the GDPR with respect of its FRO would, in the opinion of the author, be exaggerated. As pointed out above indeed, this provision does not provide for an *enhanced* right to an effective judicial remedy in the event a processing would, for example, violate one of the fundamental right or freedom of a data subject.

A more apparent facilitation mechanism with respect to the enforcement of the GDPR before national courts relates to the choice of jurisdiction. Under Article 79(2) GDPR indeed, proceedings against a controller or a processor can be brought either before the courts of the Member State where the controller or processor has an establishment, or, alternatively, before the courts of the Member State where the data subject resides. There is no doubt that this second possibility facilitates the exercise of the right to access to an effective judicial remedy since data subjects will not have to ‘chase down’ the infringer by bringing proceedings before the courts of a different Member State than the one where they live – which would often increase the level of difficulty of such endeavour mainly because of additional costs, language barrier and/or procedural differences. There exists, however, one exception to this facilitation mechanism: in the event the defendant would be a public authority of a Member State “*acting in the exercise of its public powers*”,¹²⁰³ the data subject has no other choice but to bring proceedings before the competent court of the Member State where that public authority is located. This includes proceedings against a DPA itself.¹²⁰⁴ Besides this exception, the fact that, in all other situations, data subjects are allowed to seek judicial remedies in their own Member States, regardless of where the controller or processor is located, can be seen as a factor of functionality of the GDPR, given that it facilitates access to justice in general. Hence, this facilitation mechanism contributes, at least indirectly, to the fulfilment of the FRO of the GDPR. Indeed, courts are not limited to the enforcement of data protection law *per se*, like DPAs; they can analyse and rule on different legal issues in the context of a dispute between a data subject and a controller or processor, including fundamental right interferences, either via the prism of EU data protection law, or other legislation, such as consumer protection law, anti-discrimination law, labour law, their own constitution, or the Charter. Of course, not all national courts rely on fundamental right instrument to interpret EU data protection law, or vice-versa; this

¹²⁰² See Section 3.3.2.3 of this study, here above.

¹²⁰³ Article 70(2) GDPR, last sentence.

¹²⁰⁴ Article 78(3) GDPR specifically provides: “*Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.*” The EU legislator had to allow for this exception to respect the sovereignty of Member States and of the bodies that represent them.

may vary depending on the jurisdiction, the level of instance, and the Member State concerned.¹²⁰⁵ Whether courts really exploit that possibility in the end belongs to elements that are external to the text of the GDPR. Hence, analysing, for example, the use that national courts make of the Charter when applying EU data protection law would go beyond the scope of this study. What remains relevant however is to highlight the functional role that Article 79(2) GDPR can play by facilitating access to justice by data subjects, including in cases where a processing operation would infringe not only their data protection rights but also a fundamental right. To exemplify this, one may refer to the decision of the Icelandic DPA in which the complainant (i.e., a mother and her child whose pictures had been disseminated on Facebook, without their consent, by the father of the child) were redirected towards the national courts, so that the latter could take into consideration the conflicting fundamental rights of all the parties involved before taking a final decision on the lawfulness of the processing at stake.¹²⁰⁶ Even if the defendant in that case (i.e., the father of the child) would have moved to another country, the complainants would have still had the possibility to bring judicial proceedings before the Icelandic courts to obtain an injunction, in line with Article 70(2) of the GDPR.

Another provision which may further enhance the enforcement of the GDPR by national courts for the benefit of data subjects' rights and freedoms is Article 80 GDPR, and in particular Article 80(2), already discussed above. There is no doubt indeed that allowing not-for-profit entities to represent a group or category of data subjects before national courts, even in the absence of any mandate, and without having to prove an actual harm suffered by these data subjects because of the violation of one of their subjective rights under the GDPR, may boost the number of collective redress actions for the benefit of a large number of individuals. The CJEU has further confirmed in this respect that nothing prevents those not-for-profit entities to bring an action not only based on data protection law, but also on another legislation when the infringement at stake (also) involves the processing of the personal data.¹²⁰⁷ Hence, beyond privacy and data protection, different fundamental rights may benefit from such representative actions – such as consumer protection or non-discrimination – without the data subjects having to be actively involved in the enforcement process. This is of course particularly relevant for the fulfilment of the FRO of EU data protection, as already highlighted above. It cannot be denied however that the functionality of Article 80(2) GDPR is dependent on the national procedural law of Member States, given that Article 80(2) GDPR is a so-called 'opening clause', leaving to Member States full discretion as to whether allowing such a system.¹²⁰⁸ Some Member States may thus impose strict procedural

¹²⁰⁵ With respect to the use of the Charter, for example, see Porcedda, M. G. (2017). *op. cit.*

¹²⁰⁶ Persónuvernd, Mál nr. 2020010552, 17 November 2021, <https://www.personuvernd.is/urlausnir/kvortun-yfir-birtingu-ljosmynda-a-samfelagsmidli-visad-fra>.

¹²⁰⁷ CJEU, Judgment of 28 April 2022, Case C-319/20 *Meta Platforms Ireland*, paras. 77-84.

¹²⁰⁸ Miscenic, E. & Hoffmann, A.-L. (2020). The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation. *EU and comparative law issues and challenges series*, 2020:44-61.

requirements which may create barriers to the enforcement of the GDPR by not-for-profit associations, or even worst not make use of that possibility at all. This is where the synergies between Article 79 and 80 of the GDPR becomes particularly relevant; theoretically, a not-for-profit association based in Austria could decide to seek judicial remedies before the Dutch courts in the Netherlands if the applicable law on collective redress in that country is more favourable, either because the controller would have an establishment in the Netherlands, or because some of the data subjects concerned by the infringement reside in that country.¹²⁰⁹

Another relevant article which, in the opinion of the author, contributes to the functionality of the enforcement system of the GDPR is Article 82(4) of the GDPR. This Article was already discussed within Section 3.1.3.2(iii)(d) of this study, with respect to the accountability obligations of controllers. As a reminder, according to Article 82(4) GDPR, when multiple controllers and/or processors are involved in the same litigious processing activities, each of them may be held liable for the entire damage towards the data subjects. This provision is meant to facilitate the exercise of the right to an effective judicial remedy since it allows the plaintiffs to limit the personal scope of their judicial action while preserving the right to compensation of data subjects. Data subjects who have suffered from a damage may thus request full compensation from one controller instead of having to file multiple claims against each potential infringer.

All these different mechanisms, once considered together and appreciated within the whole enforcement network of the GDPR, undeniably facilitate the exercise of the right to an effective judicial remedy and to compensation of data subjects. This, in turn, may contribute to the fulfilment of the FRO of EU data protection law, given that courts generally have jurisdiction to rule on fundamental rights issues, including interference with DFR such as non-discrimination or consumer protection in the context of the personal data processing. As far as the FRO of EU data protection law is concerned, Article 80 of the GDPR could drastically increase the functionality of the framework by allowing for collective redress, depending on how Member States implement it. This model of representative actions can indeed catalyse the efforts of civil society and other enforcement actors, thereby increasing the possibility to hold controllers or processors liable and accountable for their actions or omissions, including when the data processing practice at stake infringes data subjects' fundamental rights and freedoms. This facilitation mechanism is thus particularly likely to contribute to the fulfilment of the FRO of EU data protection law. As noted at the very beginning of this section however, access to justice in the different Member States may remain challenging because of various external factors pertaining to national law, since the organisation of the judiciary generally fall outside of the ambit of EU law. On top of that, one of the most functional provisions

¹²⁰⁹ Article 80 of the GDPR indeed specifically refers to the possibility for a not-for-profit entity to exercise the right of data subjects under Article 79 GDPR, without excluding Article 79(2) GDPR on the choice of jurisdiction.

of the GDPR for the enforcement of data subject's rights on a large scale – Article 80 GDPR – is an opening clause that Member States may either embrace or ignore. It is to be feared that the discrepancies that will persist from one Member State to another with respect to data protection-related representative actions will thus undermine harmonisation, legal certainty, and thus ultimately the effectiveness and functionality of the GDPR.¹²¹⁰ Once read in combination with Article 79 GDPR, however, it appears that the disharmonising effect of this opening clause may be tempered by the possibility for no-for-profit entities to choose among various jurisdictions when initiating such a representative action before national courts. This may, in the long run, lead to the creation of 'litigation hubs' in those Member States that allow for collective redress in the field of EU data protection law. If the courts of a Member State, in the context of collective action, declare a specific DDT or data processing practice unlawful, not only the data subjects residing in that Member State may benefit from it, but all present and future data subjects who are or could have been similarly affected by it. Hence, there is no doubt that despite being an "opening clause", Article 80 GDPR remains a functional tool that is likely to significantly contribute to the fulfilment of the FRO of EU data protection law in the future.

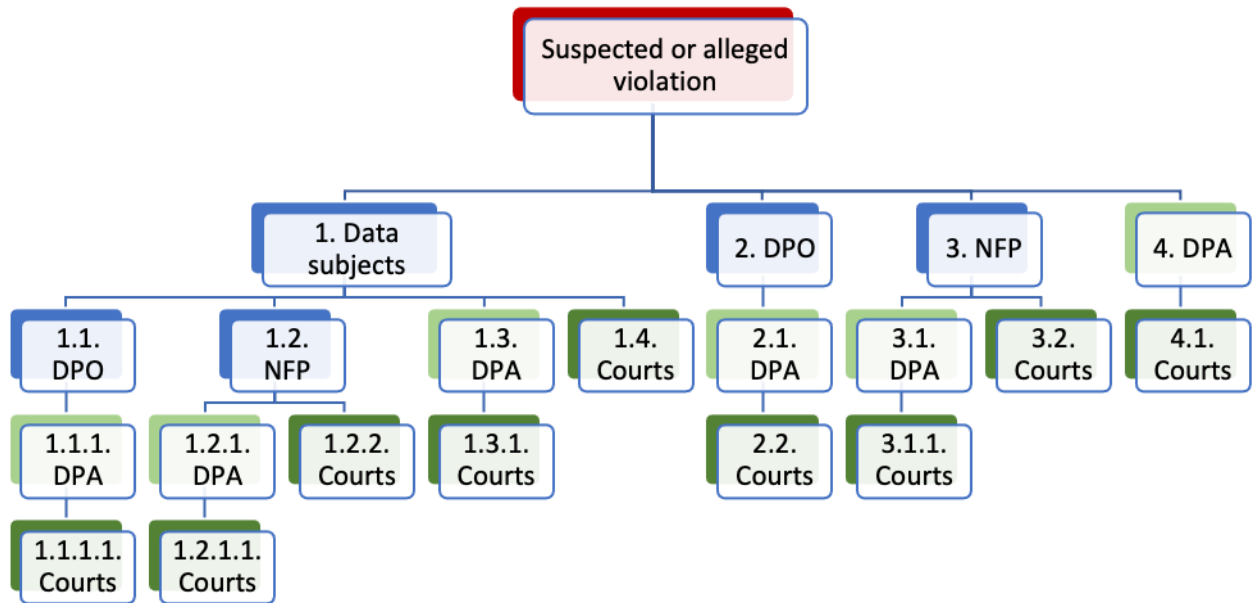
3.3.3. Concluding remarks: the multi-actor enforcement system of the GDPR as a double-edged sword for the protection of the fundamental rights of data subjects

The below table gives an overview of the different chains of enforcement that can put into motion within the decentralised, multi-actor enforcement system of the GDPR.

TABLE 9

In this table, each enforcement chain has a number. The actors with a blue colour, such as data subjects or not-for-profit entities ('NFP'), may not render a binding decision but may bring the violation to the attention of another actor with corrective powers, marked in green, i.e., DPAs and national courts. The courts may include civil, administrative or criminal courts, depending on the facts of the case and the applicable national law.

¹²¹⁰ On this point, the author fully agrees with Miscenic and Hoffmann. See Miscenic, E. and Hoffmann, A.-L. (2020). *op. cit.* pp. 55-56.



As shown by this model, a binding decision can already be rendered at the very first level of this network, in the event a DPA starts an investigation of its own volition and renders a binding decision against a controller (cf. enforcement chain n°4). It may be the case, however, that a violation is first detected by a data subject (enforcement chain n°1), a DPO (enforcement chain n°2) or a not-for-profit entity (enforcement chain n°3). In the event the controller or processor, despite having been informed of the situation, decides not to act, the concerned actor may then trigger the next level of the enforcement chain, which may ultimately lead to a binding decision being rendered by a DPA and/or a court.

From the perspective of the functionality of EU data protection law, the existence of alternative chains of enforcement offers more chance of success and flexibility, in the sense that a violation of the GDPR can be noticed from different angles by a variety of actors, who may in turn trigger the enforcement chain which they consider the most fitting to the case. On top of that, different provisions of the GDPR are meant to facilitate enforcement by simplifying procedural rules or encouraging cooperation between these different actors. In particular, the following provisions (most of which have already been discussed within this study) can be listed:

- The facts that data subjects may trigger an enforcement chain by bringing a violation to the attention of a DPO, a not-for-profit entity or a DPA, without having to invest any personal resources (Article 77 and 80 GDPR);
- The fact that a data subject may choose between lodging a complaint with a DPA in the Member State of his, her or their habitual residence, place of work or place of the alleged infringement (Article 77(1) GDPR);

- The fact that DPAs are under the obligation to facilitate the filing of complaint, for example by providing an online form on their website for that purpose (Recital 141 and Article 57(2) GDPR);
- The fact that DPOs, despite being subject to strict obligations of confidentiality and secrecy with respect to the data processing practices of their controller or processor, may still address their concern to a DPA in the event of a persistent violation, and can therefore play the role of compliance informers (Article 39(1)(e) GDPR);
- The fact that not-for-profit entities – especially entities already specialised in the protection of fundamental rights and freedoms – may be mandated by data subjects in the context of a representative collective action to put an end to a violation (Article 80(1) GDPR);
- The fact that not-for-profit entities can also decide to act against a violation of the rights of data subjects, independently from any specific mandate, in any Member State providing for this possibility (Article 80(2) GDPR);
- The fact that DPAs have been given extensive investigative and corrective powers to ensure the protection of “*the fundamental rights and freedoms of natural persons in relation to processing*”, including DFR (Article 51(1) GDPR);
- The fact that data subjects or not-for-profit entities can bring an action against a DPA that would not properly fulfil its tasks, so that DPAs are being held accountable for their (lack of) actions (Article 78 GDPR);
- The fact that data subjects (or a not-for-profit entity on their behalf) may decide to submit a case before the courts of the Member State where the controller or processor has an establishment or where the data subject has his, her or their habitual residence (Article 79(2) GDPR);
- The fact that co-controllers are considered jointly liable before national courts and may each be ordered to compensate the data subject(s) in full (Article 82(4) GDPR).

On the basis of the above considerations, it can generally be argued that the multi-actor enforcement system of the GDPR is a third important pillar for the effectiveness and functionality of the entire framework with respect to its FRO. Yet, it cannot be denied that enforcement remains often challenging in practice, also because of the multitude of actors involved in the process and the lack of harmonization at the national level. In that sense, this multi-actor system can be seen as a double-edged sword, which can be functional to combat harmful data

processing practices, but which can also turn into a procedural labyrinth, especially in the context of cross-border cases involving several DPAs. As a result, concerns over GDPR enforcement have been voiced by all relevant actors across the board, including most EU institutions and agencies, such as the European Parliament,¹²¹¹ the Commission¹²¹², the EDPS,¹²¹³ and the EDPB.¹²¹⁴

While being illustrative of general enforcement issues, these shared concerns may however also be seen as a confirmation that many actors are actively using the GDPR, identifying remaining weaknesses, and willing to improve the overall system. The EDPS recently positioned itself as a moderator of this debate by organising a conference on the enforcement of the GDPR, with the explicit objective to “*encourage a discussion on the different approaches to enforcement action, and facilitate the sharing of experiences on best practices and systemic challenges in enforcement.*”¹²¹⁵ In parallel, many NGOs experiencing procedural enforcement issues (mostly due to the lack of budget of DPA or incompatibilities with national procedures) have taken steps to denounce these issues and formulate recommendations on how to improve the system, so as to ensure that the effectiveness of the GDPR in practice.¹²¹⁶

In that context, it clearly appears that the role of data subjects, DPOs, not-for-profit entities and DPAs have become more relevant than ever for identifying internal or external factors of dysfunctionality. The fact that these actors are making active use of various enforcement mechanisms, have detected practical issues, and are pushing for improvements also suggest that the GDPR is functional, even if some external factors are currently impeding this functionality.¹²¹⁷ In other words, the fact that the addressees of the GDPR are actively seeking to improve existing enforcement procedures can be seen as a sign that they have been using the framework and want to use it even more in the future. Furthermore, the relation between each of these actors – whether cooperative or competitive – is likely to continue bringing to light procedural and practical issues, encourage critical discussions and steer

¹²¹¹ European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)).

¹²¹² See Commission Vice President Věra Jourová statement: Manancourt, V. (2021, December 2). Top EU official warns privacy rules may need to change. *Politico*. <https://www.politico.eu/article/eu-privacy-regulators-clash-gdpr-enforcement/>.

¹²¹³ EDPS Conference 16-17 June 2022. The Future of Data Protection: effective enforcement in the digital world.

¹²¹⁴ EDPB (2022, April 28). Statement on Enforcement Cooperation. https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf

¹²¹⁵ Manancourt, V. (2021, December 2). *op. cit.*

¹²¹⁶ See, inter alia: Massé Estelle (2022). Four years under the EU GDPR. How to fix its enforcement. *Access Now*. <https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf>; *noyb* (2022, January 23). Data Protection Day: 41 Years of "Compliance on Paper"?! <https://noyb.eu/en/data-protection-day-41-years-compliance-paper>. Similarly, the NGO *noyb* is currently setting up a working group to develop a GDPR Procedural Regulation to suggest the adoption and implementation of new rules to ensure the effectiveness and functionality of the GDPR enforcement system (information obtained from *noyb* directly, as the author of this study has been invited to be part of this Working Group in September 2022).

¹²¹⁷ *Ibid.*

improvements.¹²¹⁸ Against this background, potential solutions to enforcement issues, and in particular the possibility to centralize enforcement in the context of pan-European litigation, will be part of the recommendations formulated at the end of this study.

¹²¹⁸ As an illustration, in September 2022, the author of this study joined a working group made of members of the University of Luxembourg (i.e., Prof. Herwig Hofmann, Lisette Mustert and the author herself) and of the not-for-profit association *noyb* (i.e., Maximilien Schrems, Romain Robert and Marco Blocher) with a view of drafting a procedural regulation that could complement the GDPR and solve the most pressing enforcement issues in the context of the OSS mechanism. The publication of this draft regulation, along with other studies and documents published by other actors such as the EDPB, the EDPS or *Access Now* illustrate the motivation of various actors to steer improvements.

CHAPTER 4 – TESTING THE MULTI-FUNCTIONALITY OF THE GDPR FOR THE DEFENCE OF DIFFERENT FUNDAMENTAL RIGHTS

Foreword

In the Introduction of this study, the author already discussed the impact that modern DDTs can have, in general, on the fundamental rights and freedoms of data subjects. It has already been shown that DDTs have infiltrated almost all aspects of human life and may thus virtually affect *all* the rights or freedoms of the data subjects, well beyond privacy and personal data protection. In order to assess the extent and limit of the multi-functionality of EU data protection law in addressing the challenges raised by those modern DDT, the author has selected two types of data processing practices that have already proven to be harmful to DFR.

There are, of course, numerous data processing practices and data-driven technologies that can violate the fundamental rights of the data subjects, as exemplified in the first Chapter of this study. One may cite, just to name a few: the use of cameras or drones equipped with facial-recognition software for mass surveillance purposes; illegal geo-blocking preventing individuals from a certain region to gain access to products, services or information; the use of behavioural micro-targeting techniques for manipulating people's opinion in the context of a political campaign; the discrimination of individuals on the basis of profiling in the context of the provision of goods or services (e.g. price discrimination on Bookings ; housing advertising discrimination on Facebook; etc) or ; the occurrence of illegitimate censorship through automated content moderation on social media. It would be neither practical nor necessary however to test the multi-functionality of EU data protection law with respect to each and every potential harmful data processing practice which exist or may exist in the future. Rather, it suffices to select one or two different practices, involving different sectors, categories of actors and fundamental rights, in order to test (the limits of) the functionality of EU data protection law, learn from these examples and be able to draw more general conclusions.

For the sake of relevance and practicability, the author has decided to focus on the two following data processing practices in particular:

- 1) **online harassment practices**, which may violate human dignity and the right to mental integrity of the data subjects concerned, or interfere in some instances with their freedom of expression; and

2) e-recruitment practices, which may violate the right to equal treatment or non-discrimination of the data subjects.

It is not by accident or random choice that these two data processing practices have been selected by the author. Rather, this selection is the result of a reflection on the prevalence and the negative impact of these practices. In particular, three criteria have been considered in the selection of each of these two ‘test-areas’.

First, it must be noted that the selected data processing practices have each already proven to pose concrete and serious risks to the rights and freedoms of data subjects in the EU. These risks are not merely hypothetical but have already materialised, as reflected in a series of recent affairs reported by the media as well as various reports, studies and academic works published by EU institutions, agencies or scholars. In other words, the practical impact of these practices should not be underestimated, as they have already – and sometimes deeply – infiltrated and impacted our society. Beyond their theoretical relevance for testing the hypothesis formulated in this study, understanding how to prevent or minimize the harmful effects of these data processing practices is thus also important from a societal point of view.

Second, each of these practices takes place in very different contexts involving (i) different data-driven technologies (i.e., software allowing content sharing on social media vs. smart algorithms used for decision-making purpose; etc.); (ii) a different constellation of concerned actors (i.e., interactions among private individuals on social media vs interactions between a private individual and a private or public entity for the purpose of recruitment); and (iii) interferences with different fundamental rights of the data subjects (i.e., human dignity, mental integrity, and freedom of expression vs non-discrimination). Those two ‘test areas’ therefore offer a diverse sample when it comes to the impact that DDT can have on data subject’s fundamental rights and freedoms. Such diversity is necessary given that the aim of this study is to test and find ways to enhance the *multi*-functionality of EU data protection with respect to its broad FRO.

Third, each of these practices may be representative of *other* data processing practices which share identical or similar means, which involve an identical or similar combination of actors, and which pursue similar or distinct objectives. Consequently, any reflections on how to enhance the multi-functionality of EU data protection law in those ‘test areas’ may, by analogy, also be relevant for preventing the harmful effects of similar yet separate data processing practices. For example, the considerations made with respect to discrimination deriving from the use of algorithmic decision-making in the field of e-recruitment can also be relevant with respect to the use of algorithmic decision-making in the context of e-criminal justice, e-banking, e-policing, e-insurance, e-health, etc. In other words, the selected

practices can be used as representative models that may be duplicated *mutatis mutandis* to a wider range of situations.

Regarding the structure of this Chapter, within each test area, the author will first present a real case-study as a way to illustrate the effects of the data processing practice at stake; as a second step, the author will then generally define what falls within and without the concerned data processing practice; as a third step, the author will discuss the harmful effects that such practice can have on the fundamental rights of the data subjects concerned (this includes a comparison with the offline equivalent of each practice); as a fourth step, the author will provide a very brief overview of the existing legal tools against those practices and their main weaknesses besides EU data protection law; and, as a final step, the author will test how functional the GDPR is or could be for protecting the fundamental rights of the data subjects in each of these test areas.

As a final preliminary remark, the author of this study would like to clarify that the purpose of this Chapter is *not* to prove or disprove the functionality of the GDPR in an absolute manner. This Chapter is indeed not exhaustive enough to demonstrate that the GDPR is a multi-functional tool that can be used in *any* situation with a high degree of success. Rather, the purpose of this Chapter is to provide an illustration of some of the multi-functional aspects of the GDPR in at least two different test areas. The considerations and conclusions that will be drawn from these two examples can then serve as a basis to imagine other areas where the GDPR could prove functional for the protection of fundamental rights and freedoms, and to formulate general recommendations on how to approve such (multi-)functionality.

4.1. HUMAN DIGNITY, INTEGRITY AND FREEDOM OF EXPRESSION IN THE CONTEXT OF ONLINE HARASSMENT

The case of Julie Hainaut

On 12 September 2017, Julie Hainaut, a French journalist, published an article in the weekly cultural magazine *Le Petit Bulletin* about her experience in a newly opened cocktail bar in Lyon.¹²¹⁹ The bar was named *La Première Plantation* in reference to the plantations of cane sugar from which rum is made. When Julie Hainaut interviewed the two bar managers about that name that they had chosen, the latter made questionable comments regarding the French colonialist period, which they described as having “*a cool spirit, a time where people were good at entertaining*”.¹²²⁰ After the publication of the article, many readers expressed their indignation regarding the statements made by the two bar managers. In view of this

¹²¹⁹ Hainaut, J. (2017, September 12). La Première Plantation, où l’art de se planter. *Le Petit Bulletin*. <http://www.petit-bulletin.fr/lyon/guide-urbain-article-58700-La+Premiere+Plantation++ou+l+art+de+se+planter.html>.

¹²²⁰ *Ibid.* (In French in the original text: “*un esprit à la cool, une époque où l’on savait recevoir.*”)

'bad buzz', the managers apologized for their inappropriate use of words and clarified that their intention had never been to glorify the colonialist period.¹²²¹ At the end of the day, however, it was not the bar managers who suffered the most from that article, but Julie Hainaut herself. Her article was indeed picked up by *Démocratie participative*, a virulent neo-Nazi website filled with racist, sexist, xenophobic and anti-Semitic content.¹²²² In a long heinous online post, which can still be found online today,¹²²³ a man using the pseudonym "Heinrich" repeatedly insults the journalist with racial slurs.¹²²⁴ The online post mentions her full name and is accompanied by two pictures of her, copied from her social media accounts. Immediately after the publication of this post, Julie Hainaut filed a complaint with the police. This did not prevent this content from being widely shared and commented by many readers of the website *Démocratie participative*, on that website and on other social media platforms. Julie Hainaut soon became the target of hundreds of violent, insulting and/or threatening messages, including death threats and rape threats.¹²²⁵ The scope and frequency of the attacks were so important that it profoundly disrupted her life. Each time she was publishing a new article for the press, the harassers started to verbally attack her on the corresponding websites or on social media, including by insulting her or threatening to hurt, rape or kill her. In an attempt to protect herself, Julie Hainaut withdrew from certain social media. By fear of being recognised, she also stopped her master studies.¹²²⁶ Such harassment ultimately produced a deterrent effect on her willingness to publish articles under her name.¹²²⁷ For this reason, *Reporters sans frontières* and the *Syndicat national des journalistes* became parties to the criminal proceedings against her online harassers. The French criminal system however proved to be ineffective in identifying the author of the original post or stopping the attacks. All in all, the online harassment campaign against Julie Hainaut lasted more than three years. Despite the fifteen complaints filed by Julie Hainaut with the police

¹²²¹ Matthieu, H. & Desvalles, G. (2017, September 14). La Première Plantation. Droit de réponse. *Le Petit Bulletin*. <http://www.petit-bulletin.fr/lyon/guide-urbain-article-58888-Droit+de+Reponse.html>.

¹²²² On November 27, 2018, the Tribunal de Grande Instance of Paris ordered nine French telecom operators and internet service providers (SFR, Orange, Free, Bouygues and others) to block access to the website "democratieparticipative.biz" in view of its racist, antisemitic, sexist and xenophobic content. Despite this order, the website has always managed to reappear. The website is now hosted on a US server. Source: Poujol, A. (2018, January 8). Le blocage du site « Démocratie participative » prononcé en justice. Haas Avocats. <https://info.haas-avocats.com/droit-digital/le-blocage-du-site-d%C3%A9mocratie-participative-prononc%C3%A9-en-justice>.

¹²²³ Throughout 2020 and 2021, the post insulting Julie Hainaut could still be found at the following address: <https://democratieparticipative.digital/lyon-une-pute-a-negres-feministe-veut-detruire-un-bar-a-rhum-colonialiste-mobilisation/>.

¹²²⁴ Among others, the author of the post uses the terms "grosse pute" (big slut) and "pute à nègres" (negros' whores).

¹²²⁵ Untersinger, M. (2019, November 19). Julie Hainaut, harcelée sur Internet par des néonazis, attend toujours justice. *Le Monde*. https://www.lemonde.fr/pixels/article/2019/11/19/cyberharcèlement-victime-de-neonazis-il-y-a-deux-ans-julie-hainaut-attend-toujours-justice_6019680_4408996.html

¹²²⁶ Claude., C. (2020, December 16). « Bien fragiles, tout de même, tous ces hommes qui se sentent attaqués ». *Épris de Justice*. <https://www.epris-de-justice.info/bien-fragiles-tout-de-meme-tous-ces-hommes-qui-se-sentent-attaques/>

¹²²⁷ Beyond the psychological impact that such harassment has caused, Julie Hainaut explains that "the mechanism of hate leads to muzzling". Extract from a video interview : « Un procès pour ouvrir les yeux sur le cyberharcèlement », Arte, 24 November 2020, available at <https://www.arte.tv/fr/videos/101057-000-A/un-proces-pour-ouvrir-les-yeux-sur-le-cyberharcèlement/>.

over that period, only *one* individual ended up facing charges before the French criminal courts, not on ground of cyber-harassment but on ground of racist and sexist insults. While initially condemned to a conditional sentence of 6 months of prison and a 5000 EUR fine, the charges against that individual were ultimately dropped in appeal because of a statute of limitation.¹²²⁸

In the opinion of the author, the case of Julie Hainaut is representative of how online harassment may deeply impact the mental integrity and interfere with their freedom of expression of the victim. It is also representative of the dysfunctionality of traditional legislative norms in properly addressing and combatting online harassment, and in particular of provisions of criminal law against harassment or hate speech. After defining the notion of online harassment, the following sections will discuss its impact on fundamental rights and freedoms, as well as the (lack of) appropriate legal means to combat such a phenomenon. The author will then test the functionality of the GDPR to prevent or combat online harassment.

4.1.1. Defining and conceptualising ‘online harassment’

Online harassment – also sometimes called cyber-harassment or cyberbullying¹²²⁹ – is a type of harassment that occurs through the internet. There is no legal or commonly agreed definition of online harassment at the EU level.¹²³⁰ This phenomenon has however been described by the EU institutions in the context of various initiatives as “*the repeated verbal or psychological harassment carried out by an individual or a group against others through the use of online services*”.¹²³¹ Online harassment is usually considered as a synonym for, or a form of, online abuse, cyber violence or cyber-aggression.¹²³²

In the academic literature, various scholars have also attempted to define or conceptualize online harassment. With some variations, online harassment is generally understood as the use of ICTs by an individual or a group of individuals in order to cause harm to a victim who cannot easily defend themselves.¹²³³ Keeping this

¹²²⁸ Untersinger, M. (2020, December 17). Haine en ligne : relaxe en appel d’un internaute d’extrême droite à Lyon. *Le Monde*. https://www.lemonde.fr/pixels/article/2020/12/17/haine-en-ligne-relaxe-en-appel-d-un-internaute-d-extreme-droite-a-lyon_6063757_4408996.html.

¹²²⁹ The term ‘cyberbullying’ is often associated with victims of a younger age because it echoes the expression ‘school bullying’. See European Parliament (2016, August 30). Study on cyberbullying among young people. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/ IPOL_STU\(2016\)571367_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/ IPOL_STU(2016)571367_EN.pdf)

¹²³⁰ *Ibid.*, p. 21.

¹²³¹ European Commission (2009, February 10). Press release: Safer Internet Day 2009: Commission starts campaign against cyber-bullying.

¹²³² Cyber violence or cyber aggression are usually considered as synonyms. Cyber violence is usually understood as any act of violence perpetrated online. Cyber-aggression has been defined as the ‘intentional harm delivered by the use of electronic means to a person or a group of people irrespective of their age, who perceive(s) such acts as offensive, derogatory, harmful or unwanted’ (see Grigg, D. W. (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. *Australian Journal of Guidance & Counselling*, 20(2):143-156).

¹²³³ For a systematic review of the (evolving) definitions of cyberbullying and related concepts, see: Corcoran, L., Mc Guckin, C. & Prentice, G. (2015). Cyberbullying or Cyber Aggression? A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression. *Societies* 5(2):245-255.

definition in mind, online harassment can be considered as having the following characteristic elements: (i) a form of (repeated) psychological and/or verbal violence (ii) carried out by one person or a group of persons (the ‘harassers’); (iii) through the internet and the use of ICTs; (iv) with the intention to cause harm to one or multiple individuals (the ‘victims’); and (v) the victims’ relative inability to defend themselves.¹²³⁴

Taking those characteristic elements into account, and in particular the fact that the practice occurs online and that one or multiple victim(s) are targeted by the harassers, it can be concluded that online harassment generally implies, at one stage or another, the processing of personal data relating to the victim(s) by the harassers and sometimes also by third parties.¹²³⁵ These personal data may include, for example, the name of the victim, information relating to his/her/their gender, age, profession, social status, physical appearance (including through photos) or even sensitive personal data,¹²³⁶ such as information relating to the ethnicity, religious beliefs or sexual orientation of the person concerned.¹²³⁷ On this basis, the author would like to propose the following definition of online harassment for the purpose of this study: any data processing practice whereby one or multiple individuals (the harasser(s)) process, without any valid legal basis or legitimate purpose, the personal data of one or multiple data subjects (the victim(s)) in a manner that may cause mental or physical harm to them, including because of the intrusive, insulting, degrading, and/or threatening nature of the processing.

Online harassment may of course take many different forms, depending on the method used by the harassers. These different forms of online harassment have themselves been named and given variable definitions by the media, civil society or in the literature.¹²³⁸ Among those different forms of online harassment, one may refer in particular to:

- Doxing, i.e., the intentional public release onto the internet of personal information about an individual by a third party that may compromise his, her or their reputation or credibility, often with the intent to humiliate, threaten, intimidate, or punish that individual¹²³⁹;

¹²³⁴ Other identified common features may include “*a sense of anonymity and lack of accountability*” on the part of the harassers as well as “*the publicity of the actions*”. These two last characteristics are however not intrinsic given that the harassment may also be conducted by an identified person (for example, a colleague or an ex-boyfriend) in a semi-private sphere (for example, in a WhatsApp group).

¹²³⁵ For example, the internet service provider; the company behind the platform where the harassment is taking place; other users that may share the content without actively creating it; etc.

¹²³⁶ While the GDPR does not define the terms ‘sensitive data’, this terminology is usually used to refer to (i) special categories of personal data as listed in Article 9(1) of the GDPR, such as data revealing racial or ethnic origin, political opinion, religious beliefs, etc, and (ii) data relating to criminal convictions and offences or related security measures, as defined in Article 10 of the GDPR.

¹²³⁷ Article 9 GDPR.

¹²³⁸ Most of these practices have been (in)formally defined by the media, experts, scholars, or sometimes even in the law. There is, however, no fixed or commonly agreed definition at the EU level to describe these different types of practices.

¹²³⁹ Douglas, D. (2016). Doxing: A Conceptual Analysis. *Ethics and Information Technology* 18(3): 199-210.

- (Targeted) trolling, i.e., the action of leaving intentionally provocative or offensive messages on the internet, usually under the cover of anonymity, in order to get attention, cause trouble or upset someone; ¹²⁴⁰ when trolling is directed at one or multiple specific individuals with the intention to mock them, upset them or cause them harm, one may refer to ‘trolling against targeted individual(s)’ or ‘targeted trolling’;¹²⁴¹
- (Targeted) hate speech, i.e., the dissemination of hateful messages, including threatening or grossly offensive communications targeting one individual or a group of individuals on the basis of attributes such as gender, physical appearance, ethnicity, religion, sexual orientation, etc; when hate speech is directed at one or multiple identifiable individuals with the intention to denigrate or harm them, one may refer to ‘hate speech against targeted individuals’ or ‘targeted hate speech’;¹²⁴²
- Cyber-mob attacks or online harassment campaign, i.e., when a large group gathers online to try to collectively shame, harass, threaten, or discredit a target, for example by collectively spreading false information on the person, issuing death threats or rape threats;¹²⁴³
- Email bomb or message bombing, i.e., the action by a person or a group of persons to complain, annoy or show anger by intentionally flooding a target’s phone or email accounts with messages; such action may limit or block the user’s access to the operating system or platform;¹²⁴⁴

¹²⁴⁰ Diaz, F. L. (2016). Trolling & the First Amendment: Protecting Internet Speech in the Era of Cyberbullies & Internet Defamation. *University of Illinois Journal of Law, Technology & Policy*, 1:159; Aro, J. (2016). The Cyberspace War: Propaganda and Trolling as Warfare Tools. *European View* 15(1):121-32; McDermott, I. E. (2012). Trolls, Cyberbullies, and Other Offenders: Dealing with Antisocial Behaviour on the Internet. *Searcher*, 20(10):7-11.

¹²⁴¹ By opposition to non-targeted trolling. See Sanfilippo, M. R., Fichman, P. & Yang, S. (2018). Multidimensionality of online trolling behaviors. *The Information Society*, 34(1):27-39.

¹²⁴² See, among others, Assimakopoulos S., Baider F. H. , & Millar S. (2017). *Online Hate Speech in the European Union: A Discourse-Analytic Perspective*. Springer; Waldron, J. (2012). *The Harm in Hate Speech*. Cambridge: Harvard University Press; Tulkens, F. (2013). The Hate Factor in Political Speech. Where Do Responsibilities Lie? *Council of Europe*. <https://rm.coe.int/16800c170e> ; Johnson, N. F., Leahy, R., Restrepo, N.J. & al. (2019). Hidden resilience and adaptive dynamics of the global online hate ecology. *Nature*, 573:261–265; Berger Levinson, R. (2013). Targeted hate speech and the first amendment: How the supreme court should have decided Snyder. *Suffolk University Law Review*, 46(1):45;

¹²⁴³ Citron, D. (2020). Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (and as It Should Be). *Michigan Law Review*, 118(6):1073–1093.

¹²⁴⁴ Jacobsson, M. & Menczer, F. (2003, December). Untraceable Email Cluster Bombs. *login*; 28(6). <https://www.usenix.org/system/files/login/articles/1154-jacobsson.pdf> ; see also the definition in the Cambridge Dictionary (online): “an occasion when many email messages are sent to a single address at the same time, for example as a way of complaining or showing anger about something, or in order to annoy someone”.

- Online impersonation, i.e., a strategy whereby one or multiple persons pretend to be someone else and post sensitive, false or offensive information in the name of the victim;¹²⁴⁵
- Sextortion, i.e., the threat of distributing a nude or sexually explicit image or video in an effort to blackmail an individual, for example to obtain sexual favours or money;¹²⁴⁶
- Non-consensual dissemination of sexually explicit images (so-called “Revenge porn”), i.e., a practice consisting in sharing sexually-explicit images or videos of an individual – usually a woman – without her consent in order to shame or humiliate her.

It is important to note, at this point, that the above-mentioned practices may either fall within, overlap or go beyond the notion of online harassment as defined in this study, depending on the context in which they take place. Trolling, message bombing or hate speech, for example, may or may *not* fall within the notion of ‘online harassment’ as defined in this study depending on the circumstances. Notably, the identifiability of the victims is a determining element. In particular, a distinction must be made between practices that are directed against one or multiple *identifiable* individuals, and practices that are directed against one or multiple *unidentifiable* individuals or *legal persons*. Message bombing, for example, can either be directed against the mailbox of a natural person or against the mailbox of a company. In the same vein, hate speech can either be targeted at one or multiple identifiable individuals (for example, when tweeting hateful comments about a politician, an actress or any person whose identity is known or revealed) or at a group of *unidentified* persons (for example, the ‘gay community’ or ‘women’ in general).¹²⁴⁷ As stated above, the notion of ‘online harassment’ as defined in this study should be understood as covering only situations where the victims are individuals who are identified or identifiable, since they have been *individually targeted* by the harassers. As a consequence, not all forms of hate speech, trolling or message bombing will qualify as a form of ‘online harassment’ as defined in this study; rather, only harmful actions where the victim is *identified* or *identifiable* will fall within that definition

Of course, some of the above-listed practices are likely to always qualify as a form of online harassment because of their own characteristic elements. In the case of

¹²⁴⁵ Cox, C. (2014). Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosecutions and Effective Laws. *Jurimetrics Journal of Law, Science and Technology*, 54(3):277–302; Ramirez, R. (2012). Online Impersonation: a New Forum for Crime on the Internet. *Criminal Justice*, 27(2):4–9.

¹²⁴⁶ Wittes, B. (2017). Cyber Sextortion and International Justice. *Georgetown Journal of International Law* 48(3), p. 941; Carlton, A. (2020). Sextortion: the Hybrid ‘Cyber-Sex’ Crime. *North Carolina Journal of Law & Technology*, 21(3), p. 215; Wolak, J., Finkelhor, D., Walsh, W. & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health* 62(1):72-79.

¹²⁴⁷ If the hateful comments are blindly directed at a group of people without the possibility to identify one or several specific victims, it may still qualify as ‘hate speech’ or ‘*incitation à la haine*’ and be punished by a specific law but should not be considered as online harassment in the sense of this study.

doxing, sextortion, online impersonation or revenge porn, in particular, the harasser threatens to publish or publishes on the internet sensitive information about a specific individual precisely to shame or blackmail that individual, or to damage his/her credibility or reputation. Because of the intention of the harasser to cause harm to one person in particular, those types of practices will systematically fall within the notion of online harassment as defined in this study. Furthermore, from the perspective of EU data protection law, the information that the harasser publishes or threatens to publish about that natural person on the internet will normally always fall within the notion of ‘personal data’ as defined under EU data protection law, even if part or all of the information is actually forged or false.¹²⁴⁸ In the case of revenge porn, for example, the pictures or videos depicting the victim in a sexual manner will be considered ‘personal data’ under the GDPR as soon as the victim is identifiable, for example because her face is visible or because her name is linked to the publication, regardless of whether the pictures or videos are real, mere photo montages or deep fakes.¹²⁴⁹ Revenge porn, sextortion and doxing are therefore practices which, because of their characteristic elements, will almost always fall within the notion of online harassment as defined in this study. By contrast, when it comes to other forms of harassment such as mail bombings or hate speech, the specific circumstances of the case must be taken into account, and in particular whether identified or identifiable natural persons have been targeted by the attacks.

4.1.2. The impact of online harassment on human dignity, integrity and freedom of expression

Online harassment is a practice which may interfere with the right to privacy and the right to personal data protection of the victims concerned in different ways.¹²⁵⁰ It is settled case-law that the notion of ‘private life’ within the meaning of Article 8 of the Convention and Article 7 of the Charter is a broad concept which extends to a number of aspects relating to personal identity, such as a person’s name or image, but also a person’s physical and psychological integrity.¹²⁵¹ Furthermore, it is also well established in the case-law of the ECHR and the CJEU that a person’s right to be protected against defamation is encompassed by Article 8 of the Convention and Article 7 of the Charter.¹²⁵² Hence, online harassment where a person’s image or

¹²⁴⁸ van der Helm M. (2021). *Harmful deepfakes and the GDPR*. Master’s Thesis. Tilburg University. <http://arno.uvt.nl/show.cgi?fid=156861>.

¹²⁴⁹ Deep fakes are videos portraying people saying or doing things they never said or did. Deep fakes are created through sophisticated technological means using machine learning and artificial intelligence (See Raymond, J. (2019). Fakebusters Strike Back: How to Spot Deep Fakes, the Manipulated Videos That Are the Newest Form of “fake News” to Hit the Internet. *Index on Censorship* 48(1): 76-79.). On the subject of deep fakes, see also Kietzmann, J., Lee, L., McCarthy, I. & Kietzmann, T. (2019, December). Deepfakes: Trick or treat? *Business Horizons*. 63(2).

¹²⁵⁰ See, for example, ECtHR, Judgment of 9 July 2019, *Volodina v. Russian Federation*; ECtHR, 11 February 2021, *Buturugă v. Romania*.

¹²⁵¹ See, for instance, ECtHR, Judgment of 24 September 2004, *Von Hannover v. Germany*, para. 50, and; ECtHR, Judgment of 27 January 2015, *Paradiso and Campanelli v. Italy*, para. 159.

¹²⁵² See ECtHR, Judgment of 29 March 2016, *Bédat v. Switzerland*, para. 72, with further references.

reputation is being harmed can constitute a violation of these rights when such attacks attain a certain level of seriousness.¹²⁵³ The impact of online harassment is however not limited to privacy and data protection. Depending on its effects, online harassment can also pose a serious threat to at least three other fundamental rights in particular: (i) human dignity, (ii) the right to the integrity of the person, and (iii) freedom of expression and information. To better comprehend the impact of online harassment on its victims, this section will first distinguish *online* harassment from *offline* harassment, before highlighting how online harassment can interfere with human dignity, the right to integrity or freedom of expression by looking at different studies on the subject.

4.1.1.1. Distinction between the scope and effects of offline and online harassment

From the outset, it must be said that, because of the absence of commonly agreed definition of ‘online harassment’ at the EU level, the data that have been collected so far to study this phenomenon and its impact on fundamental rights must be taken with caution. Some studies, for example, have focused on cyber-bullying among children (i.e., a specific type of online harassment limited to younger victims),¹²⁵⁴ while others have focused on cyber violence against women (i.e., which broadly includes various forms of online abuses, such as hate speech against women in general, or online harassment targeted against identifiable female persons),¹²⁵⁵ or on the rise of hate speech and hate crime in general on the internet (i.e., a study whose scope is very broad and goes well beyond online harassment as defined in this study).¹²⁵⁶ As a result, it is sometimes necessary to combine different data from various reports, or conversely to break up some data within the same study, in order to form an insightful image of the extent and gravity of the phenomenon of online harassment as defined in this study. Yet, looking at the different studies on the subject,¹²⁵⁷ it clearly appears that, since the advent of the internet, online harassment has been on the rise and has become a problem distinct from previously known forms of harassment in the offline world.¹²⁵⁸ As more and more individuals access the internet, share personal data on social media, and rely on ICTs on a daily basis, online abuses – from small financial scams to large cyberattacks – have

¹²⁵³ See ECtHR, Judgment of 7 February 2012, *Axel Springer AG v. Germany*; ECtHR, Judgment of 16 June 2015, *Delfi AS v. Estonia*, para. 137; and ECtHR, Judgment of 25 September 2018, *Denisov v. Ukraine*, para. 112.

¹²⁵⁴ European Parliament (2016, August 30). Study on cyberbullying among young people.

¹²⁵⁵ European Parliament (2018, September). Study on cyber violence and hate speech online against women. [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU\(2018\)604979_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf)

¹²⁵⁶ European Parliament (2020, July). Study on hate speech and hate crime in the EU and the evaluation of online content regulation approaches. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/655135/IPOL_STU\(2020\)655135_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/655135/IPOL_STU(2020)655135_EN.pdf)

¹²⁵⁷ American experts and scholars have extensively written on the subject of online harassment in the United States, and in particular on cyber-bullying, hate speech and revenge porn. Unfortunately, those resources are less relevant in the framework of this study whose scope has been limited to the EU.

¹²⁵⁸ For example, sexual harassment at the workplace already existed before the advent of the internet and the rise of ICTs, and could take place in the form of inappropriate sexual comments, remarks or behaviours towards a colleague. Today, the same type of harassment can extend beyond the workplace because of ICTs while involving the same harasser and victim. See European Parliament (2018, September). *op. cit.*, p. 10.

significantly increased. This is particularly true for online harassment. Indeed, it is generally agreed in the literature that ICTs have facilitated and intensified harassing behaviours and often exacerbated their negative consequences¹²⁵⁹ Multiple elements explaining such facilitation and intensification can be pointed out.

First, one may point out the ease with which harassers can hide their identity on the internet, for example, behind a pseudonym, a false profile or by using a VPN. Anonymity is often perceived by harassers as an absence of rules and accountability, thereby reducing inhibition and intensifying abuses.¹²⁶⁰ In 1969 already, American psychologist Philip Zimbardo demonstrated that when individuals are being merged in an anonymised group, they were keener to lose personal control and display more violent and disinhibited behaviours.¹²⁶¹ Similarly, research has shown that, on social media platforms, anonymous users tend to act in ways that they would never dare to do in the offline world.¹²⁶² Besides this element of anonymity, the possibility for an individual to connect in a few clicks, harass somebody without having to immediately deal with the victim's reaction, and then just "*log off at the end of the day*",¹²⁶³ also make him less empathic towards the victim, and less sensitive to social norms in general. This is usually referred to as the online disinhibition effect.¹²⁶⁴ This explains why perfectly reasonable individuals in the offline world may become harassers on the internet. In other words, online disinhibition leads to an increase in abusive and harassing behaviours on the internet.¹²⁶⁵

Second, one may point out the availability of the various means for conducting online attacks at almost no cost. Unlike offline harassment, cyber abuses can indeed be conducted through various channels with little investment or efforts, for example on social media, via a private messaging app, by sending emails, by "tagging" "@-mentioning" someone,¹²⁶⁶ or by publishing hateful or degrading communications on various websites. The harassers simply need a smartphone or a laptop to conduct a

¹²⁵⁹ Langlois, G. & Slane, A. (2017). *op. cit*; Corcoran, L., Mc Guckin, C. & Prentice, G. (2015). *op. cit*.

¹²⁶⁰ For some forms of online harassment, such as cyberstalking, anonymity even becomes a constitutive element. See Roberts, L. D. (2008). Jurisdictional and Definitional Concerns with Computer-mediated Interpersonal Crimes: An Analysis on Cyber Stalking. *International Journal of Cyber Criminology*, 2(1).

¹²⁶¹ Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order vs. deindividuation, impulse, and chaos. W. J. Arnold & D. Levine (Eds.). *Nebraska Symposium on Motivation*. Lincoln: University of Nebraska Press.

¹²⁶² McCully, J. (2019, March 3). Legal Responses to Online Harassment and Abuse of Journalists: Perspectives from Finland, France and Ireland. *Organization for Security and Co-operation in Europe (OSCE) & International Press Institute (IPI)*. <https://www.osce.org/files/f/documents/1/6/413552.pdf>, p. 3.

¹²⁶³ Zimmerman, A. G. (2012) Online Aggression: The Influences of Anonymity and Social Modelling. University of North Florida. *UNF Graduate Theses and Dissertations*, 403. <https://digitalcommons.unf.edu/cgi/viewcontent.cgi? article=1472&context=etd>.

¹²⁶⁴ Suler, J. (2004). The Online Disinhibition Effect. *Cyber Psychology & Behaviour*, 7(3):321.

¹²⁶⁵ European Parliament (2018, September). *op. cit.*, p. 27.

¹²⁶⁶ As rightly pointed out by McCully in the OSCE & IPI report on online harassment of journalists, "*the practice of repeatedly "tagging" or "@-mentioning" an individual can instil the same feelings of distress, anxiety or fear as can be caused by repeated direct contact through private communication channels. Furthermore, the victim will usually be notified each time the original post "tagging" or "@-mentioning" her is "liked" by another user of the social media platform, which can intensify and aggravate the impact of the communication or even turn a once-off message into a repeated one.*" McCully, J. (2019, March 3). *op. cit.*, p. 4.

potentially unlimited number of attacks. They can also rely on various freely available platforms, search engines or software to stalk their victims, spread harmful messages, or even *create* fake harmful content (e.g., use of PDF to create documents incriminating a person, such as a fake offshore bank account statement; use photo or video editing software to fabricate photo montages or deepfake videos, such as fake pornographic pictures; etc.).

Third, ICTs have exacerbated both the scope and frequency of online harassment by erasing some of the constraints of the physical world. In the *offline* world indeed, the number of harassers or attacks is limited by both spatial and temporal boundaries. This is less the case in the online world since the internet does not know any border. Hence, online harassment may involve a very large number of individuals located in various countries around the globe, who may virtually gather around the same victim(s) and turn into an online ‘mob’. Beyond the actual number of harassers, the absence of spatial and temporal constraints in the offline world can also increase the frequency and number of daily attacks; with a smartphone and a WIFI connection, one single harasser can potentially send hundreds of degrading or insulting messages over a few hours, including by relying on automated messaging, bots and other technologies. As an illustration, it has been observed that Greta Thunberg’s Twitter account averages 30 hate messages per minute referencing in derogatory terms her age, gender or Asperger’s syndrome.¹²⁶⁷ Such average peaked to 500 per minute the day she met Barack Obama.¹²⁶⁸ Even if these numbers remain relative in the sense that there might be no direct correlation between the number of harassers/attacks on the one side, and the psychological impact on the mind of the victim on the other side, it can reasonably be argued that the overall sense of vilification and victimization is reinforced by the broad scope of online harassment. In other words, “*numbers count*”.¹²⁶⁹

Fourth, it must be acknowledged that, in the online world, the ‘audience’ witnessing those types of abuses is also incredibly wider. This audience can either be composed of passive or active witnesses. Witnesses may become active when, for example, they react to a harmful post with a comment or a click, such as a “shocked face emoji” or a “thumbs down”. The fact that some witnesses may be well-intentioned in doing so (for example, re-posting or sharing an injurious post with a view of denouncing it and condemning the harassers) still has the adverse effect of increasing the visibility of the abusive content. The AEDP “Twitter case”,¹²⁷⁰ where a user shared a video depicting a woman and her child being physically abused with the intention to raise awareness on violence against women, illustrates this issue.

¹²⁶⁷ Brown, A. (2020, May). Models of Governance of Online Hate Speech. Council of Europe. <https://rm.coe.int/models-of-governance-of-online-hate-speech/16809e671d>, p. 43, referring to comments made by Paul Giannasi.

¹²⁶⁸ *Ibid.*, p. 42.

¹²⁶⁹ *Ibid.*, p. 43.

¹²⁷⁰ AEDP, Expediente N° PS/00205/2021, 26 June 2021, available at <https://www.aepd.es/es/documento/ps-00205-2021.pdf>.

The publicity of potentially harmful content – even if well-intentioned – may indeed further increase the sense of vilification of the victim and thus negatively impact their right to integrity or dignity.

Fifth, in the context of online harassment, the temporality of the consequences needs to be appreciated taking into account the volatility of the data. As stated by Langlois and Slane, “[w]hen someone is publicly shamed online, that shaming becomes a live archive, stored on servers and circulating through information networks via search, instant messaging, sharing, liking copying and pasting.”¹²⁷¹ As a consequence, “the resulting harm is not simply about the effects of an action at a specific time and place, but also the reverberations of an action throughout information networks”.¹²⁷² In the case of doxing, targeted hate speech or revenge porn, for example, because of the volatility of data, once a hateful message, compromising information or a sexually explicit picture has been made available online by the harasser(s) on a public platform or website, it becomes virtually impossible for the victim to prevent such content from being copied, captured, downloaded, or shared, and thus to (re)appear on the same or different platforms in the future.

Finally, online harassment also differs from traditional forms of harassment with respect to its main category of victims. Indeed, research both in the EU and in the US has shown that age and gender are significant factors in the prevalence of cyber harassment, with young women being the main victims of such attacks.¹²⁷³ In 2006, a US study had for example demonstrated that, within online chatrooms, accounts with feminine usernames incurred an average of 100 malicious messages a day (such as sexually explicit or threatening messages), while masculine names would only receive 3.7 malicious messages a day.¹²⁷⁴ More recent studies conducted in the EU have confirmed this trend,¹²⁷⁵ such as a 2014 research from the European Agency for Fundamental Rights which found that, on average, 1 in 10 women have already experienced some form of cyber violence by the time they are 15 (that is, significantly more than boys of the same age).¹²⁷⁶ In other words, the misogyny and sexism that already existed in the offline world seem to have found a continuum and been further exacerbated in the online world.

¹²⁷¹ Langlois, G. & Slane, A. (2017), *op. cit.*, p. 2.

¹²⁷² *Ibid.*, p. 2.

¹²⁷³ European Parliament (2018, September). *op. cit.*, p. 8; Neill, D. (2015). Mobile Technologies and the incidence of cyberbullying in seven European countries: findings from the Net Children Go Mobile. *Societies*, 5:384-398; Hess, A. (2014, January 6). Why Women Aren't Welcome on the Internet. *Pacific Standard*. <https://psmag.com/social-justice/women-arent-welcome-internet-72170>.

¹²⁷⁴ Meyer, R. & Cukier, M. (2006). Assessing the Attack Threat due to IRC Channels. Conference: Dependable Systems and Networks. 467-472. 10.1109/DSN.2006.12.

¹²⁷⁵ Staude-Müller, F., Hansen, B. & Voss, M. (2012). How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology*, 9:260-274; European Parliament (2018, September). *op. cit.*, p. 8; Neill, D. (2015). *op. cit.*, p. 384-398; European Agency for Fundamental Rights (2014, March 5). Violence against women: an EU-wide survey. Main results report. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf

¹²⁷⁶ European Agency for Fundamental Rights (2014, March 5). *op. cit.*

One of the early affairs that shed light on the gravity of this phenomenon was the 2014 ‘GamerGate controversy’¹²⁷⁷ – a coordinated online harassment campaign directed against three female figures of the videogame industry in the US, i.e., Zoë Quinn, Brianna Wu and Anita Sarkeesian. Under the hashtag #GamerGate, an online mob composed of thousands of harassers launched coordinated and particularly vicious attacks against these three women during several months. Those attacks included, *inter alia*, doxing, rape threats, death threats and the distribution of fabricated ‘revenge porn’ content (e.g., fake nude pictures of Quinn were sent to her colleagues; Sarkeesian’s Wikipedia page was vandalized with pornographic images and her face was inserted on videos staging her rape by video games characters; etc.). The home addresses of the three women were also leaked online by their harassers, which forced them to flee from their house with their family. The main reason behind this online harassment campaign was the fact that Quinn, Wu and Sarkeesian were three women promoting novel feminist views in a traditionally male-dominated industry. Many of these attacks had been conducted on Twitter at the time, thereby triggering vivid debates on the apparent inability of the platform to effectively act upon this type of organised online harassment.¹²⁷⁸ This scandal ultimately prompted Twitter to adopt new internal policies prohibiting hate speech and revenge porn.¹²⁷⁹ Overall, Gamergate had the merit to call attention to the scope of gendered harassment on social media and to encourage further debates on the role and responsibility of major internet operators in preventing such practices.¹²⁸⁰

In view of the above, it can be concluded that online harassment significantly differs from offline harassment and poses relatively novel and seemingly growing threats to the fundamental rights and freedoms of data subjects. Beyond the right to privacy and the right to personal data protection themselves, it can be argued that online harassment impedes human dignity, the right to integrity of the person and, in some instances, the freedom of expression of the victim(s), as further discussed in the following sub-section.

¹²⁷⁷ Mortensen, T. E. & Sihvonen, T. (2020). Negative Emotions Set in Motion: The Continued Relevance of #GamerGate. Holt, T. J., Bossler, A. M. (eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Springer International Publishing, pp. 1353–1374; Salter, M. (2018). From Geek Masculinity to Gamergate: The Technological Rationality of Online Abuse. *Crime, Media, Culture* 14(2): 247-64. See, also: Wikipedia, Gamergate controversy. https://en.wikipedia.org/wiki/Gamergate_controversy

¹²⁷⁸ Brustein, J. (October 14, 2014). A #GamerGate Target Wants Twitter to Make Harassment Harder. Bloomberg BusinessWeek. <https://www.bloomberg.com/news/articles/2014-10-14/a-no-gamergate-target-wants-twitter-to-make-harassment-harder>; Meyer, R. (October 30, 2014). The Existential Crisis of Public Life Online. *The Atlantic*. <https://www.theatlantic.com/technology/archive/2014/10/the-existential-crisis-of-public-life-online/382017/>; Plante, C. (June 10, 2015). Twitter is letting you and your friends join hands to block trolls and miscreants. *The Verge*. <https://www.theverge.com/2015/6/10/8761231/twitter-block-lists-share-import-export-social-media-trolls>.

¹²⁷⁹ Jeong, S. (2016, January 14). The History of Twitter's Rules. *Vice*. https://motherboard.vice.com/en_us/article/z43xw3/the-history-of-twiters-rules.

¹²⁸⁰ Salter, M. (2018). *op. cit.* 247-248.

4.1.1.2. Outlining the impact of online harassment on human dignity, the right to integrity and freedom of expression

Online harassment, depending on its form and degree of seriousness, can cause harm to the individuals who are being targeted, and thus interfere with various rights and freedoms protected under the Convention and the Charter, including human dignity, the right to integrity and freedom of expression.

As far as **human dignity** is concerned (Article 1 of the Charter), it is generally agreed that online harassment, especially when it takes the form of offensive, degrading or insulting comments, consists into a direct attack on human dignity. The dignity of the person is not only a fundamental right in itself but constitutes a value underpinning all other fundamental rights and freedoms, and forms thus the basis or core of fundamental rights protection in the EU.¹²⁸¹ As such, any attack on an individual's fundamental rights or freedoms will thus, to some extent, be considered as an attack on human dignity. The term 'dignity' is commonly understood as the value that a person has and "*that makes other people respect them or makes them respect themselves*".¹²⁸² The terms "*human dignity*" indicates that dignity is inherent to the human person. Under EU law, human dignity is a core value made inviolable. As a consequence, "*none of the rights laid down in [the] Charter may be used to harm the dignity of another person*".¹²⁸³ Because human dignity forms part of the substance of every other right and freedom laid down in the Charter, it can be argued that the violation of one of this right and freedom will also always entail a violation of human dignity itself. Keeping this in mind, a violation of the right to privacy and/or the right to personal data protection of an individual, including in the context of online harassment, can also be regarded as an attack on human dignity. When a woman, for example, becomes the victim of revenge porn, and sees intimate pictures of her being widely disseminated on the internet, she will often feel stripped of her dignity.¹²⁸⁴ Of course, online attacks are not similar to physical attacks in the sense that they remain exposed to the subjective reaction and feelings of the target. The relative effect of verbal attacks is embodied in the famous phrase "*sticks and stones may break my bones, but words shall never hurt me.*" Yet, according to the 'Speech Act theory', speech is not merely a cause of action but is an action itself. This is illustrated by the fact that verbal harassment, including in the form of hate speech,

¹²⁸¹ See Explanations to the Charter, Article 1, *op. cit.*, which states: "*The dignity of the human person is not only a fundamental right in itself but constitutes the real basis of fundamental rights.*"

¹²⁸² Cambridge dictionary (online).

¹²⁸³ See Explanations to the Charter, *op. cit.*, Article 1.

¹²⁸⁴ Madden, R. (2019). *Equity, 'Revenge Porn', and Cambridge Analytica: The Doctrine of Confidence as a Protection for Human Dignity in the Technological Age*. *Griffith Journal of Law & Human Dignity*, pp. 1-30; Bloustein, E. J. (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review*, 39:962

can cause real harm to their victims. These attacks on human dignity can, in turn, put at risk the **mental** or **physical integrity** of the victim concerned.¹²⁸⁵

As far as the **right to integrity** is concerned (Article 3 of the Charter), and in particular **mental integrity**, the purpose of online harasser(s) is often to plant in the mind of the victims a constant sense of unease or fear. Even when the attacks are not taking place, the victims continue to fear the next one, without knowing if, when or how it will appear. Online harassment, even when ‘*on pause*’, thus hangs above the head of the victim like a sword of Damocles. This further induces “*a loss of agency and power over one’s own narrative*”.¹²⁸⁶ One of the key findings of recent studies on online harassment is that this loss of agency can have a lasting mental impact on those who are victimised, with effects ranging from lower self-esteem or loss of self-confidence, to mental or emotional stress, to anxiety or panic attacks, to financial loss and in some cases difficulty in securing employment and housing.¹²⁸⁷ Revenge porn, in particular, has been described as a sort digital sexual assault with devastating consequences for the mental integrity of the victims.¹²⁸⁸ As explained by Langlois and Slane, the publication of intimate images without consent is “*robbing the victim of her sexual integrity and of her dignity to inhabit her body as her own*”.¹²⁸⁹ Hence, victims of ‘revenge porn’ often experience emotional distress, post traumatic disorder or suicidal thoughts.¹²⁹⁰

Beyond the mental integrity of the victim, online harassment may also endanger the **physical integrity** of the victim if death or rape threats are formulated, or if verbal attacks ultimately turn into physical attacks. One may refer to the Mila Affair by way of example (in French: ‘*Affaire Mila*’). Mila, a 16-years old teenager living in France, became the target of an intensive online harassment campaign after posting a video on Instagram where she is harshly criticising Islam as a religion. The video was initially posted by Mila in response to the sexist and homophobic comments sent by one of her Instagram followers during a live session. In the video, she states, *inter alia*, that she “*hated religions*” in general, that the Coran was “*full of hatred*” and

¹²⁸⁵ Waldron, J. (2017). *op. cit.*, pp. 105-143; Duggan, M. (2017, July 11). Online Harassment 2017. *Pew Research Center*. http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf; European Parliament (2018, September). *op. cit.*, p. 33.

¹²⁸⁶ European Parliament (2018, September). *op. cit.*, p. 28.

¹²⁸⁷ Amnesty International (2017). Amnesty reveals alarming impact of online abuse against women. <https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/>; UK Council for Internet Safety (2019, June 26). Adult Online Hate, Harassment and Abuse: A rapid evidence assessment. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf.

¹²⁸⁸ Wilson, O. (2017, December 6). Revenge Porn Is More Than a Violation of Privacy It Is Digital Sexual Assault. *The Huffington Post*. http://www.huffingtonpost.com/olivia-wilson/revenge-porn-is-more-than_b_7641876.html.

¹²⁸⁹ Langlois, G. & Slane, A. (2017), *op. cit.*, p. 7, referring to Elaine Craig (2012). *Troubling Sex: Towards a Legal Theory of Sexual Integrity*. Vancouver: UBC Press.

¹²⁹⁰ Franks, M. A. (2015). Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators. University of Miami School of Law (web version).

that “*Islam was shit*”.¹²⁹¹ After the video was widely shared on social media, Mila became the target tens of thousands of heinous messages, including fifty thousand death threats.¹²⁹² Her full name, personal home address and high school location are quickly revealed on the internet (i.e., ‘doxing’).¹²⁹³ Because the serious risk of physical harm or attempt on Mila’s life, the young teenager had to leave school, move away from her home and was put under police protection for more than a year. In July 2021, i.e., more than one year after the facts, only 11 individuals are recognised liable by the Paris Criminal Court. All in all, this affair shows not only the systemic failure of the criminal justice system to hold harassers liable, but also the interference that online harassment can cause with the right mental and physical integrity of the victim. With respect to the risk of interference with the physical integrity of the victims, it must also be pointed out that physical attacks may be inflicted by the online harasser(s), by a third-party who supports or adheres to the ideas spread by the harassers, or by the victim herself or himself through self-harm or suicide attempts. As far as self-harm is concerned, different EU studies on cyberbullying have shown that victims of these types of attacks are at a greater risk than others of both self-harm and suicides.¹²⁹⁴ Victims of revenge porn seem particularly affected; the repetitive character of the attacks, as well as the feeling of shame and powerlessness, has already led many young women to take their own life.¹²⁹⁵ The same goes for young victims of cyber-bullying; those last fifteen years, the media have reported many cases of cyberbullying where the victims ultimately committed suicide, especially among teenagers.¹²⁹⁶ In a 2014 EU study, more than 50% of children bullied online said that they became depressed as a result and over a third of them stated that they harmed themselves or thought about suicide.¹²⁹⁷ Finally, in most severe instances, it must be noted that online harassment can escalate into actual physical violence. Research has shown, in particular, that cyber violence against women can be a precursor for physical abuses in the offline world

¹²⁹¹ In French: “*Je déteste la religion. [...] Le Coran il n’y a que de la haine là-dedans, l’islam c’est de la merde. [...] J’ai dit ce que j’en pensais, vous n’allez pas me le faire regretter. Il y a encore des gens qui vont s’exciter, j’en ai clairement rien à foutre, je dis ce que je veux, ce que je pense. Votre religion, c’est de la merde, votre Dieu, je lui mets un doigt dans le trou du cul. Merci, au revoir.*”. Statement transcribed from Arama, V. (2020, January 29). *Affaire Mila : retour sur dix jours de polémiques*. *Le Point*. https://www.lepoint.fr/societe/affaire-mila-retour-sur-dix-jours-de-polemiques-29-01-2020-2360339_23.php.

¹²⁹² Sasyer, P. (2021, January 20). EXCLUSIF. Mila: « *Ça fait un an que j’ai perdu ma vie* ». *Le Point*. https://www.lepoint.fr/politique/exclusif-mila-ca-fait-un-an-que-j-ai-perdu-ma-vie-20-01-2021-2410522_20.php.

¹²⁹³ Champenois, S. & Moran, A. (2020, February 7). *Affaire Mila : d’Instagram au Sénat, itinéraire d’une polémique*. *Libération*. https://www.liberation.fr/france/2020/02/07/d-instagram-au-senat-itinerai-re-d-une-polemique_1777706/

¹²⁹⁴ Council of Europe (2016). Background note on sexist hate speech. <https://bit.ly/2LDTcVt>; John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., & Hawton, K. (2018). Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review. *Journal of medical Internet research*, 20(4); Litwiller, B. & Brausch, A. (2013). Cyber Bullying and Physical Bullying in Adolescent Suicide: The Role of Violent Behavior and Substance Use. *Journal of Youth and Adolescence*, 42(5):675-84; Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among Bullying, Cyberbullying, and Suicide in High School Students. *Journal of Adolescence*, 36(2):341-50.

¹²⁹⁵ Council of Europe (2016). *op. cit.*

¹²⁹⁶ Among the cases that got media attention, one may refer in particular to the case of Megan Meier, Jessica, Rosalie Avila, Hope Witsell, Phoebe Prince, Audie Taylor Pott, Amanda Todd, Kenneth Weishuhn, Brandy Vela, Ashawty Davis and Gabriella Green.

¹²⁹⁷ European Parliament (2018, September). *op. cit.*, p. 14.

by the same harassers.¹²⁹⁸ In some other instances, online harassment campaigns directed against an individual may attract the attention of a third-party who – although not having taken part in the online attacks himself/herself – can become convinced by the arguments or righteousness of an online ‘mob’, and decides to physically aggress the target in the physical world. This is what happened, for example, in the case of Samuel Paty, a French history teacher who was beheaded in the street by an 18-year-old man, following an online harassment campaign initiated by the father of one of Mr Paty’s students.¹²⁹⁹ The murderer had neither initiated nor contributed to the online harassment campaign against the teacher, but had become convinced of the wrongdoing of the latter as presented by the online mob. As a result, he tracked down Samuel Paty and brutally killed him.¹³⁰⁰

Online harassment may also, in some cases, interfere with the **freedom of expression** of the victims, as protected in Article 11 of the Charter, if the latter decide to withdraw previously shared ideas, material or opinions, and/or not to share new ones, by fear of further attacks. The link between online harassment and restrictions on free speech appears more evident when considering that social media have been replacing traditional media in terms of information dissemination, and are at the same time the most common place where online harassment takes place.¹³⁰¹ The primary function of these platforms is normally to enable its users to share content, either privately or publicly, such as pictures, videos but also opinions or ideas, at no or little costs, thereby offering new possibilities for freedom of expression to flourish. However, the abuse, by one or multiple users, of their freedom of expression in the form of threatening, insulting or degrading communications against other users, may lead the latter to refrain from using that same freedom. Of course, generally prohibiting any form of expression that may appear shocking, insulting or threatening would also violate freedom of expression as guaranteed by Article 11 of the Charter. In 1976, the ECtHR had already made clear that freedom of expression is “*applicable not only to ‘information’ or ‘ideas’ that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there would be no democratic society*”.¹³⁰² Overall, a balance needs to be established between, on the one hand, the need to protect the freedom of expression of individuals whose ideas or comments may appear harmful to others, and the need to protect human, the right to the integrity of the person, the right to

¹²⁹⁸ *Ibid.*, p. 21.

¹²⁹⁹ Willsher, K. (2020, December 4). Samuel Paty: French security services failed to act over incendiary social media campaign. *The Guardian*. <https://www.theguardian.com/world/2020/dec/04/samuel-paty-french-security-services-failed-to-act-over-incendiary-social-media-campaign>.

¹³⁰⁰ Aron, M. & al. (2020, Octobre 21). Samuel Paty, victime de l’engrenage de la haine. *L’Obs* ; Leloup, D. (2020, Octobre 20). Incriminés après l’assassinat de Samuel Paty, les réseaux sociaux auraient-ils pu faire davantage ? *Le Monde*.

¹³⁰¹ Vogels, E. A. (2021, January 13). The State of Online Harassment. *Pew Research Center*. file:///Users/Flo/Downloads/PI_2021.01.13_Online-Harassment_FINAL-1.pdf.

¹³⁰² ECtHR, Judgment of 7 December 1976, *Handyside v. the UK*, para. 49.

privacy and – to some extent – the freedom of expression of the persons who are targeted by those ideas or comments. This task, of course, is far from being easy, as exemplified by the many political, legislative and academic debates on the regulation of hate speech (within or outside of the context of online harassment).¹³⁰³

Beyond the debates on the effect of online abuses on free speech in general, the online harassment of *journalists* is a particular phenomenon which has prompted growing concern in recent years. Various studies have indeed shown that journalists, and in particular female journalists, increasingly find themselves the target of abuses through social media or other forums, including in some instances violent death and rape threats.¹³⁰⁴ Journalists form a specific category of victims when it comes to the effect of online harassment on free speech, as sharing their point of view or opinions can sometimes trigger an online hailstorm of denigrating comments, insults, blackmailing or threats. Out of fear, or in an attempt to put an end to those online attacks, journalists may decide to avoid covering certain topics, as it has been the case for the French journalist Julie Hainaut.¹³⁰⁵ This, in turn, can prevent their audience from receiving and departing information of public interest. The ‘chilling effect’ of online harassment on female journalists has unfortunately become alarmingly common over the last decade. Today, approximately 70% of female journalists are subject to online harassment.¹³⁰⁶ Among those women, 40% have already avoided covering certain stories as a result and, one-third already considered leaving the profession due to online attacks and threats.¹³⁰⁷ As regards the psychological effects of such harassment, a 2018 survey conducted by the International Federation of Journalists showed that a majority of the victims (63%) suffered from stress, panic attacks or severe anxiety because of the messages they were receiving from their harassers. Regularly, new testimonies of online attacks against female journalists involving revenge porn, doxing, cyber-mobbing, or

¹³⁰³ Gillespie, T. (2020). Content Moderation, AI, and the Question of Scale. *Big Data & Society*, 7(1); Cowls J. & al. (2020). Freedom of Expression in the Digital Public Sphere. Policy brief. *Graphite* <https://graphite.page/policy-brief-values/>.

¹³⁰⁴ McCully, J. (2019, March 3), *op. cit.*, p. 2; Bartlett, J. (2014). Misogyny on Twitter. *Demos*. <https://www.demos.co.uk/project/misogyny-on-twitter>; Ferrier, M. (2018). Attacks and Harassment: The Impact on Female Journalists and Their Reporting. *International Women's Media Foundation*. <https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf>; Elks, S. (2018, September 13). 'I will rape you': female journalists face 'relentless' abuse. Reuters. <https://www.reuters.com/article/us-global-women-media/i-will-rape-you-female-journalists-face-relentless-abuse-idUSKCN1LT39G>.

¹³⁰⁵ See summary of this case above, directly under section 4.1 of this study.

¹³⁰⁶ Ferrier, M. (2018). *op. cit.*; International Federation of Journalists (2017, November 24). IFJ Survey: two-thirds of women journalists suffered gender-based online attacks. <https://www.ifj.org/media-centre/reports/detail/ifj-survey-one-in-two-women-journalists-suffer-gender-based-violence-at-work/category/press-releases.html>

¹³⁰⁷ *Ibid.*

impersonation emerge in EU media.¹³⁰⁸ This online harassment often find sexist motivation, while female journalists from minority groups can also be attacked with respect to their religion or ethnicity.¹³⁰⁹ The online harassment of journalists poses a real risk to the free flow of information and the exchange of ideas in our democratic societies. Beyond the impact that online harassment can have on the mental integrity of its victims, such attacks can indeed also become “*a problem for the whole society*” when access to information is restricted because journalists self-censor.¹³¹⁰

Overall, the effect of online harassment on the freedom of expression of its victims – whether journalists or ‘normal’ citizens – is a topic which probably requires further research, as the data available are still scarce. In many cases, there is also a lack of clarity about how best to pursue legal accountability for online harassment. One of the most challenging questions in this respect is how to refrain the ability of the harassers to publish harmful content without compromising freedom of expression *ex ante*.¹³¹¹ It would however go beyond the scope of this study to analyse the potential chilling effect that anti-harassment norms could have on freedom of expression, and to balance this chilling effect with the positive impact that anti-harassment norms could have *for* freedom of expression. It is enough, at this stage, to acknowledge that online harassment can negatively affect the digital inclusion of the victims of such attacks, and thus their freedom of expression, and that when online harassment is directed against journalists, freedom of expression is particularly endangered.¹³¹²

¹³⁰⁸ See, among others, the testimonies of ten female journalist, blogger or politician in the documentary « #SalePute » / « #dreckschure », by Florence Hainaut and Myriam Leroy, available on ARTE, <https://www.youtube.com/watch?v=U6liaCL2mZI>; Segura, O. (2020, August 21). Une dizaine de journalistes belges cyber-harcelées parce qu’elles sont des femmes. *Les Inrockuptibles*. <https://www.lesinrocks.com/actu/une-dizaine-de-journalistes-belges-cyberharceeles-parce-queelles-sont-des-femmes-177701-21-08-2020/>; International Federation of Journalists (2018, November) 21. #DontTroll testimonies : Florence Hainaut (Belgique). <https://www.ifj.org/media-centre/news/detail/category/international-day-for-the-elimination-of-violence-against-women-and-girls/article/donttroll-testimonies-florence-hainaut-belgique.html>; Anonymous (2018, June 4). Procès des harceleurs présumés de Nadia Daam : le cyber-harcèlement à l’encontre des journalistes ne doit pas rester impuni. *Reporters sans frontières*. <https://rsf.org/fr/actualites/proces-des-harceleurs-presumes-de-nadia-daam-le-cyber-harcelement-lencontre-des-journalistes-ne-doit>; Bergé, J. (2019, Novembre 29). "Suceuses de bites", "grosses putes", "grosses salopes": le quotidien des femmes journalistes sur les réseaux sociaux. *RTBF*. https://www.rtb.be/info/dossier/les-grenades/detail_cyberharcelement-des-femmes-journalistes-temoignages?id=10376540; R. V. (2020, Septembre 3). Harcèlement sur les réseaux sociaux: renvoi en correctionnelle du harceleur de Myriam Leroy. *L’Avenir*. https://www.lavenir.net/cnt/dmf20200903_01504521/harcelement-sur-les-reseaux-sociaux-renvoi-en-correctionnelle-du-harceleur-de-myriam-leroy.

¹³⁰⁹ Belga (2019, June 20). La journaliste de RTL Salima Belabbas victime de propos racistes: le CSA réagit. *Le Soir*. <https://www.lesoir.be/231923/article/2019-06-20/la-journaliste-de-rtl-salima-belabbas-victime-de-propos-racistes-le-csa-reagit>; Belga (2021, March 9). Six mois de prison requis pour propos haineux et racistes envers l’animatrice de la RTBF, Cécile Djunga. *Le Soir*. <https://www.lesoir.be/359798/article/2021-03-09/six-mois-de-prison-requis-pour-propos-haineux-et-racistes-envers-lanimatrice-de>.

¹³¹⁰ *Ibid.*

¹³¹¹ McCully, J. (2019, March 3). *op. cit.*, p. 2

¹³¹² And in particular women’s digital inclusion, given that they are the primary victims of such attacks. Source: European Parliament (2018, September). *op. cit.*, p. 34; McCully, J. (2019, March 3). *op. cit.*

It clearly appears from the above considerations that state-led measures are necessary to combat online harassment as a societal phenomenon which may endanger human dignity, the right to integrity and, in some instances, the freedom of expression of the victims concerned. Among those measures, encouraging self-regulation among online platforms, adopting new legislation or amending existing one is considered as key step in most Member States and at the EU level, as reflected in the various studies and reports conducted at the initiative of public institutions on the subject. Yet, those legislations may still fail at comprehensively addressing the phenomenon of online harassment because of substantial flaws or enforcement issues, as further briefly discussed below.

4.1.3. The (lack of) EU or national legislation to tackle online harassment

The aim of this study is to show how EU data protection law, because of its multi-functional nature, could – if properly interpreted and applied – offer some effective tools to protect data subjects' rights and freedoms against harmful data processing practices such as online harassment. Before assessing the extent and limits of the functionality of EU data protection for combatting online harassment, it seems relevant to first briefly review what other legislative norms already exist in this respect. Rather than analysing in depth the scope and content of all existing or future legislation aiming at tackling (some forms of) online harassment within the EU, this section will draw a general picture of the existing or proposed norms in order to highlight their main gaps or flaws. Yet, it must be kept in mind that painting a detailed picture of the legislative landscape meant to tackle online harassment falls far beyond the scope of this study. Hence, the below analysis is in no way meant to be comprehensive. Rather, it focuses on the most apparent gaps and weaknesses of anti-harassment legislation, as already identified and discussed in the media, political debates or the relevant literature. This will in turn enable the author to show how using the functional nature of EU data protection law could potentially fill these gaps or correct these flaws, for the benefit of human dignity, integrity and freedom of expression of victims of online harassment.

As further explained below, despite being recognised as a growing and serious issue,¹³¹³ there is, to date, no specific and comprehensive legislation at the EU level to tackle online harassment. Currently, the absence of a general legal framework is partly compensated by (i) self-regulation, (ii) national law targeting (some forms of) online harassment, or (iii) other (non-)binding EU law instruments which, although not specifically targeting online harassment, may become relevant in some instances (for example, the Directive on e-commerce, the Victims' Rights Directive, or the EU Code of Conduct against Hate Speech).

¹³¹³ See the various reports published by the EU institutions and/or the Council of Europe on multiple forms of online harassment and/or abuses: European Parliament (2016, August 30). *op. cit.*; European Parliament (2019, July). *op. cit.*; European Parliament (2018, September). *op. cit.*; Brown, A. (2020, May). *op. cit.*

4.1.3.1. Contractual or self-regulatory norms against online harassment: reliance on a (not-so) gentlemen's club?

Victims of online harassment may, in some instances, rely on private norms enacted by internet operators themselves to denounce or put an end to online attacks. For example, Facebook, Google or Twitter have their own set of rules (called Terms of Services,¹³¹⁴ Community Standards¹³¹⁵ or Community Guidelines¹³¹⁶) that explicitly deal with, *inter alia*, nudity, violence or hate speech, and which can result in either the refusal to publish a specific content or in the content being removed *a posteriori*.¹³¹⁷ On Facebook, YouTube and Twitter, bullying and harassment are two types of behaviours that are explicitly prohibited.¹³¹⁸

Because these rules are meant to regulate the relation between internet operators and their users, and/or among users of a given website between themselves, they are usually considered as being of a contractual nature. However, instead of being negotiated between the different parties involved, they are usually unilaterally established by the internet operators themselves. If an individual wants to create an account on Facebook, for example, he/she has no other choice than accepting the terms of services and community standards of Facebook. Among all these terms or standards, it may happen that some rules go beyond what is formally required by the applicable laws of the countries or region where the company operates. In other words, some internet operators voluntarily enact internal rules that fill the current legislative gaps in this matter.¹³¹⁹ Because of this specificity, these norms are usually labelled as 'self-regulatory'.

Self-regulation against online abuses may represent an important first layer of protection for victims of online harassment. To illustrate this, this section will focus in particular on the self-regulatory systems put in place by three major internet

¹³¹⁴ On Google, for example, <https://policies.google.com/terms?hl=en-US>

¹³¹⁵ On Facebook, for example: <https://www.facebook.com/communitystandards>

¹³¹⁶ On Youtube, for example, <https://www.youtube.com/howyoutubeworks/policies/community-guidelines/>.

¹³¹⁷ Roberts, S. (2019). *Behind the screen. Content moderation in the shadows of social media*. Yale University Press; Common, M. F. (2020). Fear the Reaper: How Content Moderation Rules Are Enforced on Social Media. *International Review of Law, Computers & Technology*, 34(2): 126-52; Jhaver, S., Ghoshal, S., Bruckman, A., & Gilbert, E. (2018). Online Harassment and Content Moderation: The Case of Blocklists. *ACM Transactions on Computer-human Interaction*, 25(2):1-33.

¹³¹⁸ In its *Rules & Policies*, Twitter provides: "You may not engage in the targeted harassment of someone, or incite other people to do so. We consider abusive behavior an attempt to harass, intimidate, or silence someone else's voice." (see <https://help.twitter.com/en/rules-and-policies/abusive-behavior>). In a similar way, Facebook states in its Community standards: "Bullying and harassment happen in many places and come in many different forms, from making threats to releasing personally identifiable information, to sending threatening messages, and making unwanted malicious contact. We do not tolerate this kind of behavior because it prevents people from feeling safe and respected on Facebook." See <https://www.facebook.com/communitystandards/bullying>. Youtube also has an anti-harassment and cyberbullying policy which may lead to the removal of videos from its platform: https://support.google.com/youtube/answer/2802268?hl=en&ref_topic=9282436.

¹³¹⁹ See, on this topic, Quintel, Teresa & Ullrich, Carsten (2020). Self-Regulation of Fundamental Rights? *The EU Code of Conduct on Hate Speech, related initiatives and beyond*. Petkova/Ojanen (eds.) *Fundamental Rights Protection Online: The Future Regulation of Intermediaries*. Elgar; Cole, M., Etteldorf, C. & Ullrich, C. (2021). Updating the Rules for Online Content Dissemination - Legislative Options of the European Union and the Digital Services Act Proposal. *Schriftenreihe Medienforschung der Landesanstalt für Medien NRW*, 83.

operators whose websites or platforms are widely used by billions of individuals over the world: Meta (which owns Facebook, but also Instagram and WhatsApp), Google (which, beyond its search engine, also owns the video sharing platform YouTube) and Twitter. Of course, online harassment as a social phenomenon is not limited to these websites or platforms; some attacks may indeed be conducted on comparably big or smaller websites or apps that may have or do not have comparable self-regulatory standards against online abuses. However, when it comes to the effects of online harassment, it must be acknowledged that they are usually more devastating when the attacks are conducted in a place where the victim is usually conducting part of his, her or their social or professional life. The disruption in the life of the victims via these social media platforms may thus be perceived as more intense because depriving them of the possibility to continue using those websites in the normal course of their life. Hence, the self-regulatory standards enacted by those social media platforms are particularly relevant in the context of this study.

Meta, Google and Twitter have a particularity in common: their website or platforms are based on the content generated by their users. In other words, they do not create content themselves, but enable their users to create, publish and/or share content (e.g., emails, messages, videos, photos, 'stories', likes, tweets, etc). Due to the industrial scale at which these three major companies are operating, their self-regulatory measures generally focus on the *content* of the publication, rather than on both the content and the *context*.¹³²⁰ Posting pictures depicting sexual intercourses on Facebook, for example, is not allowed, regardless of whether such pictures are posted for the purpose of artistic expression, body liberation or harassment.¹³²¹ The prohibition is thus 'absolute'. As an exception however, some self-regulatory standards have been elaborated to take both the content *and* the context of the publication into account for determining whether it should be allowed or not. On Facebook, for example, while it is normally not allowed to publish pictures displaying female nudity, and in particular pictures where the nipples of a woman are visible, such pictures are permitted when they depict acts of protest (e.g., Femen movement), breastfeeding, or post-mastectomy scarring.¹³²²

As far as online harassment is concerned, it must be observed that, beyond the actual content of the publication, the *context* is particularly important in distinguishing harmful communications from legitimate ones. If a person publishes under somebody else's profile the statement "*I'm gonna kill you!*", only the context

¹³²⁰ Caplan, R. (2018, November 14). Content or Context Moderation? *Data & Society*. https://datasociety.net/wp-content/uploads/2018/11/DS_Content_or_Context_Moderation.pdf.

¹³²¹ Facebook Community Standards (2021 version). Article 14: Adult nudity and sexual activity. https://www.facebook.com/communitystandards/adult_nudity_sexual_activity.

¹³²² Article 14 of Facebook Community rules states in this respect: "*Our Nudity Policies have become more nuanced over time. We understand that nudity can be shared for a variety of reasons, including as a form of protest, to raise awareness about a cause or for educational or medical reasons. Where such intent is clear, we make allowances for the content. For example, while we restrict some images of female breasts that include the nipple, we allow other images, including those depicting acts of protest, women actively engaged in breastfeeding and photos of post-mastectomy scarring.*"

(including, for example, the type of relationship between the two persons, the rest of the conversation (if any), or the use of emojis accompanying this text) can help determining whether such a statement must be interpreted as a joke, a hyperbolic assertion or as an actual death threat.¹³²³ Similarly, an originally ‘harmful’ publication can sometimes be re-posted or shared by another user not with the intention to further harm a person, but on the contrary for the purpose of denouncing it or for raising awareness on an issue.¹³²⁴ In this last scenario, while the content of the publication may appear unacceptable at first sight, the context in which it is posted may render it compliant with the anti-hate speech or anti-harassment rules.

Because of the importance of the overall context, the task of distinguishing harmful communications from legitimate ones often proves difficult and may lead to two types of labelling errors:¹³²⁵ (i) false negatives or (ii) false positives. In the first case-scenario, an abusive publication is considered as acceptable and left on the concerned platform (although it does contradict the anti-harassment policy of that platform) while, on in the second case-scenarios, a legitimate publication (for example, in the form of a sarcastic comment) is wrongly considered as injurious and taken down from the platform.

Due to the immense amount of content that is published on social media every day, all major operators rely on technical solutions to moderate their platform. These technical solutions normally require the use of algorithms (hereafter referred to as ‘algorithmic moderation systems’ or ‘AMS’).¹³²⁶ Usually, two different stages can be distinguished in every moderation process: (1) flagging and (2) filtering. AMS can be used alone or in combination with humans at each of these stages.

The first stage of content moderation (‘flagging’) consists in identifying content that may be in breach of the applicable rules. If conducted by an AMS, this operation is usually referred to as ‘automated flagging’.¹³²⁷ Next to those AMS, however, most of the major internet operators also rely on their own users to flag content (this is the

¹³²³ For example, Article 1, para. 1 of Facebook Community Standards states: “(...) *We remove content, disable accounts and work with law enforcement when we believe that there is a genuine risk of physical harm or direct threats to public safety. We also try to consider the language and context in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety. In determining whether a threat is credible, we may also consider additional information such as a person’s public visibility and the risks to their physical safety.*”

¹³²⁴ For example, Article 14, para. 3 of Facebook Community Standards states: “*Sometimes people share content containing someone else’s hate speech for the purpose of raising awareness or educating others. In some cases, words or terms that might otherwise violate our standards are used self-referentially or in an empowering way. People sometimes express contempt in the context of a romantic break-up. Other times, they use gender-exclusive language to control membership in a health or positive support group, such as a breastfeeding group for women only. In all of these cases, we allow the content but expect people to clearly indicate their intent, which helps us better understand why they shared it. Where the intention is unclear, we may remove the content.*”

¹³²⁵ Sartor, G. & Loreggia, A. (2020, September). *The impact of algorithms for online content filtering or moderation*. Policy Department for Citizens’ Rights and Constitutional Affairs. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU\(2020\)657101_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf).

¹³²⁶ Gorwa, R., Binns, R. & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big data & society*, 7(1).

¹³²⁷ Gillespie, T. (2018), *op. cit.*

case, for example, on Facebook, YouTube or Twitter). Hence, if a user considers a specific publication as problematic or contrary to the applicable company's rules, they can notify the platform about it. Usually, those reporting tools are available next to each publication and only require a few clicks to be activated. Users are however rarely given the possibility to explain, in their own words, why the content is problematic, and they are usually not informed about the procedure or the final decision taken by the operator with respect to the flagged content.¹³²⁸ Despite these flaws, the possibility for users to report problematic content remains particularly important for victims of online harassment, since they usually have a better understanding of the overall context.

After a content has been flagged as potentially harmful (either by an AMS or by a user), the decision to keep or reject the content must be taken by the internet operator. This second stage is usually referred to as 'filtering'. Filtered content is either (i) not published at all (ex-ante filtering), (ii) taken down/deleted after its publication (ex-post filtering) or (iii) allowed/accepted (in which case, it is left or reinstated on the platform).¹³²⁹ Filtering is either fully automated, conducted by a human reviewer, or performed through a combination of AMS and human moderators. Fully automated filtering (without any human intervention) is often used by internet operators in instances where the infringement to the applicable rules is straightforward and can be automatically detected by an AMS (for example, the publication of copyrighted material,¹³³⁰ or an attempt to publish a content which has already been labelled in the past as contrary to the applicable rules, such as a racist comment or a video depicting nudity). In those cases, the upload of the litigious content on the platform can be detected by a content matching technology and can lead to its automated rejection (ex-ante filtering) or deletion (ex-post filtering).¹³³¹

Among existing content matching technologies, 'image hashing'¹³³² is widely used by all major operators to moderate photo and video content. As an illustration, the company administrating Pornhub is currently employing an image hashing

¹³²⁸ Carlson, C. R. & Rousselle, H. (2020). Report and repeat: Investigating Facebook's hate speech removal process. *First Monday*, 25(2).

¹³²⁹ Gorwa, R., Binns, R. & Katzenbach, C., (2020), *op. cit.*

¹³³⁰ Sartor, G. & Loreggia, A. (2020, September). *op. cit.*, p. 23.

¹³³¹ Cambridge Consultants (2019). Use of AI in content moderation. *Ofcom*. https://www.ofcom.org.uk/data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf.

¹³³² Image hashing is a mathematical process relying on cryptography which translates any image or a sequence of images into a unique string of data called a 'hash'. In that context, a hash can thus be compared to a digital fingerprint of an image or video. Image hashing is a one-way process, in the sense that any image can be turned into a unique hash, but that hash itself cannot be decrypted to recreate the image that it corresponds to. Hence, operators can store those hashes for the purpose of preventing a given image/video from being uploaded on their platforms, without being taxed of conserving litigious or illegal content.

technology developed by Vobile¹³³³ for preventing the upload and sharing of non-consensual pornographic videos or rape videos on Pornhub – a phenomenon which has been plaguing the adult videos website and has had devastating consequences on its victims.¹³³⁴ Facebook and YouTube also rely on image hashing to prevent copyrighted or harmful content from being (re)uploaded on their platforms.

As far as online harassment is concerned, in November 2017, Facebook even went a step further by launching a pilot program through which individuals who were fearing that intimate images of them were at risk of being shared were given the possibility to preventively act upon it.¹³³⁵ This pilot program is today known as ‘Not Without My Consent’, and allows users to securely and proactively submit to Facebook one or several ‘hashed’ sensitive picture(s) or video(s) of them.¹³³⁶ These hashes are then kept by Facebook with a view of automatically blocking any attempt by another user to publish such pictures/videos.¹³³⁷ This ex-ante filtration process, designed to proactively combat revenge porn on Facebook, is however limited in scope. Other forms of online harassment do not benefit from the same scheme and may be more difficult to detect and suppress.

Another form of *ex ante* type of filtering that may exist on social media or communication services consists in allowing the users themselves to block certain other users. This is the case, for example, on Facebook, WhatsApp, or Twitter, where each user may actively select and block one or multiple other users based on a unique identifier, such as their profile name or phone number. These other users are thereby prevented to directly communicate with the person who has blocked them on the concerned platform or service.¹³³⁸ The scope of this type of *ex-ante* filtering is however here limited to specific channels of communications on a given service or platform between the blocked users and the user who blocked them. Furthermore,

¹³³³ In a statement to the BBC, Pornhub has described Vobile as “a state-of-the-art third-party fingerprinting software, which scans any new uploads for potential matches to unauthorised material and makes sure the original video doesn’t go back up on the platform”. Source: <https://www.vobilegroup.com/about-vobile>. See, also, Mohan M. (2020, February 10). I was raped at 14, and the video ended up on a porn site. <https://www.bbc.com/news/stories-51391981>.

¹³³⁴ Kristof N. (2020, December 4). The Children of Pornhub. *New York Times*. <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>; Lamy C. (2020, December 9). Mise en cause par le New York Times, le site pornographique Pornhub annonce des mesures. *Le Monde*. https://www.lemonde.fr/pixels/article/2020/12/09/mis-en-cause-par-le-new-york-times-le-site-pornographique-pornhub-annonce-des-mesures_6062782_4408996.html ; Grant, H. (2020, March 9). World’s biggest porn site under fire over rape and abuse videos. *The Guardian*. <https://www.theguardian.com/global-development/2020/mar/09/worlds-biggest-porn-site-under-fire-over-videos-pornhub>.

¹³³⁵ See, in particular, this communication from Facebook: <https://about.fb.com/news/h/non-consensual-intimate-image-pilot-the-facts/>

¹³³⁶ See, in particular, this communication from Facebook on the project “Not without my consent”: <https://www.facebook.com/safety/notwithoutmyconsent>

¹³³⁷ This pilot program, relabelled “Not Without My Consent”, is conducted in cooperation with country-specific organisations that are already active in the field of internet safety. While initially launched in Australia, it has now been extended to Asia, North America and Europe. In Europe, this pilot is currently limited to Italy and the UK. See <https://www.facebook.com/safety/notwithoutmyconsent/pilot/partners>.

¹³³⁸ As far as Twitter is concerned, see, for example: Jhaver, S., Ghoshal, S., Bruckman, A., & Gilbert, E. (2018). Online Harassment and Content Moderation: The Case of Blocklists. *ACM Transactions on Computer-human Interaction*, 25(2):1-33.

the act of blocking is performed by a user rather than by an algorithm. Hence, this type of blocking is not made by AMS and does not qualify *stricto sensu* as ‘content moderation’, even if it can play an important role as well in the context of online harassment.¹³³⁹

Despite the absence of clear numbers,¹³⁴⁰ it is suspected that a substantial part of the filtering process on all major social media platforms is conducted by AMS alone, i.e., without the intervention of any user or human moderator.¹³⁴¹ Yet, when it comes to more subtle semantic content, AMS are not always performant enough to distinguish legitimate communications from illegal or harmful ones. This is because AMS are usually context-blind and thus produce highly inaccurate results when it comes to detecting forms of online harassment that are intrinsically linked to the context.¹³⁴² This is the case in particular for semantic or verbal communications that require a subjective interpretation. Whether such communications consist in harassment may depend on many factors such as the relationship between the users, their social/cultural background, the use of irony, parody or sarcasm, the use of emoticons, etc.¹³⁴³ For instance, the word ‘nigga’ which has historically been used as a racial slur might be considered as hateful if used by a white person against a man of colour, but can also be used as a self-empowering word by members of the black community among themselves.¹³⁴⁴ Similarly, the word ‘bitch’ might either be used in an insulting manner against a woman, or in an affectionate or empowering manner by a woman, depending on the relationship between the two persons concerned, or the use of emoticons or emojis accompanying such a word (e.g. “you stupid bitch!!” vs. “I love you, bitch <3”). Algorithms are today not capable of detecting parody, sarcasm, re-appropriation of slurs or irony, thereby increasing the risk of undue censorship through automated removal by AMS.¹³⁴⁵ For more complicated cases of content moderation, including verbal or figurative communications which are context-dependent, a hybrid approach involving both

¹³³⁹ *Ibid.*

¹³⁴⁰ Not all operators relying on AMS to moderate their platforms are transparent in this respect. Furthermore, among operators who do publish transparency reports on content moderation, some data may be missing. In their 2020 reports, for example, Facebook and Youtube both reveal the percentage of content that has been flagged and taken down, and further make a distinction between content that has been flagged by AMS or by users. However, these reports remain silent on the percentage of content which has been automatically taken down by AMS (i.e., without any human review).

¹³⁴¹ Caplan, R. (2018, November 14). *op. cit.*, pp. 23-24; Seering, J., Kraut, R. & Dabbish, L. (2017). Shaping pro and anti-social behaviour on twitch through moderation and example-setting. *ACM*. <https://dl.acm.org/doi/10.1145/2998181.2998277>; Jhaver, S. & al. (2019). Human-machine collaboration for content regulation: The case of Reddit Automoderator. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26(5): 1-35.

¹³⁴² Gillespie, T. (2020), *op. cit.*

¹³⁴³ Cows, J. & al. (2020). *op. cit.* p. 7.

¹³⁴⁴ Bradford B. & al. (2019). Report of the Facebook Data Transparency Advisory Group. *Yale Law School*, p. 12; Galinsky, A. D. & al. (2013). The Reappropriation of Stigmatizing Labels: The Reciprocal Relationship Between Power and Self-Labeling. *Psychological Science*, 24(10):2020–2029; Netflix (2021). *The History of Swear Words*. Season 1, Episode 3 (“Bitch”).

¹³⁴⁵ Council of Europe (2017). *op. cit.*, p. 21.

AMS and human decision-making is thus usually preferred by social media platforms.¹³⁴⁶

On big platforms, when the decision to accept or reject a flagged content cannot be taken by fully automated means, the flagged content is usually put in a 'queue' before being subject to human review.¹³⁴⁷ Those human reviewers are usually referred to as '*content moderators*';¹³⁴⁸ they may be employees of the operator itself, or of a sub-contractor, and are given the task to confirm whether the flagged content contradicts the rules of the platform or not.¹³⁴⁹ It must be stressed, however, that the number of these human moderators are limited, and that they can themselves be context blind to some situations. Human moderators can thus still commit mistakes when taking the decision to accept or reject a specific post in accordance with the standards or rules of the concerned operator.

Regardless of the methods used, what must be stressed out is that each operator decides how content is moderated on its platform in accordance with its own internal standards and rules. In other words, moderation standards and rules are primarily established by private actors with no democratic legitimacy and are later enforced by those same actors without the oversight of public authorities. Over time, quite foreseeably, various issues have thus arisen in relation to content moderation by major internet operators, causing a lot of ink to be shed on this topic. Those issues range from concerns over undue censorship (where content is wrongfully or arbitrarily removed, thereby interfering with freedom of expression),¹³⁵⁰ to labour concerns (about the working conditions and mental health problems faced by content moderators),¹³⁵¹ to the relative inability of platforms to prevent hate speech, misinformation or manipulation (including with respect to

¹³⁴⁶ Sartor, G. & Loreggia, A. (2020, September). *op. cit.*, p. 23.

¹³⁴⁷ Lyons K. (2020, August 25). YouTube took down more videos than ever last quarter as it relied more on non-human moderators. *The Verge*. <https://www.theverge.com/2020/8/25/21401435/youtube-videos-moderators-filters-human-appeals>.

¹³⁴⁸ The documentary film « The Cleaners » by Hans Block und Moritz Riesewieck depicts the difficult work of those individuals, and beyond the psychological impact, shows the many errors that human operators may commit while reviewing content because of their own cultural/social background, the lack of time or bias.

¹³⁴⁹ Although insufficiently, according to Common and other scholars. See, among others: Common, M. F. K. (2020). Fear the Reaper: How Content Moderation Rules Are Enforced on Social Media. *International Review of Law, Computers & Technology*, 34(2): 126-52.

¹³⁵⁰ Balkin, J. M. (2018). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *UC Davis Law Review*, 51:1149, p.1153; Gillespie T. (2020), *op. cit.*; Cowls, J. & al. (2020), *op. cit.* The report and articles to which this study refers only represent a drop in the ocean of publications that is available on that topic.

¹³⁵¹ Arsht A. & Etcovitch D. (2018, March 2). The Human Cost of Online Content Moderation. Commentary. *Harvard Journal of Law & Technology*. <https://jolt.law.harvard.edu/digest/the-human-cost-of-online-content-moderation>; Newton C. (2020, May 13). Half of all Facebook moderators may develop mental health issues. *The Verge*. <https://www.theverge.com/interface/2020/5/13/21255994/facebook-content-moderator-lawsuit-settlement-mental-health-issues>. See, also, « The Cleaners », a documentary film directed by Hans Block und Moritz Riesewieck.

political elections or in the context of a pandemic),¹³⁵² to criticism about the legitimacy of big platforms to unilaterally establish standards with respect to content moderation, to the general lack of accountability of the concerned operators.¹³⁵³ It would of course go beyond the scope of this study to analyse and discuss each of these issues. Rather, it suffices, for the purpose of this study, to highlight the limited effectiveness of those rules in combatting online harassment.

For victims of online harassment, the self-regulatory measures adopted by major internet operators such as Media, Google or Twitter can represent an important first layer of protection. Yet, it must be acknowledged that those self-regulatory measures also suffer from severe flaws that undermine their overall effectiveness or functionality in combatting online harassment. Among these flaws, the following may be considered as the most important ones:

- 1) Limited ‘territorial’ scope:** one of the main flaws of those self-regulatory rules when it comes to combatting online harassment is that they are only applicable on the platforms/websites of the operators who have adopted them. As explained above however, online harassment is usually conducted through various channels, including in different online spheres (mailbox; social media; messaging apps; adult websites; etc.). The fact that a victim has successfully reported a form of harassment on *one* platform does not mean that the harmful content will be prevented from appearing on other platforms or websites. Most importantly, many smaller websites and/or applications do not necessarily have self-regulatory rules or enforcement mechanisms in place to combat online harassment (or one of the forms that it can take). In other words, the level of protection afforded to victims of online harassment by self-regulatory measures is ‘territorially’ limited to online platforms, websites or applications which have adopted such rules.

- 2) Lack of harmonised material scope:** another issue is that different platforms may abide to different definitions and/or enforcement practices with respect to the same issue. In particular, some operators can be more protective or,

¹³⁵² Kramer, A., Guillory, J. & Hancock, J. (2014). Experimental Evidence of Massive-scale Emotional Contagion Through Social Networks. *Proceedings of the National Academy of Sciences of the USA*, 111:8788; Shah, Dhavan V. & al. (2005). Information and Expression in a Digital Age: Modeling Internet Effects on Civic Participation. *Communication Research*, 35:531; Carlson, C. R. & Rousselle, H. (2020). *op. cit.*; Sartor, G. & Loreggia, A. (2020, September). *op. cit.*; ERGA (2020). Notions of Disinformation and Related Concepts Report. <https://erga-online.eu/wp-content/uploads/2021/01/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts.pdf>; European Commission (2018, April 26). Communication Tackling online disinformation: a European Approach. COM(2018) 236 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>; Baker, S. A., Wade, M. & Walsh, M. J. (2020). The Challenges of Responding to Misinformation during a Pandemic: Content Moderation and the Limitations of the Concept of Harm. *Media International Australia* 177(1): 103-07.

¹³⁵³ Citron, D. & Norton, H. (2011). Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age. *Boston University Law Review*, 91(4): 1435-1484; Gillespie, T. (2018). *op. cit.*; Katzenbach, C. & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review*, 8(4):118; Gorwa, R. & al. (2020). *op. cit.*; Suzor, N. P. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press; Flew, T., Martin, F. & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, 101:33–50.

on the contrary, more liberal with respect to online harassment, depending on the importance given to freedom of speech. As an illustration, a post may be considered as ‘hate speech’ and be prohibited on one platform, but not on another. Hence, victims of online harassment may be facing contradictory decisions by different platforms. Furthermore, harassers may be aware of those differences and take advantage of them by adopting, depending on each platform, a specific form of abuse that is likely to be ‘accepted’ by the operator. As an illustration, while posting an erotic video of a person without his/her consent on Facebook may lead to its swift deletion, this might not be the case on an adult website. On the other hand, while posting a video where a person recites an injurious poem on an adult website may lead to its deletion, it may be allowed on Facebook because considered as form of artistic expression.

- 3) Difficulties in detecting harassment because of the relevance of the context:** as discussed above, online harassment may take many forms. Some abuses can be quite conspicuous and clearly qualify as participating to online harassment, such as the non-consensual publication of intimate or sexually explicit images. Some other abuses may however be less evident because they are context dependent. Because AMS are often context-blind, they often fail at distinguishing abusive messages from legitimate communications; hence, attempts to combat online harassment via AMS may lead to a higher number of false positives or false negatives.¹³⁵⁴ Having recourse to human moderators may improve the overall records. Yet, as stressed above, human reviewers themselves may not be well aware of the overall context (e.g., lack of appropriate linguistic or cultural background, lack of knowledge regarding the pre-existing relationship of the users, etc) and therefore not react appropriately. Furthermore, it remains difficult for content moderators to detect these violations that are subjective by nature. Indeed, whether a communication is perceived as injurious or threatening will ultimately depend on the target’s perception or understanding.¹³⁵⁵ At the end of the day, the most relevant input comes from the users themselves, and in particular from the targeted victims. The possibility for a victim of online harassment to flag a specific content as abusive is thus crucial to help a platform better detect and prevent this type of behaviours. This system is however not available on every platform and does not systematically lead to swift or proper enforcement (see issue on the lack of transparency and accountability of platforms below).

¹³⁵⁴ Facebook, for example, admits in its 2020 Transparency report that the pro-active enforcement of its Community standards on the basis of AMS against cyber bullying and harassment led to an increased number of false positives in the third quarter of 2020: “Content actioned increased from 2.4 million pieces of content in Q2 2020 to 3.5 million in Q3 2020. This was partly due to an issue with our proactive detection technology **that caused us to mistakenly remove non-violating comments**, which we later restored. We also increased our automation abilities beginning in Q2. Our proactive rate increased from 13.3% to 26.4% for these same reasons” (emphasis added).

¹³⁵⁵ Bradford, B. & al.(2019), *op. cit.*, p. 7.

4) The issue with ex-post filtering and re-surfacing: an effective manner to combat online harassment is to prevent harasser to conduct an attack in the first place. The pilot program of Facebook against revenge porn offers a good illustration in this respect; if the harasser attempts at publishing the litigious photo/video, Facebook can preventively block it. For this to be possible, however, the victim must have proactively submitted the corresponding hashed pictures/videos to Facebook. Except for a handful of cases, ex-ante filtering remains quite rare in the context of self-regulatory measures against online harassment (also for obvious reasons relating to freedom of expression). In most cases, the filtering of harmful content is thus taking place *after* its publication. Hence, for a short or longer period of time, the publication is available online, and can be shared among users, ‘captured’ in the form of screenshots, or in some instances, even downloaded.¹³⁵⁶ As a consequence, the deletion of such content on a given platform (as well as the removal of any copies of it on that platform through the use of content matching technologies) may not prevent it from being further shared or published on other platforms, or even to later re-surface on the same platform.

5) Lack of transparency towards the victims with respect to enforcement: some operators, such as Facebook or YouTube, may publish quarterly, bi-annual or yearly reports on the enforcement of their community standards. These transparency initiatives usually give a general overview of the performance of platforms in enforcing their own rules but remain often meaningless at the level of each individual who suffered from online abuses. Once a victim of online harassment has reported a given content as abusive, there is indeed no systematic sharing of information regarding the process and/or the decision taken by the operator.¹³⁵⁷ Hence, victims must sometimes look themselves whether a specific content is still available on the platform to find out whether it has been taken down or not. Furthermore, in the context of ex-ante filtering or deletion of content *before* the victim has been able to view it, there is usually no notification to the victim. Hence, the victim can remain unaware of the origin and existence of an attack or series of

¹³⁵⁶ On PornHub, up until December 8, 2020, videos could be uploaded and downloaded by users. Hence, victims of revenge porn which may have successfully obtained the removal, by PornHub, of a non-consensual pornographic video, were not protected against the re-surfacing of that same video on different porn websites. This risk was increased by the important number of users who may have downloaded the litigious video at the time it was available on PornHub. See, on this issue, Russel B, “Pornhub limits uploads and disables downloads after New York Times exposé”, 8 December 2020, <https://www.theverge.com/2020/12/8/22164031/pornhub-upload-limit-blocked-download-nyt-kristof-child-abuse> ; referring to the article of Kristof N., “The Children of PornHub”, New York Times, 4 December 2020, <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>.

¹³⁵⁷ In the case of Facebook/Instagram, the lack of communications towards users has been expressly considered as problematic by the independent Advisory Group in charge of reviewing their transparency report. See Bradford B. et al (2019), Report of the Facebook Data Transparency Advisory Group, The Justice Collaboratory, Yale Law School, April 2019, p. 36.

attacks, and thus not be able to report them to the competent authorities. As an illustration, women who have taken part in the pilot program of Facebook “Not Without my Consent” are not notified of the attempts by one or multiple other users to upload the concerned pictures/videos on Facebook.¹³⁵⁸ As a consequence of this lack of transparency, victims are often deprived of important information on the frequency, numbers or forms of attacks, as well as on the users/accounts who have launched such attacks – information that usually play a crucial role in identifying and/or holding the harassers accountable.

- 6) Difficulties in holding harassers legally accountable:** some operators may punish harassers by temporarily or definitively disabling their account. Yet, those operators are usually not actively looking to identify the individual(s) behind those accounts, and do not share with the victim information that may help reveal their identity in order for the latter to be able to report them to the authorities. As a matter of general principle, operators only cooperate with the victim and/or the authorities when forced to do so.¹³⁵⁹ In other words, although some punitive measures may be taken against harassers by the operators, they usually do not permit to hold the harassers legally accountable for their actions and are rarely effective in preventing further attacks on the same or other platforms through different accounts.

Despite the above-listed flaws, self-regulation remains an essential part of any system seeking to prevent and combat online harassment. Operators should therefore be encouraged to further refine their policies and enforcement processes in accordance with the framework provided by national or EU law. In the opinion of the author, public authorities have a duty to further guide these operators towards that purpose by providing and updating a harmonised set of definitions, standards and obligations that could apply across various platforms and websites. The below sections will precisely aim at identifying the most relevant national and EU provisions for combatting online harassment as well as their main limitations.

4.1.3.2. National laws against online harassment: a fragmented system in a unified digital world

At the Member States level, several national laws aim at addressing online harassment, either by criminalising the behaviours of the harassers, or by holding the parties that (in)directly participate to such harassment criminally or civilly liable.

¹³⁵⁸ Declaration of the Head of Women Safety at Facebook during the 2020 Online CPDP Conference 27 January 2020, which the author of this study attended.

¹³⁵⁹ Exceptionally, they may also voluntarily disclose information to law enforcement in matters involving imminent risk of serious physical injury or death. In the case of Facebook/Instagram, the company publishes as part of its transparency initiative the number of requests from authorities to obtain users’ data (per country), including the percentage of access requests that have been granted. See, in this respect, <https://transparency.facebook.com/government-data-requests>.

Several Member States have also recently amended existing laws or adopted new laws to combat online harassment, either in general or by focusing on one or multiple specific form(s) of online harassment. Belgium and the Netherlands, for example, have both recently adopted a law against the non-consensual diffusion of sexually explicit images,¹³⁶⁰ thereby specifically targeting ‘revenge porn’, while in Ireland, the Parliament approved a more general bill prohibiting the recording, distributing or publishing of (i) intimate images or (ii) threatening or grossly offensive communications,¹³⁶¹ thereby covering various forms of online harassment, from revenge porn, to cyberbullying among minors, to targeted hate speech on social media. Other Member States, by contrast, have not reformed their national law to address this phenomenon, leaving no other choices to the victims but to rely on general provisions of criminal law condemning ‘traditional’ forms of harassment, even if not particularly fitted to the online world. This is the case, for example, of Luxembourg, where harassment is recognised as an offence in the Criminal code, but where no specific law or provision has been adopted to more efficiently tackle (one or multiple form(s) of) *online* harassment.¹³⁶²

In most Member States, regardless of whether legislative reforms have been adopted or not, the issue of online harassment is still usually addressed through the lens of criminal law. Yet, it is commonly agreed in the literature that criminal law mostly fails at effectively protecting the victims of online harassment due to its limited material and personal scope, as well as the lack of technical capabilities or knowledge of the enforcement authorities to address this type of claims, as further detailed below.¹³⁶³ The case of Julie Hainaut, presented at the beginning of this Chapter, illustrates the failure of the criminal justice system to hold harassers accountable. Indeed, despite the fact that Julie Hainaut filed multiple complaints with the police, and despite the fact that several harassers were identified and appeared before the French criminal courts, not one single harasser was held accountable in the end.

A first major issue in this respect relates to the lack of resources and expertise of the police force. Regarding the resources, first, it must be recalled that in most cases, the harassers may be numerous and conduct attack through various channels behind pseudonyms, anonymous accounts or VPN. Often, the police or the prosecutors are

¹³⁶⁰ In Belgium: *Loi du 4 mai 2020 visant à combattre la diffusion non consensuelle d’images et d’enregistrements à caractère sexuel*, M. B. 18/05/2020 ; in the Netherlands: *Wet van 27 september 2019 tot wijziging van onder meer het Wetboek van StrfRecht in verband met de herwaardering van de strafbaarstelling van enkele actuele delictsvormen*, which introduced Article 139h in the Dutch Criminal Code, valid as from 1 January 2020.

¹³⁶¹ Harassment, Harmful Communications and Related Offences Bill 2017, No. 63a of 2017, available at https://data.oireachtas.ie/ie/oireachtas/bill/2017/63/eng/ver_a/b63a17d.pdf.

¹³⁶² Victims may rely principally on Article 442-2 of the Luxembourg criminal code and on some provisions of the Luxembourg law of 11 August 1982 relating to private life, which both criminalise traditional forms of harassment, such as stalking, on Article 457-1 of the Luxembourg criminal code against racist or discriminatory speech.

¹³⁶³ Langlois, G. & Slane, A. (2017), *op. cit.*, p. 7; McCully, J. (2019, March 3). *op. cit.*, p. 2; Ankel, S. (2020, February 3). ‘Is this you?!’ How revenge porn victims are forced to deal with the incompetence of the police. *Insider*. <https://www.insider.com/revenge-porn-victims-and-the-law-2019-12>.

simply unable to track and identify the persons concerned because they do not have the necessary financial and technical means to do so.¹³⁶⁴ Second, the lack of knowledge and training of the police force in handling such complaints is also an issue. Quite famously, in 2014, when American journalist Amanda Hess attempted to report the harasser that was sending her online death and rape threats via Twitter, the officer handling her case asked, “*What is Twitter?*”.¹³⁶⁵ In the EU, victims of online harassment often experience similarly poor or ignorant reactions from the police when they attempt to file a claim,¹³⁶⁶ if they find the courage to do so.¹³⁶⁷

A second major issue, directly linked to the first one, is that online harassment rarely gets reported, mainly because of the lack of trust of the victims in the capabilities of the police to respond to it. Because of its nature, sexual online harassment in particular may be more difficult for a victim to report to the police than other forms of harassment. In a 2018 survey¹³⁶⁸ conducted in the UK on the phenomenon of revenge porn, it was found that a staggering 76% of respondents did not report the crime to the police mainly because they felt embarrassed and ashamed. And among the 24% of victims who *did* report their online harasser(s) to the police, only 4% successfully prosecuted their offender – and this, despite the UK having created a specific offence against revenge porn, unlike other EU Member States at the time.¹³⁶⁹

A third major issue in addressing online harassment through the lens of criminal law relates to the material scope of such norms, and in particular the legal definition of ‘harassment’ as an offence, or related offences; usually, provisions of criminal law require a certain threshold of seriousness, repetition and/or threat for a certain behaviour to be considered as unlawful. This is partly to remedy such an issue that some Member States have adopted specific provisions against revenge porn, on the basis of which the publication of *one* sexually explicit image of a victim, without her consent, may suffice to prosecute the harasser. Other forms of harassment, however, do not benefit from the same regime. Furthermore, the offence must be linked to an identifiable individual on the basis of the principle of personal criminal liability. In the online world, however it is easy for an individual to conduct many small attacks under various identities which, unless linked to one another and

¹³⁶⁴ European Parliament (2020, July). *op. cit.*, p. 52. Citron, D. (2014). Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace. *Journal of Law, Technology and the Internet*, 6:1-12, p. 5.

¹³⁶⁵ Hess, A. (2014, January 6). Why Women Aren't Welcome on the Internet. *Pacific Standard*. <https://psmag.com/social-justice/women-arent-welcome-internet-72170>.

¹³⁶⁶ De Vries, A. (2017, October 13). Wraakporno wordt strafbaar. *Social Media*. <https://socialmediadna.nl/wraakporno-wordt-strafbaar/>; Smith, J. (2016, May 10). Police reaction to revenge porn is playing into predators' hands. *The Guardian*; Ankel, S. (2020, February 3). *op. cit.*

¹³⁶⁷ Many women who fall victims to revenge porn, for example, are often reluctant to file a claim with the police because it may imply showing the litigious images or videos to the police officer(s) in charge of the investigation, the prosecutor(s) or other enforcement authorities. See North Yorkshire Police, Fire & Crime Commissioner (2018). *Suffering in Silence, Why revenge porn victims are afraid and unwilling to come forward because of a fear they'll be named and shamed – and why that needs to change*. Image-based Sexual Abuse Report 2018. <https://www.northyorkshire-pfcc.gov.uk/content/uploads/2018/11/Suffering-in-Silence-Report.pdf>.

¹³⁶⁸ *Ibid.* (in total, 92 victims of revenge porn were interviewed for that survey).

¹³⁶⁹ Section 33 of the UK Criminal Justice and Courts Act 2015 has indeed created a specific offence for the non-consensual diffusion of sexually explicit images.

appreciated together, do not meet the necessary threshold of seriousness, repetition and/or threat. In parallel, online harassment campaigns or online mob attacks, where many individuals send one insulting or threatening message, often falls short of the legal definition of “harassment” in many jurisdictions because, taken separately, these messages do meet the threshold of seriousness codified in the law.¹³⁷⁰ This is principally due to the fact that criminal justice systems were often built upon the concept of *personal* criminal liability rather than group or shared criminal liability. In the case of online mobbing, for example, the frequency, continuity, and offensive character of the attacks are usually clearly perceived as a form of online harassment by the victims. Yet, a majority of the members of the mob may have just sent one harmful communication and may thus not qualify as a ‘harasser’ under the applicable law. This is because the online mob is usually composed of hundreds or thousands of separate individuals whose actions, once analysed on a personal basis, do not meet the threshold or repeated harm required under criminal or tort law to qualify as *harassment*.

Another issue relates to the limited personal scope of anti-harassment laws, in the sense that criminal law usually focuses on the harasser, with no or little possibility for the victim to hold liable other parties which directly or indirectly enable the harassment, such as social media platforms or internet services providers (hereafter, generally referred to as ‘operators’).¹³⁷¹ There are of course some specific exceptions to this rule. France and Germany, for example, have each adopted ‘anti-hate speech law’ on the basis of which operators may be held liable for failure to properly monitor and, when required, take down unlawful content, including, for example, racial or sexist insults, or revenge porn. These laws (i.e., the so-called ‘Avia law’ in France and the NetzDG Act in Germany) have been putting additional pressure on operators for moderating content on their platforms. In Germany, for example, the new NetzDG Act provides fines of up to 50 million euros for social media companies that do not take quick steps to remove hate speech from their platforms. Similarly, in Belgium, the Law of 4 May 2020 against revenge porn provides for the possibility to prosecute and fine the operator which has enabled the diffusion of the sexually explicit images, such as the social media platform where it has been published. Yet, once again, the criminal liability of those operators is limited to instances where they have failed to withdraw the litigious publications after having been summoned by the competent authorities to do so,¹³⁷² that is, at a moment where the harm to the victim has already been done. Furthermore, the material scope of the law is limited to the on-consensual diffusion of sexually explicit images and does not cover other forms of online harassment, such as doxing or the publication of insulting or threatening messages. More general ‘anti hate-speech’ laws as adopted in France and Germany would therefore be preferable. Victims of online harassment could

¹³⁷⁰ McCully, J. (2019, March 3). *op. cit.*, p. 5.

¹³⁷¹ Langlois, G. & Slane, A. (2017). *op. cit.*, p. 7.

¹³⁷² Article 7 of the *Loi du 4 mai 2020 visant à combattre la diffusion non consensuelle d’images et d’enregistrements à caractère sexuel*, M. B. 18/05/2020.

indeed rely on these laws, in parallel to the applicable criminal law, in order to hold the operators liable. Yet, resorting to national anti-hate speech laws would only be feasible if (i) the victims are located in a jurisdiction where these laws apply (e.g., France, Germany); if (ii) the content indeed qualifies as illegal under the applicable law, and if (iii) the operator has failed to take it down after having been required to do so by the competent authorities. These national laws therefore still suffer from three important flaws when it comes to effectively protecting victims of online harassment in the EU: first, they only apply within a given territory and are thus at odd with the borderless nature of the internet (cf. limited territorial scope); second, they do not apply to part or some forms of harassment when the content concerned does not qualify as illegal under the applicable law (cf. a large number of small attacks perpetrated by an online mob could easily fall outside their scope of application) ; and third, these measures are punitive rather than preventive in the sense that, for the victim, the harm has already be done, and may even reappear (cf. issues relating to ex-post filtering and re-surfacing). It therefore clearly appears that a more harmonized and fitted legal response to online harassment is required. As stated above however, there is, to date, no comprehensive legislation at the EU level against the phenomenon of online harassment. Within the scope of their competences, the EU institutions have nonetheless already adopted various soft law or legislative instruments which, although not covering all aspects of online harassment, regulate some aspects of it. The below sections will briefly review them.

4.1.3.3. Brief overview of EU instruments for combatting some forms of online harassment

There are numerous pieces of EU law that can be relevant to combat some forms of online abuses. As already stated at the beginning of this Chapter however, this section is not meant to comprehensively review and analyse all these instruments of EU law, as this would go far beyond the scope of this study. Rather, the purpose of this section is to acknowledge that the GDPR is definitely not the only EU law instrument that can be relied on for the purpose of combatting online harassment, even if it may become handy in situations where other instruments are difficultly applicable, or not applicable at all. Hence, the author of this study will merely list and briefly describe the objective and material scope of these other EU law instruments, so as to highlight the complementary nature of the GDPR.

Among the EU soft-law and legislative instruments that may, in some instances, be used by victims of online harassment, one may refer, among others, to the e-Commerce Directive and the Digital Services Act,¹³⁷³ the revised Audio-Visual Media

¹³⁷³ (Proposal for a) Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Procedure 2020/0361/COD (to be published in the OJ).

Services Directive,¹³⁷⁴ the Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law,¹³⁷⁵ the EU Code of Conduct against Hate Speech Online,¹³⁷⁶ and several EU directives promoting equal treatment or combatting discriminatory behaviors in specific fields, including employment.¹³⁷⁷ The objective and material scope of these instruments will briefly be described here below, so as to highlight the functional and complementary nature of the GDPR.

(i) The e-Commerce Directive, the revised Audio-Visual Media Services Directive and the (upcoming) Digital Services Act

The word ‘harassment’ or ‘abuse’ does not appear in the text of the e-Commerce Directive. Indeed, the object of the e-Commerce directive is not to combat online harassment. Rather, its primary objective is to *“contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.”*¹³⁷⁸

As far as fundamental rights are concerned, the e-commerce Directive mainly aims at protecting freedom of expression by establishing that internet operators,¹³⁷⁹ and in particular providers of information society services such as Meta, TikTok or Google, can neither be put under a general obligation to monitor the information which they transmit or store, nor a general obligation to seek facts or circumstances indicating illegal activities.¹³⁸⁰ In other words, the e-Commerce Directive generally allows internet operators to remain neutral in relation to the content that transit through their platforms or websites, by providing that these operators cannot be held responsible *per se* in the event illegal activities are conducted by third parties through the use of their services. In parallel, however, the Directive allows Member States to adopt specific rules putting internet operators under the obligation to *“expeditiously”*¹³⁸¹ remove or disable illegal content hosted on their websites or

¹³⁷⁴ Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, OJ L 303, 28.11.2018, p. 69–92.

¹³⁷⁵ Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, p. 55–58.

¹³⁷⁶ European Commission. (2016, June 30). EU Code of Conduct on Countering Illegal Hate Speech Online. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=42985.

¹³⁷⁷ Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303, 2.12.2000; Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000, p. 22–26 ; and Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), OJ L 204, 26.7.2006, p. 23–36.

¹³⁷⁸ Article 1(1) of the e-Commerce Directive.

¹³⁷⁹ Referred to in the e-Commerce Directive as information society service providers, i.e., any natural or legal person providing an information society service (Article 2(a) and (b) of the e-Commerce Directive).

¹³⁸⁰ Article 15(1) of the e-Commerce Directive.

¹³⁸¹ Article 14(1)(b) of the e-Commerce Directive.

platforms upon becoming aware of it, and to cooperate with the competent authorities (such as the police force, a data protection authority or a national court) in order to detect and prevent certain types of illegal activities. This obligation to cooperate includes the obligation to “promptly”¹³⁸² inform the competent authorities about any alleged illegal activity taking place on their websites or platforms once they are (made) aware of it. This, in turn, can enable the competent authorities to adopt specific measures to put an end to illegal activities conducted online, such as ordering the removal of illegal content, as the case may be. However, the e-Commerce Directive itself does not define what must be considered as an illegal activity or as illegal content. Whether an activity or content is illegal must thus be determined through the lens of other EU or national law. At the EU level, for example, such illegal activity or content may include the dissemination of terrorist content,¹³⁸³ of child sexual abuse material¹³⁸⁴ or qualified hate speech.¹³⁸⁵ From the perspective of EU data protection law, it can also be considered that personal data that are being processed in breach of the GDPR can themselves be regarded as ‘illegal content’ in the sense of the e-Commerce Directive. This would however require a breach of the GDPR to be first established by a DPA or a national court. Hence, the e-Commerce Directive and the GDPR could be used in a complementary manner for the purpose of preventing or combatting the dissemination of harmful content. The baseline regulatory regime of the e-Commerce Directive has been complemented in 2018 by the revised Audio-Visual Media Services Directive, which imposes more obligations to one category of online platforms in particular: video-sharing platforms. According to that Directive, these platforms should take appropriate and proportionate measures, preferably through co-regulation, in order to protect the general public from illegal content (such as terrorist content, child sexual abuse material, racism, xenophobia or other hate speech), and to protect minors from harmful content. Although it may be invoked in some instances, the limited material scope of this Directive makes it inapplicable in most cases of online harassment.

Most EU Member States have transposed the e-Commerce Directive and the revised Audio-Visual Media Services Directive into national law, thereby offering the possibility for victims of online harassment to hold the concerned operators liable if they have remained passive after having been alerted about the existence of the harmful content. This presupposes however that the content published by the harasser is either manifestly illegal or has been characterized as illegal by a competent authority. Hence, these rules would only apply to *specific* cases of online harassment, where the content is not only harmful in the eyes of the victim but in

¹³⁸² Article 15(2) of the e-Commerce Directive.

¹³⁸³ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172, 17.5.2021, p. 79–109.

¹³⁸⁴ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA.

¹³⁸⁵ See, in particular, the Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, p. 55–58.

the eyes of society as a whole, in the sense that the law explicitly prohibits its dissemination. Furthermore, these rules cannot be used to hold the harassers themselves accountable, since they only apply to internet operators. By contrast, the GDPR applies to any content that includes personal data (even if such a content would be legal from the perspective of other legislations) and could be used to hold both internet operators and the harasser(s) accountable. Another important difference between the e-Commerce Directive and the GDPR is that the first instrument is a directive while the second is a regulation. Rules with respect to the obligations of internet service providers to take down illegal content have thus not been fully harmonized within the EU. This, of course, can become problematic since the digital world knows no borders, and harmful content can usually be accessed from anywhere in the EU.

The Digital Services Act, which amends and complements the e-Commerce Directive, is supposed to partially remedy those issues once it will be adopted and will enter into force. The Digital Services Act is a regulation that will directly apply across the EU and will thus bring more uniformity with respect to the obligations of digital service providers to prevent and combat illegal online activities. The need to specify and adopt stricter rules vis-à-vis digital services providers mainly stems from that fact that Member States were increasingly discussing or introducing new rules at the national level relating to diligence requirements for internet operators to better tackle illegal content, online disinformation or other societal risks.¹³⁸⁶ The Commission therefore saw the risk posed by diverging national laws that could negatively affect the internal market, taking into account the inherently cross-border nature of the internet. Although the European Parliament and Council have reached a political agreement on the new rules to be adopted on 23 April 2022,¹³⁸⁷ the final draft of the Digital Services Act must still be formally adopted and published in the Official Journal of the EU, and will only be applicable in 2024. In the meantime, some Member States, and in particular France and Germany, have already adopted stricter rules (see above, on the NetzDG Act and the Avia law). As briefly mentioned above however, this type of laws may still be considered as inefficient in the eyes of victims of online harassment given that the harm has, for a large part, already been done and that the content (if taken down) may still quickly reappear on the same or other platforms if no other measures are taken. With respect to re-surfacing or reappearance of harmful content on the same platform, however, the CJEU has already confirmed in the case *Glawischnig-Piesczek* that the national authorities of a Member State could deliver an injunction against a social media platform to delete not only the original harmful content, but also any subsequently uploaded content

¹³⁸⁶ Recital 2 of the (draft) Digital Services Act. See, in particular, European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.pdf.

¹³⁸⁷ European parliament (2022, July 5). Press release: Digital Services: landmark rules adopted for a safer, open online environment

that is identical or “*essentially unchanged*”.¹³⁸⁸ This, however, only concerns content that has already been declared illegal by a national court and which reappears on the same platform, as opposed to content which has been flagged by the victim or which re-surfaces on another platform.

In summary, both the e-Commerce Directive, the Audio-Visual Media Services Directive and the upcoming Digital Services Act are instruments that will probably continue playing an important role in combatting the dissemination of illegal content on the internet. As highlighted above, however, the material and personal scope of these instruments are limited in a manner that restrict their effectiveness and functionality when it comes to combatting online harassment, mainly because (a) not all forms of harassment involve the dissemination of (manifestly) illegal content in the sense of these instruments, and because (b) these rules are meant to regulate the behaviors of internet operators, by obliging them to take a more active role in combatting the dissemination of illegal content, but cannot be used to hold accountable the harassers themselves.

(ii) The EU Framework Decision against racist and xenophobic hate speech and the EU Code of Conduct against Hate Speech

This Decision provides that Member States must ensure that racist and xenophobic hate speech is punishable under criminal law. From a general perspective, this Framework Decision has served as a guideline for Member States to adopt new rules for preventing racist or xenophobic insults to be disseminated on the internet, including in the context of online harassment campaigns. This Framework Decision does not impose however more detailed or general obligations for combatting online harassment in its other forms. This is the reason why most provisions of criminal law at the national level prohibit racist or xenophobic expression, but do not regulate other forms of expression that can participate to online harassment, such as threats of physical violence, sexist insults or the non-consensual sharing of sexually explicit images.

Next to this Framework Decision, the European Commission entered into an agreement with Meta, Twitter, Microsoft and YouTube in 2016 in the form of the EU Code of Conduct on Countering Illegal Hate Speech Online. By approving this Code of Conduct, these big tech companies have agreed to review all reports of hate speech online within a 24-hour time frame. Although it has further encouraged debates and initiatives to limit abuses online, the major flaw of this Code of Conduct is its limited personal scope and its non-binding nature. As such, victims of online harassment may thus not rely on this Code to engage the liability of the concerned harassers or operators.

¹³⁸⁸ CJEU, Judgment of 3 October 2019, *Glawischnig-Piesczek*, Case C-18/18, para. 55.

(iii) EU anti-discrimination directives against racist, sexist or xenophobic communications

When online harassment includes racial, sexist or xenophobic attacks, EU anti-discrimination legislation may also come into play. The scope, content as well as weaknesses of such a legislation will however be analysed in the following section of this study, in the context of the second test area for assessing the multi-functionality of EU data protection (i.e., e-recruitment). It suffices to point out at this stage that EU anti-discrimination laws usually contains a special provision according to which harassment is deemed to be a form of discrimination *“when unwanted conduct [relating to gender, race, ethnicity or another protected characteristic] takes place with the purpose or effect of violating the dignity of the victim and of creating an intimidating, hostile, degrading, humiliating or offensive environment.”*¹³⁸⁹ The issue is that, within this same provision, it is also stated that: *“the concept of harassment may be defined in accordance with the national laws and practice of the Member States.”*¹³⁹⁰ Although giving the appearance of harmonisation, EU law thus leaves complete discretion to Member States regarding the possibility to tackle some forms of harassment by relying on anti-discrimination laws. This has led to a flagrant lack of harmonisation and legal effectiveness at the Member State’s level, as further discussed below.

In summary, a complex network of provisions of national or EU law may be invoked to combat some (specific) forms of online harassment by engaging the criminal liability of the harasser(s) or the criminal or civil liability of the concerned internet operator, when the latter fails to take down illegal content within the timeframe imposed by law. Yet, as discussed above, these norms are largely incomplete when it comes to addressing online harassment as a whole, mainly because of procedural hurdles or because of the limited material, personal or territorial scope of those provisions. Unlike most of these instruments, the GDPR is directly applicable, concerns both the harassers and the intermediaries, and can apply to any type of content as long as it includes personal data. In other words, the broad scope of the GDPR enables to fill in some of the gaps left by other instruments of EU law adopted to combat the sharing of illegal content or hate speech on the internet. It is probably for this reason that an increasing number of cases reaching DPAs seem to be concerned with online harassment.¹³⁹¹ The below section will focus on the question ‘if’, ‘how’ and ‘why’ the GDPR can or should be used to fill in the gaps left by national and EU law and protect the right to privacy, data protection, dignity and integrity of victims of online harassment.

¹³⁸⁹ See, for example, Article 2(3) of the Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, *OJ L 303, 2.12.2000, p. 16–22.*

¹³⁹⁰ *Ibid.*

¹³⁹¹ See references to the DPA cases in the following sections.

4.1.4. The GDPR as an alternative or complementary framework for combatting online harassment: evidence of the secondary functionality of EU data protection law

In the first Chapter of this study, the author has formulated the hypothesis that the GDPR could be used as a handy multi-functional toolbox for protecting data subject's fundamental rights and freedoms against a variety of data processing practices. Looking at the case-law of the CJEU, however, such multi-functionality appears deficient or underexploited, in view of the meagre number of cases where EU data protection law has actually been deployed for the defence of a fundamental right(s) *other* than privacy or personal data protection (cf. conclusion of Chapter 2, Section 2.3.4). In order to further understand and clarify the main causes behind this apparent shortfall in the fulfilment of the FRO of EU data protection law, the author of this study has decided to apply the GDPR within two 'test areas' where modern data processing practices have proven to interfere with DFR. The below section will precisely aim at testing the functionality of EU data protection law in the context of online harassment – i.e., the first 'test area' of this study. It will be analysed in particular whether EU data protection law could be used as a gap-filling framework to better protect the dignity, integrity and freedom of expression of victims of online harassment.

It should be admitted at the outset that the GDPR was not specifically conceived or envisaged by the EU legislator as a legal instrument to tackle online harassment. There is, indeed, not one single reference to cyberbullying, doxing or other abusive online behaviours in the text of the GDPR. Some have thus described the GDPR as "*not fit for purpose*" when used, for example, to combat online impersonation or the non-consensual publication of sexually explicit images.¹³⁹²

In the opinion of the author, however, this statement must be nuanced. First, it must be noted that nothing in the GDPR indicates that it would not be applicable to cases of online harassment. As a result, the general rules and exceptions applicable to any processing of personal data would also apply to cases of online harassment. Second, as further demonstrated below, the scope and tools of the GDPR can be functional for combatting most forms of online harassment, either as an alternative or in complement to other legislative tools. For the sake of clarity, this section will be structured around two main questions: (1) to what extent is the GDPR applicable to cases of online harassment? (i.e., questions relating to scope of the GDPR); and (2) which tools provided in the GDPR could be particularly functional against (some sort of) online harassment? (i.e., questions relating to the convenience with which victims can rely on the GDPR to protect themselves).

¹³⁹² Cater, L. (2021, January 13). How Europe's privacy laws are failing victims of sexual abuse. *Politico*. <https://www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/>.

4.1.4.1. The applicability of the GDPR to cases of online harassment

This section will analyse which forms of online harassment could fall within the material and territorial scope of the GDPR, and therefore provide data subjects, DPAs and courts with tools to combat such harmful practices.

(i) As a general rule, all forms of online harassment fall within the material scope of the GDPR, including when false information about an unnamed victim is being processed

As far as the material scope of the GDPR is concerned, the latter would apply as soon as '*personal data*' of the victim are being '*processed*'. As discussed in the previous Chapter of this study, both the notion of personal data and the notion of processing have been broadly defined and interpreted in the case-law of the CJEU.¹³⁹³ In particular, three key criteria need to be fulfilled for an harassment practice to qualify as processing of personal data : the harasser(s) must be (1) *processing by automated means*; (2) of *information relating to a natural person* (3) who is either *identified or identifiable*.

The first criterium is without any doubt the easiest to fulfil, given the broad definition given to the notion of '*processing*', and the fact that online harassment involves, by definition, the use of ICT connected to the internet. Hence, any online harassment practice where information relating to the victim would be hacked, copied, transferred, published, shared, disseminated or otherwise processed via a smartphone, computer, an app or on social media, would, in principle, qualify as '*processing by automated means*' and trigger the application of the GDPR.

As far as the data themselves are concerned, anything that is '*information*' can fall under the concept of personal data, irrespective of its nature, content or format.¹³⁹⁴ Of particular importance in this respect is the fact that the information in itself does not need to be accurate to qualify as '*personal data*', as long as it relates to an identifiable individual; hence, even deepfakes, photo montages or an outdated data relating to the victim would qualify as '*personal data*' under the GDPR, and could thus trigger its application.¹³⁹⁵ If, for example, an ill-intentioned individual publishes on a pornographic website a video of one of his ex-girlfriends, it does not matter whether such a video consists in a real-life recording or a deepfake. In both cases, it still constitutes information as understood under the GDPR. Similarly, if a harasser creates a fake profile on a dating app and shares the postal address of a victim with third parties, inviting them to '*come over*' while the victim never agreed to this, it does not matter whether the given postal address is outdated or inaccurate; in both

¹³⁹³ See section 3.1.1, above.

¹³⁹⁴ van der Helm M. (2021, December 10). Harmful deepfakes and the GDPR. Master's Thesis Law and Technology. Tilburg University. <http://arno.uvt.nl/show.cgi?fid=156861>, p. 24.

¹³⁹⁵ *Ibid.*

cases, it still constitutes information relating to the victim, given that such postal address is linked to her profile.

Finally, for the GDPR to apply, the information must also 'relate to' the victim. As discussed above,¹³⁹⁶ the EDPB and the CJEU have adopted a broad interpretation of this notion by considering that information may relate to a person either in *content, effect or purpose*.¹³⁹⁷ Hence, virtually all information used in the context of online harassment may be considered as 'relating to' the victim, either because it provides information *about* the victim (e.g. a photo, a name, a profession, a gender, an ethnicity, etc.), because it will have negative effects on the emotional stability or mental health of the victim (e.g. threats to rape or kill the victim to upset or scare him or her), and/or because the objective is to obtain a certain result (e.g. spreading false information about the victim so that the latter loses his/her job, closes a social media account or accepts to give the harasser a favour or monetary gain).

To illustrate this, one may cite the harassment campaign which took place on Twitter against Greta Thunberg after her speech before the United Nations. Some individuals mocked her Asperger's syndrome, calling her "*deeply disturbed*";¹³⁹⁸ some other people insulted her or formulated explicit death wishes against her;¹³⁹⁹ while others taunted her by stating, for example, that they were about to eat a big steak, or that they had just booked long haul flight tickets for their entire family and felt "*no guilt*" about it.¹⁴⁰⁰ The mention of her name in these tweets or the tagging of her Twitter account undeniably consist in the processing of her personal data, since Great Thunberg is thereby specifically identified. Moreover, some of the comments themselves may qualify as personal data when relating to her in content, effect or purpose. For example, comments mocking her mental condition could be considered as information *in content*, while posts wishing her death or mocking her could be considered as information *in effect or in purpose*, in the sense that the impact or objective of these tweets was to daunt her. Based on these considerations, the author of this study considers that the vast majority of information used to harass a person online can be considered as information relating to that person either in content, or in effect or purpose.

The last important criterium is the fact that the victim whose data are being processed must be *identified or identifiable*. In accordance with the notion of identifiability, the victims must not always be identified by name in the context of

¹³⁹⁶ See, in particular, section 3.1.1.2, above.

¹³⁹⁷ CJEU, Judgment of 20 December 2017, *Nowak*, Case C-434/16, para. 35.

¹³⁹⁸ Hitchings-Hales, J. (2019, September 2). Greta Thunberg Tells Twitter Trolls: Asperger's is a 'Superpower'. <https://www.globalcitizen.org/en/content/greta-thunberg-aspergers-superpower-trolls-autism/>.

¹³⁹⁹ Busby, M. (2019, August 15). Arron Banks jokes about Greta Thunberg and 'freak yachting accidents'. *The Guardian*. <https://www.theguardian.com/uk-news/2019/aug/15/arron-banks-jokes-about-greta-thunberg-and-freak-yachting-accidents>.

¹⁴⁰⁰ Ball, S. (2019, August 15). A British media personality tried to mock teenage climate activist Greta Thunberg—and got promptly ratioed. *Daily dot*. <https://www.dailydot.com/unclick/greta-thunberg-julia-hartley-brewer-climate-change/>.

the harassment practice to benefit from the protection of the GDPR, as long as they remain identifiable, taking into account all the means that are “*reasonably likely*” to be used for their identification.¹⁴⁰¹ This test thus requires a case-by-case analysis of the relevant facts in order to determine whether the information processed in the context of the harassment enables to identify the victim. Comparably to the two previous criteria, it can reasonably be assumed that this identifiability condition is normally fulfilled in the context of online harassment since, by definition, online harassment is targeted at one or more specific individuals with the intention to upset them or cause them harm. In other words, harassment normally presupposes that the victim is identified or at least identifiable to achieve its purpose.

In most instances, online harassment is taking place on websites or social media where the victims are properly *identified*, either by their full name or by a pseudonym. Greta Thunberg and Julie Hainaut, for example, were both identified by their full name during the harassment campaign directed against them. Similarly, female gamers who are harassed online are usually identified by a unique pseudonym attached to their gaming persona.¹⁴⁰² In both these cases, the victims can be differentiated from other users and are thus clearly ‘identified’ in the sense of the GDPR.

In other instances, the harassment can consist in the sharing of (sensitive) information about the victims in a manner which enables their identification, and therefore make them *identifiable*. For example, the fact that a woman is insulted by a man who describes her as his ‘ex’ is an element which can make the victim identifiable, even if her full name is not revealed. Similarly, sharing information about the physical appearance of the victims, including in the form of pictures or videos, can also make them identifiable, even if such pictures or videos are not linked to any specific name, pseudonym or account belonging to the victims. This was confirmed, for example, in the AEDP ‘Twitter case’,¹⁴⁰³ where a video showing a woman and her child being physically abused was shared on the internet without their knowledge or consent. The video in itself was considered as personal data, because the woman and her child were identifiable.

¹⁴⁰¹ Recital 26 GDPR.

¹⁴⁰² Easpaing, B. N. (2018). An exploratory study of sexism in online gaming communities: Mapping contested digital terrain. *Community Psychology in Global Perspective*, 4(2):119-135; Cote, A. (2020). *Gaming Sexism: Gender and Identity in the Era of Casual Video Games*. NY University Press; Phillips, A. (2020). *Gamer Trouble : Feminist Confrontations in Digital Culture*. Feuilleter. Gray, K. L., Buyukozturk, B. & Hill, Z. G. (2017). Blurring the boundaries: Using Gamergate to examine “real” and symbolic violence against women in contemporary gaming culture. *Sociology Compass*, 11(3). In 2020, the marketing research company Bryter, in collaboration with the NGO ‘Women in Game’, released a report that suggests around 40% of female gamers have experienced some form of abuse from male gamers while playing online and 28% have experienced sexual harassment from male or other gamers in the form of objectifying comments or death and rape threats. Bryter (2020, November 12). Female Gamer Survey 2020. <https://www.womeningames.org/wp-content/uploads/2021/03/Bryter-Female-Gamers-Survey-2020-12.11.20-SHORT-no-quotes.pdf>. Oppenheim, M. (2021, June 6). The dark threats and sexual abuse women gamers endure. *The Independent*. <https://www.independent.co.uk/news/uk/home-news/women-gamers-sexual-abuse-harassment-b1860003.html>.

¹⁴⁰³ AEDP, Expediente N° PS/00205/2021, 26 June 2021, available at <https://www.aepd.es/es/documento/ps-00205-2021.pdf>.

At the end of the day, given the very nature and purpose of online harassment, it can thus be concluded that the information processed will almost always relate to an identified or identifiable victim. This is true for all forms of harassment listed in section 4.1.1, above. Indeed, as summarised in the below table, the GDPR would thus in principle always apply when a person harasses one or multiple identified or identifiable victims, regardless of whether such harassment consists in releasing (sensitive) data about them online in order to compromise their reputation or credibility ('doxing'), insulting or denigrating their victims on the basis of attributes such as gender or physical appearance ('targeted hate speech'), mocking or upsetting their victims by leaving intentionally provocative or offensive messages ('targeted trolling'), creating a fake profile and posting compromising messages in the name of the victim to cause the latter harm ('impersonation') or by sharing sexually-explicit images or videos of a victim without consent in order to shame or humiliate him, her or them (so-called 'revenge porn').

TABLE 10

The below table is meant to show that most types of online harassment necessarily implies (i) the processing through automated means (ii) of information relating to an individual, (iii) who is identified or identifiable (when indeed the attacks are targeted against one or multiple individuals rather than a generic group).

	Processing through automated means	...of information relating to a person	...who is either identified or identifiable
Doxing	✓	✓	✓
Trolling	✓	✓	if targeting (a) specific individual(s)
Online hate speech	✓	✓	if targeting (a) specific individual(s)
Online harassment campaign	✓	✓	✓
Message bombing	✓	✓	if targeting (a) specific individual(s)
Online impersonation	✓	✓	✓
Sextortion	✓	✓	✓
Non-consensual dissemination of sexually explicit image	✓	✓	✓

As discussed above however,¹⁴⁰⁴ there also exist general exemptions to the material scope of the GDPR. In particular, the household exemption needs to be considered in the context of online harassment, as it may sometimes exempt the harasser from liability under the GDPR, as further discussed below.

¹⁴⁰⁴ See section 3.1.1.3, above.

(ii) As an exception, harassers will not be subject to the GDPR when the processing is not directed outwards from their private sphere

As a reminder, the GDPR does not apply to the processing of personal data by a natural person “*in the course of a purely personal or household activity*”.¹⁴⁰⁵ Personal or household activities include correspondence and the holding of addresses, but also social networking and online activity undertaken for personal purposes only. Hence, online harassers could be tempted to claim that they are not subject of the GDPR because their processing activities would be purely personal and would thus fall within this household exemption. Before analysing in which circumstances the household exemption could indeed apply, two different types of controllers must be distinguished:

- 1) Controllers who are natural persons:** in this case, the processing practice which consists in harassing a person through the use of ICT could fall outside of the material scope of the GDPR, if the harasser is indeed acting in the course of a “*purely personal or household activity*” (which, as argued below, would only happen in limited instances);
- 2) Controllers who are legal persons:** in that case, the household exemption cannot apply, for the simple reason that a legal person cannot be conducting processing activities for purely personal or domestic purposes. Indeed, processing of personal data by legal persons is necessarily conducted in the course of a commercial or not-for-profit activity. Within that category, two sub-scenarios can further be distinguished:
 - a. The legal person is the harasser:** it may happen that a legal person undertakes a harassment campaign against an individual, such as in the Spanish case PS/00227/2020, where the AEDP imposed a fine of €12.000 on a company, for spreading harmful allegations through Facebook and WhatsApp against a homeless person who, according to the company, had stolen money from its office cash register. In such a case, there is no doubt that the GDPR applies to such processing activities, given that the company cannot pretend having acted in the course of purely personal or domestic activities;
 - b. The legal person is an intermediary:** harassers usually rely on tools or services developed by legal entities (e.g., a social media company or an app service provider) to harass their victim. These companies will thus also indirectly and/or passively process the personal data of the victim, for example by publishing them or storing them. Indeed, the

¹⁴⁰⁵ Article 2(2)(c) GDPR.

GDPR makes clear that its rules apply “to controllers or processors which provide the means for processing personal data for such personal or household activities.” Hence, even when the household exemption applies with respect to the processing carried out by the harasser himself or herself, the GDPR can remain functional to combat this practice by targeting the intermediary, as further discussed below. If a man, for example, posts denigrating comments about one of his colleagues on a private Facebook page, this man may (to some extent) benefit from the household exemption, but the company Meta itself will have to comply with the GDPR given that the storage and publication of the victim’s personal data on the Facebook page is taking place in the course of Meta’s commercial activities.

Now that this distinction has been made, it remains important to establish when a natural person may benefit or not from the household exemption in the context of online harassment. For that purpose, the delineation of the household exemption itself needs to be clearly understood. As already discussed above,¹⁴⁰⁶ the household exemption has so far been interpreted restrictively by the CJEU in the *Lindqvist*, *Rynes* and *Jehovan todistajat* cases. As a result, harassers will only be exempted from their obligations under the GDPR in a limited number of cases.

In *Lindqvist*, in particular, it was already established that an individual could not benefit from the household exemption in the context of online blogging when the personal data were made accessible to “an indefinite number of people”. Hence, any online harassing practice taking place on a publicly accessible web page supposes that the harassers in question may be held liable under the GDPR. In practice, many forms of online harassment take place on publicly accessible digital spaces since the purpose is often to harm the victim by using the general public as a passive audience. As an illustration, when harassers post denigrating comments or aggressive threats on a public Twitter account, or when a revengeful individual publishes a sexually explicit video of an ex-partner on a publicly accessible pornographic website, such content can be seen by an indefinite number of people around the world, with the consequence that such processing does no longer take place in the course of a ‘purely personal or household activity’. On this basis, it can be concluded that online harassing practices taking place on a publicly accessible website necessarily fall within the material scope of the GDPR.

In *Rynes* and *Jehovan todistajat*, the CJEU adopted an even more restrictive approach of the household exemption by stating that a processing activity could not be considered as ‘purely personal’ where that activity would “extend, even partially, to a public space” and is accordingly “directed outwards from the private

¹⁴⁰⁶ See section 3.1.1.3, above.

setting of the person processing the data".¹⁴⁰⁷ In the *Jehovah todistajat* case, for example, it was determined that the Jehovah witnesses could not benefit from the household exemption because their door-to-door preaching activity was meant to spread their faith by finding new members beyond their existing community. By analogy, it could be argued that any harasser who is extending the processing practice, even partially, to a public space, or who is sharing a victim's personal data beyond his private circle, may no longer validly invoke the household exemption. Because of the absence of clear criteria to determine what constitutes the 'private sphere' of an individual however, it may sometimes be challenging to determine whether a processing practice is directed inward or outward from such a private sphere. In practice, a careful case-by-case assessment of all relevant factual elements would be required. For example, if a harasser personally knows the victim and is sending insults directly and exclusively to the victim, either via a messaging app or via normal text messages, the household exemption would normally apply, since such processing is *prima facie* not directed 'outward' from the private setting of the harasser. In that case, the victim would therefore be more advised to rely on provisions of criminal law prohibiting more traditional forms of harassment than on the GDPR.¹⁴⁰⁸ By contrast, if a person shares a victim's personal data with individuals with whom that person did not have any pre-existing relations, such processing could fall within the scope of the GDPR, because directed outward from the harasser's private sphere. Similarly, if an individual adopts a harassing behaviour towards third parties in a public space, such processing can be considered as directed outward from that individual's private sphere and could thus fall within the scope of the GDPR. This reading of Article 2(2)(c) GDPR seems to be supported by the AEDP, which sanctioned a man for taking pictures of young women at the beach without their knowledge or consent.¹⁴⁰⁹ Even if the harasser in question only processed the personal data on his own personal device and did not share the images with third-parties, the fact that he took pictures of women that he did not know personally in a public space was considered as automated processing of personal data extending to a public space. As a result, the harasser was ordered to delete the pictures and was imposed a fine of 4.000 EUR by the AEDP for breach of Article 6(1) GDPR (i.e., absence of any valid legal basis for the processing of personal data).¹⁴¹⁰

In the opinion of the author of this study, the fact that the GDPR would only apply to forms of online harassment that extend beyond the private sphere of the harasser is in line with the general objective of the GDPR to guarantee a high level of protection of natural persons with regard to the processing of personal data without, however,

¹⁴⁰⁷ CJEU, *Ryneš*, paras. 31 and 33; *Jehovah Todisjavat*, para. 42.

¹⁴⁰⁸ In Belgium, for example, Article 442bis of the Penal Code provides for a prison sentence and/or a fine for anyone who harasses a person when he knew or should have known that he was seriously affecting the tranquility of the person concerned by this behavior.

¹⁴⁰⁹ AEDP, Expediente n° PS/00335/2019, available at <https://www.aepd.es/es/documento/ps-00335-2019.pdf>.

¹⁴¹⁰ *Ibid.*

interfering with the right to privacy or the freedom of expression of natural persons who are processing personal data in the context of purely personal activities.

In this respect, it must be pointed out that harassment behaviours that do not go beyond the private sphere of the harassers will normally have a more limited scope, and thus a different impact on the victim. This type of harassment, hereafter referred to as ‘inter-personal harassment’, may however still be sanctioned through other means, such as provisions of criminal law. In the opinion of the author, the distinction between public online harassment and inter-personal online harassment, as well as the different legal regime applicable to such behaviours, can be regarded as appropriate and legitimate given that their effects also differ in practice. As far as inter-personal harassment is concerned, the absence of publicity will normally protect the victim from the negative effects that one may experience when personal data are shared with a large or indefinite number of persons, such as an increased feeling of shame, or the loss of control over one’s personal data. Furthermore, if the harassment is exclusively taking place through private messaging apps or accounts, the victim has an increased chance to be able to put an end to the harassment through technical means. Today indeed, most personal devices or apps allow users to block one or more individuals from sending direct messages. Hence, victims of inter-personal harassment normally have the ability to block their harassers, even if it may require the victim to repeat this operation several times on different devices or social media accounts.¹⁴¹¹

There may be, of course, some grey areas, where it could appear that the processing of personal data is confined within the private setting of the harasser, even if the scope of such processing is intended to expand beyond that private sphere. Such could be the case, for example, when a hacker collects sensitive information about a person and blackmails the latter, by threatening to release such information among the private circle of the victim, or on the internet.¹⁴¹² If the information is never disclosed, but only used as a mean to blackmail the victim, the harassers could be tempted to invoke the household exemption. Yet, in the opinion of the author, the notion of ‘*purely personal or domestic activities*’ should only encompass lawful activities where the personal data in question are not intended to be disclosed beyond the private setting of the individual concerned. Sextortion or threat of doxing implies, by definition, either the threat or the act of disclosing sensitive information to an indefinite amount of person, or to a definite number of persons within the private sphere of the victim. In both cases, the processing of personal data is thus directed, or at least intended to be directed, outwards from the private setting of the harasser. As a result, the author of this study is of the opinion that online blackmailers cannot validly rely on the household exemption to escape

¹⁴¹¹ On the differences between online and more ‘traditional’ forms of harassment, see section 4.1.1.1, above.

¹⁴¹² When the sensitive information consists in sexually explicit images (whether real or fake), the practice is usually referred to as ‘sexortion’. When the sensitive information consists in other type of data, the practice may be referred to as ‘threat of doxing’.

liability under the GDPR. The same reasoning may further be applied to the practice of ‘message bombing’ or ‘online harassment campaign’, where multiple individuals each target the same victim. In the opinion of the author of this study, it could be argued that the *ex-ante* sharing of personal data for the purpose of collectively harassing a target (albeit such harassment may take place exclusively through private means, such as a direct email or message) cannot be considered as directed ‘inwards’ from the private sphere of the individual, since the purpose is to participate to a public and/or large digital movement to harm an external target. In that respect, the absence of any pre-existing relation between the multiple harassers and the victim designated as a target can also be considered as an element which confirms that the processing of personal data is taking place in the context of activities which extend beyond the private sphere of the harassers.

Based on the above considerations, the author of this study believes that the following three elements in particular should be considered (where relevant) for determining whether the household exemption could apply to a case of online harassment:

- 1) Is the processing of personal data extending (at least partially) to the public sphere?
- 2) Does the harasser personally know the victim, or is the victim someone outside from his/her own private sphere?
- 3) Did the harasser provide the personal data to other persons with the intention or consequence that the data were further processed and spread by these other persons beyond his/her private sphere?

By taking these elements into account, processing activities falling within the material scope of the GDPR can be better distinguished from other type of processing practices taking place in the context of purely inter-personal relations. This reading of Article 2(2)(c) of the GDPR seem consistent with the approach adopted by most DPAs with respect to cases of online harassment, as further exemplified below through the analysis of several decisions rendered the Spanish and Italian DPAs.

(iii) As a general rule, the GDPR could apply whenever (one of) the controller(s) is located in the EU, or processes personal data of data subjects located in the EU for offering them goods and services

Finally, it can also be observed that the broad territorial scope of the GDPR can turn into an advantage for victims of online harassment, given that such a scope goes

beyond the borders of the EU, and is thus more fitted to the digital environment where online harassment is taking place. Three case-scenarios can be distinguished in particular.

In the first case-scenario, the harasser is located in the EU. In that case, the GDPR will apply, regardless of whether the victim of the harassment is located in the EU or not, in accordance with Article 3(1) GDPR. Hence, if a female US journalist, for example, is being 'doxed', impersonated or otherwise harassed through DDTs by a group of individuals located in the EU, she may file a complaint with a DPA to report such behaviours. Such a complaint could target not only the harasser(s), but also any intermediary or its representative located in the EU, such as Meta, Twitter or YouTube, in the event her personal data are being processed on one of the websites owned by these big tech companies.

In the second case-scenario, the harassers are either located outside of the EU, or it is not possible to know their location because of the use of anonymity.¹⁴¹³ In that event, the GDPR may still apply vis-a-vis any EU-based intermediary enabling the processing of personal data in the context of such online harassment, thereby still offering tools to the data subjects and the competent authority to prevent the harmful processing of personal data. In the AEDP case PS/00200/2021, for example, a Spanish woman filed a complaint in her capacity as a data subject against a German company owning a dating website, after somebody had added her telephone number on a dating profile containing sexually suggestive pictures.¹⁴¹⁴ The identity of the harasser was unknown; the victim only became aware of the issue after repetitively receiving unsolicited calls from men who were interested in meeting her. As a consequence, she decided to contact the dating website directly. Despite having clearly requested the company owning the dating website to delete her personal data, the latter failed to do so within the required timeframe.¹⁴¹⁵ The case was thus brought to the attention of the AEDP through the intervention of an NGO specialised in consumer protection. After reviewing the facts of the case, the AEDP imposed a fine of 2.000 EUR on the company and formally ordered the latter to delete the data of the complainant.¹⁴¹⁶ This case illustrates the benefit of relying on the GDPR against an intermediary in the event the identity of the harasser(s) is unknown.

In the third case-scenario – the most challenging one for victims, both the harassers and the intermediary are located outside of the EU. Under traditional provisions of criminal law, the victims would often be left without access to any effective remedy,

¹⁴¹³ The issue of anonymity in the context of online harassment, and what can be done to lift such anonymity through the use of the GDPR, will further be explored below.

¹⁴¹⁴ AEDP, Decision n°PS/00200/2021, 9 July 2021, available in Spanish (original language) at <https://www.aepd.es/es/documento/ps-00200-2021.pdf>.

¹⁴¹⁵ As a reminder, Article 12(3) GDPR provides that the controller must answer a data subject's request within one month of receipt of the request.

¹⁴¹⁶ *Ibid.*

because the doctrine of state sovereignty normally limits the scope and applicability of criminal law to crimes that have been committed on the territory of a state.¹⁴¹⁷ By contrast, the GDPR may apply to controllers established abroad when they process personal data of data subjects located in the EU for offering them goods and services, or for monitoring their behaviours in the EU.¹⁴¹⁸ As a result, most tech companies offering communication services to EU users, such as social media or dating websites, will still have to comply with the GDPR, and may thus be requested to stop processing personal data used in the context of online harassment. As discussed above, enforcement may remain challenging because of external factors pertaining to the resources and practices of DPA.¹⁴¹⁹ As far as the internal factors of functionality of the GDPR are concerned however, there is no doubt that the extra-territorial reach of the GDPR can present a clear advantage for data subjects willing to ascertain their rights and freedoms against harmful online behaviours involving foreign actors.

Even if the GDPR applies to a case of harassment because of its broad material and territorial scope, it does not mean that the processing will automatically be declared unlawful. If the GDPR is compared to a toolbox, applicability means that the toolbox is unlocked. The data subject must however still find the right tool to put an end to the harassment. The below section will precisely aim at assessing the functionality of the main tools offered by the GDPR to combat cases of online harassment.

4.1.4.2. Functionality of the tools provided by the GDPR to combat online harassment

In the above section, it has been shown that most forms of online harassment fall within the scope of the GDPR. The fact that the GDPR is applicable does not mean, however, that the processing in question is necessarily unlawful, or that the victim will be able to put an end to it. Indeed, the question remains whether the tools that the GDPR offers are practical enough for data subjects, DPAs and national courts to effectively combat online harassment. The below section will focus on that second important question by looking into the existing case-law at the level of DPAs and national courts confronted to cases of online harassment.

Looking at the substance of the GDPR, the author of this study will discuss how the following tools in particular could be used to combat diverse forms of online harassment: (a) the principle of lawfulness, fairness, and transparency, invoked together with (b) the obligation for controllers to have a valid legal basis for processing the personal data; (c) the right to object to the processing of personal,

¹⁴¹⁷ van der Helm M. (2021). *op. cit.*, p. 48, referring to El Zeidy, M. (2002). The Principle of Complementarity: A New Machinery to Implement International Criminal Law. *Michigan Journal of International Law*, 23(4), p. 870.

¹⁴¹⁸ Article 3(2)(a) and (b) GDPR.

¹⁴¹⁹ See section 3.3.3, above.

and/or (d) the right to erasure, together with (e) the right of data subjects to lodge a complaint with the competent DPA, (f) the right to obtain an effective remedy when data protection law has been breached, and (g) the investigative and corrective powers of DPAs. The combined use of these tools as well as the extent of their functionality for combatting online harassment will be illustrated through the analysis of decisions rendered by DPAs and national courts in relation to online harassment.

(i) The principle of lawfulness, fairness and transparency and the obligation for the controller or processor to have a valid legal basis under Article 6 or 9 GDPR

As already discussed above,¹⁴²⁰ the principle of lawfulness, fairness and transparency consists of three different components which can be linked to further provisions of the GDPR. In particular, the principle of lawfulness entails that the processing activity may not contravene the law and must have a valid legal basis; this principle can thus be linked to the obligation of controllers to have a valid legal basis before processing the personal data, as restrictively listed in Article 6(1), 9(2) and 10 of the GDPR. The principle of fairness, for its part, entails that even if a processing activity appears lawful, controllers must process personal data in good faith and with honesty, and pay due regard to the reasonable expectations of the data subjects;¹⁴²¹ such principle can thus be linked to Article(6)(1)(f) GDPR, which provides that when controllers rely on their own legitimate interests to process personal data, they must ensure at all time that such interests are not overridden by the rights and freedoms of the data subjects. Finally, the principle of transparency requires controllers to be transparent about the nature, effects or any changes in the processing activities; this principle can thus be linked to Article 12 to 14 GDPR on the obligation of controllers to inform data subjects about the processing of their personal data in a comprehensive way, as well as the right of data subjects to access their personal data, as foreseen in Article 15 GDPR. For these reasons, should a data subject consider that EU data protection law has been breached because a harassing behavior involves the unfair or illegitimate use of his/her data, the principle of lawfulness, fairness, and transparency can be invoked together with one or more of these specific provisions.

By default, it may be tempting to consider that online harassment is a type of processing practice that can never be considered as lawful, fair or transparent, taking into account the harmful effects that it may have on the dignity, mental integrity and right to privacy of the data subjects concerned. Yet, as shown above, online harassment may take many different forms; while some of these forms will appear clearly and strictly illegal under EU and national law because they include, for example, the disclosure of confidential information or racist or xenophobic attacks,

¹⁴²⁰ See section 3.2.1.1, above.

¹⁴²¹ Hoofnagle, C., van der Sloot, B. & Zuiderveen Borgesius, F. J. (2019). *op. cit.*, p. 77.

other forms of harassment may lead to a discussion as to whether the communications, although perceived as harmful in the eye of the data subjects, are not legitimate and permissible in a democratic society, taking into account in particular the freedom of expression of the controllers. The need to balance diverging rights and interests can find its expression in Article 6(1)(f) GDPR, according to which controllers may process personal data where necessary to pursue their legitimate interests, as far as the rights and freedoms of the data subjects do not prevail over such interests. In that respect however, it must first be reminded that Article 6(1)(f) GDPR only applies to the processing of non-sensitive data. As a consequence, a clear distinction must be made between forms of harassment involving the processing of sensitive personal data, and forms of online harassment that involve the processing of other categories of personal data.

(a) The manifestly unlawful character of harassment practices involving the processing of sensitive data: a functional aspect of Article 9 GDPR

As discussed above, sensitive personal data include information relating to the racial or ethnic origin, political opinions, religion, sexual orientation or health of the data subject.¹⁴²² Under Article 9(1) GDPR, it is simply prohibited for controllers to process sensitive personal data. Hence, by default, any form of online harassment that involves the processing of sensitive personal data can be considered as unlawful. Among the existing exceptions to this general prohibition, as listed in Article 9(2) GDPR, only one appears relevant in the context of online harassment: the fact that the personal data were already manifestly made public by the data subject. This element should thus be taken into account when a form of online harassment involves the processing of sensitive data about the victim. If, for example, a fake dating profile is created on an app dedicated to non-heterosexual users, such as Grindr,¹⁴²³ while the victim in question never made their sexual orientation public, it can be considered without further analysis that such a processing violates the principle of lawfulness and the obligation of the controller to have a valid legal basis under Article 9 GDPR (regardless of whether the information is correct or not). Similarly, if a form of online harassment involves the sharing of information about the health status of a person, while such information had been kept strictly confidential by the data subject, such a processing can by default be considered as being in breach of Articles 5(1)(a) and 9 of the GDPR. In these instances, it is not required to establish a balance between the legitimate interests of the controller on the one side, and the rights and freedoms of the data subjects on the other side, since Article 6(1)(f) GDPR do not apply to sensitive personal data. In light of this, it can thus be concluded that Article 9 GDPR can be particularly ‘functional’ for combatting some forms of online harassment involving the processing of sensitive

¹⁴²² See section 3.1.1.2, above.

¹⁴²³ Grindr is the world largest social networking app for the LGBTQ+ community. Source: <https://www.grindr.com>.

data, given that it must not be proven that the disseminated information is accurate or defamatory for the processing to be considered unlawful. It may be the case, however, that a form of processing does not involve the processing of sensitive data. In that case, the lawful or unlawful character of the processing must be decided in light of Article 5 and 6 GDPR, as discussed below.

If sensitive data have already been made public by the data subject, or if *non-sensitive* data are being processed by a controller, the lawfulness of such processing must still be analyzed in light of Article 5(1)(a) GDPR and Article 6 GDPR. Within Article 6 GDPR, one legal basis appears particularly relevant in the context of online harassment: the necessity for the controllers to process personal data for the purpose of their own legitimate interests, i.e., Article 6(1)(f) GDPR. Of course, other legal bases than the legitimate interests of the controller can also justify the processing of personal data, such as the consent of the data subjects (Article 6(1)(a) GDPR), or the necessity to perform a contract (Article 6(1)(b) GDPR). In the context of online harassment however, it is difficult to imagine any situation where one of these other legal bases would apply. To illustrate this, one may refer to a recent case decided by the AEDP regarding the non-consensual publication of sexually explicit images.¹⁴²⁴

The facts of the case concerned the publication by a man (the controller) of pictures and comments relating to the BDSM relationship that the latter had with his ex-wife (the data subject) on a publicly accessible website. The controller alleged that his ex-wife had contractually consented to the publication of these pictures. Following a complaint filed by the data subject, the AEDP conducted an investigation that confirmed that the website belonged to the controller.¹⁴²⁵ The AEDP then collected the point of view of each party. The controller argued that the website was meant to be private and had been created as a remembrance of the 7-years relationship that he had with his ex-wife. The controller also argued that the name of his ex-wife was not mentioned on the website, and that the pictures were pixelated, so that the data subject was not identifiable. On this basis, the controller considered that the GDPR did not apply to this processing because of the household exemption, and because the data did not qualify as ‘personal data’. Finally, even in the event the GDPR would apply to this processing, the controller argued that the data subject and him had signed a BDSM contract in 2013 in which his ex-wife had consented to the dissemination of images, photographs, videos, or any similar content about their BDSM relationship. The controller provided a copy of this contract to the AEDP.¹⁴²⁶ The AEDP noted that the contract contained a clause in which the data subject waived her right to privacy, giving herself up as a ‘slave/submissive’, and allowing the defendant to disseminate any content about her. The AEDP however noted that the contract also contained another clause allowing either of the parties to

¹⁴²⁴ AEDP, PS/00410/2020, 17 June 2021, <https://www.aepd.es/es/documento/ps-00410-2020.pdf>.

¹⁴²⁵ *Ibid.*, p. 2.

¹⁴²⁶ *Ibid.*, p. 3-5.

terminate it at any time. After having heard the parties and analyzed the evidence of the case, the AEDP rendered its decision in June 2021.¹⁴²⁷ With respect to the household exemption, first, the AEDP found that it was not applicable in the case at hand, since the website in question was public and thus accessible to an indefinite number of persons. Referring to *Lindqvist*, *Rynes* and *Jehovan todistajat*, the AEDP thus concluded that the processing of the personal data by the controller could not be considered as falling within activities that are ‘*exclusively personal or domestic*’. The AEDP also found that not all pictures on the website had been pixelated, and that the data subject was thus clearly identifiable. As a consequence, the data in question could be considered as personal data, and the GDPR applied to their processing. After confirming that the processing activity in question was falling within the material scope of the GDPR, the AEDP analyzed whether such processing could be considered as lawful under Article 6 GDPR.¹⁴²⁸ Regarding the legal basis for the processing, the AEDP rejected the ‘consent of the data subject’ as a valid legal basis, pointing out that the privacy waiver in the BDSM contract was not valid in light of the Spanish Civil Code, the Spanish Constitution and the Charter, and in particular in light of the protection afforded to human dignity. In any case, the AEDP also noted that the data subject had terminated the contract at the time of the divorce between her and the controller. Because of the manifest breach of the principle of lawfulness, and because the controller had not argued that the processing could be based on Article 6(1)(f) GDPR, the AEDP did not consider it necessary to assess whether the dissemination of the sexually explicit pictures and comments could be justified on the basis of the legitimate interests of the controller to exercise his freedom of expression. As a result, the AEDP concluded that the processing in question was unlawful and imposed a fine of 1.500 EUR on the data subject. Because the website had already been taken down on a voluntary basis by the controller during the investigation, the AEDP did not have to deliver an injunction to delete the personal data. In the opinion of the author of this study, this decision can be criticized with respect to the underlying legal reasoning of the AEDP, since the latter failed to recognize that the pictures and comments published on the website qualified as sensitive personal data. These data indeed revealed information relating to the sexual orientation of the victim. Hence, the AEDP should have recognized the manifestly unlawful nature of the processing on the basis of Article 9(2)(a) GDPR, rather than 6(1)(a) GDPR. Yet, this case has the merit of showing that the consent of the data subject or the existence of a contract can hardly be used as legal basis in the context of online harassment. This is the reason why the below section will focus in particular on the possibility for controllers to rely on Article 6(1)(f) GDPR to justify

¹⁴²⁷An English summary of the decision is available on the GDPRhub database at [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-PS/00410/2020](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-PS/00410/2020). For the original, please refer to: AEDP, PS/00410/2020, 17 June 2021, <https://www.aepd.es/es/documento/ps-00410-2020.pdf>.

¹⁴²⁸In the opinion of the author, the AEDP committed a mistake in this respect, since the personal data included information relating to the sexual orientation of the data subjects, which is a special category of data under Article 9 GDPR. As a consequence, it would have been more appropriate to apply Article 9 GDPR to determine whether the processing was lawful or not. See, also: CJEU, *Chief Ethics Commission*, Case C-184/20, discussed above.

the processing of personal data, even when such a processing can be felt like a type of harassment in the eye of the data subject.

(b) The unlawful character of forms of harassment involving the processing of *non-sensitive* data: a flexible use of Article 6(1)(f) GDPR, reinforced by the principle of accountability

In the above-mentioned case, there was hardly any doubt about the unlawful nature of the processing because of the absence of any valid legal basis for the dissemination of sexually explicit images. Other cases may however require deeper analysis as to whether the processing of personal data could not be justified on the basis of Article 6(1)(f) GDPR. In some specific instances, indeed, the controllers could argue that they had a legitimate interest to process the personal data of the data subjects for the purpose of contributing to a public debate, raising awareness on a social issue, or more generally exercising their freedom of expression. This argumentation was for example chosen by Mrs. Lindqvist, who invoked her freedom of expression to justify the publication of her colleagues' personal data on her blog. Similarly, in the Icelandic case discussed above relating to a dispute opposing two parents with respect to the custody of their child, the father relied on his freedom of expression to justify the publication of pictures and comments about his child and ex-wife on a publicly accessible Facebook account.¹⁴²⁹ Whether such behaviors amount to a breach of the principle of lawfulness must thus be analyzed in light of Article 5 and Article 6(1)(f) GDPR.

Depending on the nature and scope of the online harassment, establishing a balance between the legitimate interests of (each of) the controller(s) on the one side, and the rights and freedoms of data subjects on the other side, is not always an easy task. In this respect, there is no doubt that the case-law of the CJEU and of the ECtHR relating to the exercise of freedom of expression provides useful guidance as to the elements which should be taken into account when attempting to establish such a balance. In the context of online harassment, the following elements in particular could be taken into account by the relevant authority: the content and scope of the communication, the context in which the processing took place, the effect it had on the data subject, the notoriety or conduct of the data subject prior to the processing of personal data, the relationship between the data subjects and the persons involved, and the reasonable expectations of the data subjects with respect to such processing.¹⁴³⁰

¹⁴²⁹ Persónuvernd, Mál nr. 2020010552, 17 November 2021, <https://www.personuvernd.is/urlausnir/kvortun-yfir-birtingu-ljosmynda-a-samfelagsmidli-visad-fra>.

¹⁴³⁰ Council of Europe (2021). Guide on Article 10 of the European Court of Human Rights – Freedom of expression, updated on 30 April 2021. https://www.echr.coe.int/documents/guide_art_10_eng.pdf.

The GDPR itself refers to the reasonable expectation of the data subject as an important element to weigh when applying Article 6(1)(f) GDPR. The 47th Recital of the GDPR states, in particular that “*the legitimate interests of a controller (...) may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller*”. Depending on whether the data subject is a public figure, this level of reasonable expectations may vary. Hence, although similar, the case of Greta Thunberg – a well-known public figure who was subject to insults and mockery on Twitter after advocating for climate protection, should be distinguished from the case of Mila – the 16-years-old French teenager who was harassed through social media after publishing an Instagram story criticizing Islam as a religion.¹⁴³¹ In the first case, the communications were sent to a public figure, that is, a person who, through her acts and position, has entered the public arena, and should therefore expect to be more scrutinized or criticized than a non-public figure.¹⁴³² By contrast, a teenager such as Mila who was not a public figure at the time she published her video on Instagram could not reasonably expect to become the target of a vast online harassment campaign, even if her prior behavior – i.e., posting a video criticizing Islam in very harsh terms – could also weigh in the overall balance to be established under Article 6(1)(f) GDPR. The notoriety of the victims, their prior behavior, or the relationship they have with the harasser(s) are only some of the elements that need to be weighed in deciding whether a processing activity can be regarded as fair and lawful. All other relevant circumstances, and in particular the content of the communications themselves, must also be considered to determine whether the legitimate interest of the controller(s) to exercise their freedom of expression could prevail over the rights of the data subjects, including human dignity, integrity or privacy.

To illustrate this, one may refer to two recent decisions rendered by the Italian DPA and the AEDP respectively, concerning the publication of personal data on the internet by a political figure. The first case relates to a form of cyberbullying exercised by the Mayor of an Italian city against several individuals.¹⁴³³ Mr. Cateno De Luca, Mayor of the city of Messina, was regularly posting pictures, videos and comments on his Facebook page showing and describing individuals in a denigrating or defaming manner or accusing them of minor offences such as littering. Most of these individuals were persons in conditions of social and economic difficulty,

¹⁴³¹ See, among others: Safe, A. (2021, June 4). Mila trial: 13 in the dock over threats to French teenager who insulted Islam. *The Times UK*. <https://www.thetimes.co.uk/article/mila-trial-13-in-the-dock-over-threats-to-french-teenager-who-insulted-islam-j9pm3rcw8> ; Garaicoechea, M. (2021, June 2). Mila vit, à plus grande échelle, ce que vivent toutes les victimes de cyberharcèlement. *Libération*. https://www.liberation.fr/societe/police-justice/mila-vit-a-plus-grande-echelle-ce-que-vivent-toutes-les-victimes-de-cyberharcèlement-20210602_FUGOK3SNIRCIPNZU74LRNKRGE/.

¹⁴³² ECtHR, Judgment of 19 April 2019, *Kapsis and Danikas v. Greece*, para. 35. According to the Merriam Webster, a public figure can more generally be defined as an individual that has acquired fame or notoriety or has participated in a particular public controversy.

¹⁴³³ Garante per la protezione dei dati personali, decision n°9670001, 13 May 2021, available at <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670001>.

including homeless people. The mayor also published a comment criticizing in an offensive manner some employees of the Municipality. Several associations for the protection of citizens and consumers reported this practice to the Italian DPA (hereafter, the '*Garante*'), considering that such processing practice was unfair and harmful to the dignity of the individuals concerned. The *Garante* conducted an investigation on the matter and collected the point of view of the Mayor. The latter explained that he had posted this content in order to raise public awareness on issues relating to delinquency and other matters of public interest in the city of Messina. In the course of the investigation, the *Garante* decided to already issue a warning against the Mayor pursuant to Article 58(2)(a) GDPR, informing him that these processing practices were likely to be in breach of the GDPR. Despite this warning, the Mayor refused to take down the publications from his Facebook page, except for one video showing minors littering on the street. After closing its investigation, the *Garante* rendered a final decision against the Mayor, finding that the latter had breached the GDPR as well as several provisions of national law. In its decision, the *Garante* first noted that the Mayor could not invoke Article 6(1)(e) GDPR as a valid legal basis for processing these data, since the Mayor was not acting in his official capacity when posting content of this nature on his Facebook account, as evidenced by the fact that the Municipality of Messina had never officially endorsed this Facebook page, and that the Mayor was mainly using it to express his personal opinions or to share information about his private and family life. With respect to the legitimate interest of the Mayor to inform the population about urban issues, the *Garante* found that the content published did not constitute essential information, in the sense that raising awareness on issues of public interest did not require the posting of material where individuals were identifiable. The *Garante* therefore considered that the processing of personal data was unlawful, given that respect for human dignity and the right to privacy of the individuals concerned were prevailing over the freedom of expression and information of the Mayor. The *Garante* furthermore specified that the breaches of the GDPR were aggravated by the public role played by the Mayor who, by virtue of his position, could spread information more easily and widely, and had made an improper use of this power for the purpose of political propaganda. At the end of the day, taking all relevant circumstances of the case into account, the *Garante* decided to issue an injunction against the Mayor and to impose a fine of 50.000 EUR on him, pursuant to Article 83 GDPR.

The second decision illustrating how the principle of fairness and lawfulness can be used for protecting victims of online harassment relates to a case of 'doxing', i.e., the act of publicly revealing previously private personal information about an individual on the Internet, often with the intention to harm the latter. The factual background of the case concerned a judicial dispute between the Mayor of a Spanish city (the controller) and an employee of the municipality (the data subject). The employee had previously sued the Mayor before the Spanish labor court, claiming to have been harassed and persecuted at work by the latter. A judgment dismissing the claim of

the employee for lack of evidence was rendered on 9 December 2018 by the competent court. The day after, the Mayor published an unredacted copy of this judgment on his Facebook account, accompanied by a comment in which he blamed the employee for having spread false allegations and announced that he would present himself again for the next elections. The Facebook account in question was public, in the sense that any Facebook users or non-users could have access to it and read the full judgment, including personal information relating to the identity, position and past working conditions of the employee. In response, the employee filed a complaint with the AEDP against the Mayor for unlawful processing of personal data. Before the AEDP, the Mayor argued that the processing was valid under Article 6(1)(f) GDPR, mainly because the publication of the judgment was necessary to restore his professional reputation. After considering all the relevant circumstances of the case, and in particular the fact that the judgment contained many personal information about the employee, the AEDP found however that publishing the full judgment, including the name of the former employee and other personal information, was not necessary for restoring the Mayor's reputation. Rather, a redacted version of the judgment, where no personal data relating to the employee would appear, would have been sufficient. To reach this decision, the AEDP took into consideration the content of the communication, the way it was disseminated, the effect that it could have on the data subject, and the relationship between the data subject and the controller, among others.

In the opinion of the author of this study, these two decisions rendered by the Italian and Spanish DPA respectively show how Article 6(1)(f) GDPR can be used as a functional tool for the protection of the rights and freedoms of data subjects in the context of online harassment, in the sense that it offers the necessary flexibility for DPAs or national courts to weigh different interests and rights in order to distinguish between lawful and unlawful communications, and put an end to processing behaviors that would disproportionately interfere with the data subjects' right to data protection, privacy, mental integrity and human dignity.

In applying Articles 5 and/or 6(1)(f) of the GDPR, another tool which may further enhance the functionality of the GDPR is the principle of accountability. According to this principle indeed, the controller is responsible for, and should be able to demonstrate compliance with the other key-principles of the GDPR. Should a debate arise as to the lawfulness or fairness of the content sent or published by a controller, it would thus be for the latter to prove that they had a legitimate purpose for processing the data of the target, and that, for example, the target could reasonably expect such a processing. This therefore takes the burden of proof away from the victim and puts it on the shoulder of the harasser. By contrast, under provisions of criminal law, it is for the victim or the prosecutor in charge of the case to prove that the harasser committed an offence. Furthermore, this will usually require proving that the harasser had the intention to cause harm to the victim. In comparison, Article 6(1) GDPR can be considered as breached even if the harasser had no

intention to cause harm. For these reasons, invoking the GDPR to combat online harassment can sometimes appear more convenient than traditional provisions of criminal law. Once the unlawfulness of the data processing has been established, the next step is to put an end to the processing at stake and/or to erase the harmful content. This is where other important tools offered by the GDPR may come into play: mainly, the right to erasure and the joint liability of other controllers, together with the right to lodge a complaint with a DPA, and the corrective powers of DPAs.

(ii) The right to erasure, the powers of DPAs and the respective responsibility of harassers and intermediaries as additional tools to combat (anonymous forms of) online harassment

When personal data are being processed to harass a natural person, the desire of the victim is often three-fold: first, to put an end to the online harassment practice; second, to obtain the erasure of the harmful content, and; third, to hold the responsible parties liable. Obvious tools that the data subject may rely on for achieving these purposes are Article 17 GDPR (i.e., the right to erasure), Article 24 (i.e., responsibility of the controllers), as well as Article 77 of the GDPR (i.e., right to lodge a complaint). In parallel, DPAs may use their corrective powers under the GDPR, as well as their sanctioning powers, in order to identify the responsible parties and put an end to their processing behaviors, in application of Article 58 and 83 GDPR.

As far as the right to erasure is concerned, the latter can be activated by the data subject when the processing of personal data is unlawful, in accordance with Article 17(1)(d) GDPR. Hence, when a data subject is being the victim of doxing, revenge porn, impersonation, or another harassment practice, the latter may directly address an erasure request to the controller(s) concerned. Should the harasser or intermediary fail to take the appropriate steps after having received an erasure request from the data subject, the latter may file a complaint with the competent DPA. As explained above indeed,¹⁴³⁴ DPAs have the power to order the erasure of the litigious personal data on the basis of 58(2)(g) GDPR. If the identity of the harasser(s) is unknown, the data subject may still obtain the erasure of the litigious personal data from the intermediary enabling the processing. For example, in the AEDP case n°PS/00200/2021 already mentioned above, the data subject was unaware of the identity of the person who had added her phone number to a fake dating profile, resulting in her receiving unsolicited phone calls from strangers. A functional aspect of the GDPR in this respect is that the intermediary allowing for the publication of the phone number also qualified as a controller; hence, the data subject had the possibility to file her complaint directly against this controller, on the basis of Article 17 and 24 GDPR, and to have her data removed.

¹⁴³⁴ See section 3.3.1, above.

By filing a complaint against an intermediary, the data subject may further attract the attention of a DPA on a systemic issue imputable to the intermediary, which may be addressed more generally by the DPA through the use of its corrective powers. In the decision at stake, for example, the AEDP found out that the intermediary owing the dating website had failed to put in place an adequate identification system aimed at ensuring that only legitimate contact details were being added into newly created or existing dating profiles.¹⁴³⁵ Despite this, the AEDP did not deliver a formal injunction against the intermediary to improve its security measures. In the opinion of the author of this study, such an injunction could have been delivered on the basis of Article 32 GDPR (on the security of processing) and of Article 58(2)(d) GDPR, which provides that each DPA has the corrective power *“to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period”*. Theoretically, it would have thus been possible (and, in the opinion of the author of this study, desirable) for the AEDP to deliver an injunction against the company owing the dating website to implement new security measures allowing for the verification of telephone numbers before such information would be published on a dating profile. In other words, the right of the data subjects to file a complaint and request the erasure of the personal data, combined with the corrective powers of the DPA, may not only lead to the erasure of the data, but also prevent further unlawful processing of personal data in a manner which can be harmful to the complainant as well as other data subjects. Another interesting fact to note in this respect is that, in all online harassment cases discussed in the previous section, the DPA did not have to deliver an injunction against the controller(s) concerned to put an end to the litigious processing and/or delete the personal data; the simple fact that a complaint was filed with the DPA prompted the controllers to erase the data before a final decision was even reached. Hence, the possibility for victims of harassment to file a complaint with a DPA can in itself be considered as a functional tool to combat online harassment, and eventually deter the harasser(s) from attacking the victims again, or the intermediary from allowing the posting of harmful content on its website or platform. Should the harasser(s) or the intermediary not take any action after a complaint has been filed, the DPAs remain in all case competent for delivering an injunction against the controller(s) to erase the personal data in question, given the unlawful nature of the processing.

As far as the responsibility of the controller is concerned, a distinction must be made between the responsibility of the harassers themselves and the responsibility of the intermediary. Under EU law, internet service providers cannot be put under the obligation to generally monitor all content before they are being transmitted, shared or published. This prohibition of general monitoring is one the core principle of both the e-Commerce Directive and of the Digital Service Act, which has been upheld by

¹⁴³⁵ AEDP, Decision n°PS/00200/2021, 9 July 2021, available in Spanish (original language) at <https://www.aepd.es/es/documento/ps-00200-2021.pdf>.

the CJEU in order to ensure the respect of freedom of expression, among others.¹⁴³⁶ Hence, intermediaries cannot be held liable for having failed to prevent the posting or dissemination of unlawful content. Rather, intermediaries can become liable for having failed to take down illegal content after having been ordered to do so by a relevant national judicial or administrative authority (including a DPA, as the case may be).¹⁴³⁷ As a result, a victim of online harassment seeking to have some harmful content deleted will only be able to hold the intermediary liable in the event the latter has failed to respect an injunction from a DPA, a court, or another competent national authority. By contrast, the harassers themselves can be held liable from the outset for the unlawful collection, use, sharing, publication or other processing operations that they have conducted on the personal data of the victim. This would suppose, however, that the identity of the harasser(s) is known.

Anonymity on the internet is without any doubt a recurrent obstacle for holding harassers liable under the GDPR. In some instances, however, DPAs may use their investigative powers to lift such anonymity by requiring the intermediary to provide additional information. In an impersonation case handled by the AEDP, for example, the latter was successful in identifying the harasser by requiring additional information from the intermediary about the person who had published the personal data of the victim.¹⁴³⁸ In this case, an anonymous individual had created and posted the profile of a woman on an adult website without her consent. The victim realized that her photograph, name and telephone number had been uploaded on that adult website after having received numerous phone calls from individuals wanting to have sex with her. Being unaware of the identity of the harasser, the victim had requested the website owner to erase her personal data; the company reacted immediately to this request by taking down the profile. She then filed a complaint against the unknown harasser with the AEDP so that the latter could be identified and held liable. The AEDP used its investigative powers pursuant to Article 57(1) GDPR, and requested, *inter alia*, the website owner and the telecommunication company 'Vodafone' to provide information about the IP address of the user which had uploaded the fake profile, as well as the postal address of the person paying the bills for the internet connection. It was found that this IP address belonged to a company (hereafter, Company A). After the AEDP contacted Company A, the latter explained that it was no longer registered at the indicated address and redirected the AEDP towards the individual who had taken over the IP address. The AEDP contacted the individual in question, who was found to be a co-worker of the victim. The latter submitted a written brief to the AEDP, in which he admitted that he had indeed published the fake profile, apologized for his behavior and explained that he had acted in this way after having suffered from a psychotic breakdown. Taking all relevant circumstances into account, the AEDP ultimately decided that the co-worker, in his capacity as controller, had breached Article 6(1) GDPR and imposed

¹⁴³⁶ CJEU, Judgment of 3 October 2019, *Glawischnig-Piesczek*, Case C-18/18.

¹⁴³⁷ Article 8 of the Digital Services Act

¹⁴³⁸ AEDP, decision n° PS/00292/2019, November 2019.

a fine of 1.000 EUR on him. This case shows that the investigative powers of DPAs may, in some instances, enable the identification of the harassers to hold the latter liable for a violation of the GDPR. On this basis, the victim may also engage the personal responsibility of the harasser before the competent court in order to receive compensation for any damage done, in accordance with Article 64 and Article 65 GDPR.

One may of course wonder if the GDPR itself could not be invoked by an intermediary or a third party to refuse to disclose information about an individual who is suspected to have unlawfully processed personal data, including in the context of an online harassment cases. In this respect, the CJEU has however already clarified that EU data protection law does not preclude the disclosure of personal data by a controller (such an intermediary) to a third party (such as a data subject or a DPA) in order to enable the latter to bring an action for damages before a civil court for harm caused by the person concerned, on the basis of EU or national law.¹⁴³⁹ Hence, even when harassers are natural persons who also benefit from protection afforded by the GDPR, the disclosure of their data by intermediaries is allowed as long as a valid legal basis exists under EU or national law. By looking at Article 6 of the GDPR, such legal basis can be found in Article 6(1)(c) (where EU or national law compels the intermediary to disclose the data), 6(1)(d) (where it appears that the life of the data subject may be threatened), Article 6(1)(e) (where the disclosure is necessary for a task carried in a public interest, such as when a DPA seeks to enforce the GDPR), or Article 6(1)(f) GDPR (where the intermediary disclosing the data finds it necessary for the purpose of its own legitimate interests, such as guaranteeing the compliance and safety of its services). Therefore, even if anonymity may sometimes be regarded as a barrier to enforcement, the GDPR, alone or in combination with national law or the Digital Services Act, may still offer different paths to lift such anonymity, with a view of holding the harassers liable, besides requiring intermediaries to take down the harmful communication or content, and implement appropriate measures to ensure data protection by design and by default.

(iii) Joint liability of controllers and intermediaries' liability in the context of online harassment campaigns involving a multitude of harassers

As exemplified above, the GDPR has already been used several times, seemingly quite successfully, for combatting specific forms of online harassment involving the processing by one harasser of the personal data of a data subject. This may be referred to as 'one-to-one online harassment', and can take the form of individual doxing, impersonation or the non-consensual dissemination of sexually explicit images. If the identity of the harasser is known (e.g., an ex-husband, a co-worker, a

¹⁴³⁹ CJEU, Judgment of 4 May 2017, *Rīgas satiksme*, Case C-13/16.

political figure, etc.), the victim may hold the latter liable by directly filing a complaint against that person. The DPA may then issue an injunction against the harasser if the latter has not already taken down the litigious content, and/or impose an administrative fine on the harasser to deter the latter from adopting the same behaviour again. Even when the identity of the harasser is unknown, it has been shown that the victim may, as an alternative, rely on the GDPR to force the intermediary to take down the harmful content and hold the latter liable for failure to comply with its security or other obligations, as the case may be; this has been a successful approach in several cases of ‘revenge porn’¹⁴⁴⁰ or impersonation.¹⁴⁴¹ A third option is that the data subject may file a complaint against the intermediary and the unidentified harasser for breach of the GDPR. The DPA has then the possibility to use its investigative and corrective powers to identify the harasser, for example, through the IP address used by the latter, and hold either the harasser, the intermediary, or both parties liable under the GDPR in the event of a breach.

As a general rule, the more limited the personal scope of the harassment is, the easier it is for the DPAs to investigate the matter, hear the different parties and put an end to the unlawful processing behaviour. Other forms of harassment, however, involve a multitude of harassers and/or internet users who may, by sharing or forwarding harmful content, participate to its publicity. Such is the case, for example, in the context of online harassment campaign or message bombing. In the ‘Mila affair’, for example, tens of thousands of individuals directly or indirectly contributed to the harassment of the young woman on social media and instant messaging apps, with communications ranging from simple insults to death threats. In these instances, the GDPR may appear less functional when it comes to hold each harasser responsible. Identifying all the involved parties (sometimes, hundreds of internet users), lifting anonymity where required, and determining, in each case, whether the processing amounts to a breach of the GDPR depending on the context and content of the communication, may indeed render such task very difficult. Yet, it must be acknowledged that the same conclusion can be reached for any legislation whose purpose is to hold a multitude of harassers accountable. Criminal law or anti hate-speech law, for example, do not offer any specific solution to the issue posed by the difficulty to hold a multitude of (anonymous) harassers accountable for their actions. This has been demonstrated in practice by the case of Julie Hainaut in Belgium or the Mila affair in France, among others. In the opinion of the author of this study, a creative use of the GDPR may however still help victims of wide online harassment campaigns where multiple individuals harass together the same data subject(s). The first seemingly functional provision of the GDPR in this respect would be Article 26 GDPR, on the **joint liability of co-controllers**. According to that Article indeed, when two or more controllers jointly determine the purposes and means of processing, they must be considered as joint controllers, and the data subject may

¹⁴⁴⁰ AEPD, Decision n° PS/00198/2020 of 1 September 2019; AEDP, Decision n°PS/00292/2019 of November 2019.

¹⁴⁴¹ AEDP, Decision n°PS/00278/2020 of 13 November 2020; AEDP, Decision n°PS/00200/2021 of 9 July 2021.

exercise their rights under the GDPR in respect of and against each of the controllers.¹⁴⁴² Hence, if it clearly appears from the facts of a case that several individuals have conferred or collaborated to harass a third-party in a certain way, thereby determining together the “*purpose and means of the processing*”, the data subject could strategically direct a complaint against the one of them (choosing, for example, one who is already or can be identified), with a view of holding that person jointly liable for the actions of all other co-harassers. This, in turn, may deter individuals from participating in such harassment in the first place, as each of them could be held liable for the entire scope of the unlawful processing.

In parallel, and as already discussed above, the data subjects could direct their complaint against the intermediary or intermediaries on the basis of Article 24 GDPR on **controllers’ responsibility**, if the latter has or have failed to take down illegal content after having received an order to do so, or to respect other obligations under the GDPR, such as (i) the obligation to have a valid legal basis for the processing, (ii) the obligation to implement privacy by design or by default on their website or platform, or (iii) their obligation to ensure the security of personal data (in the event, for example, the data would have been stolen from an intermediary because of its lack of security measures).¹⁴⁴³ As far as the lawfulness of the processing is concerned in particular, it has already been pointed out that intermediaries cannot be subject to a general obligation to monitor the lawfulness of the transmission, sharing, publication or other processing of personal data by internet users in a preventive manner, as this would be an almost impossible resource-consuming task that could also lead to serious interferences with freedom of expression and information on the internet. In other words, intermediaries cannot be put under the obligation to prevent all forms of harassment on their platform, website, app, or other medium of information transmission. This derives from Article 7 of the Data Services Act, read in combination with Article 2(4) GDPR. Yet, when a data subject has flagged a content as unlawful or has requested the intermediary to take it down on the basis of Article 17 or 21 GDPR, the intermediary has the obligation to answer such requests, and thus to verify itself the lawfulness of the processing, with a view of reaching a final decision on the matter. The absence of any reaction on the part of the intermediary would otherwise amount to a breach of Article 12(3) GDPR, according to which controllers must respond “*without undue delay*” to the data subject’s request. As discussed above, processing of personal data for the purpose of harassing a data subject violates the principle of lawfulness, fairness and transparency, as well as Article 6 or 9 GDPR because of the absence of valid legal basis. When the processing is manifestly unlawful and the intermediary has been notified thereof, the latter should thus take down the litigious content, and take appropriate security measures to further prevent the unlawful processing of personal data, for example by addressing a warning to the harassers or blocking their access or account (if such a measure is contractually or legally allowed). If the

¹⁴⁴² See, in particular, Article 26(3) GDPR.

¹⁴⁴³ Articles 6 and 9, as well Article 25, Article 32 and Article 35 GDPR, respectively.

intermediary has a doubt as to the unlawful nature of the processing, it should inform the data subject thereof in accordance with Article 12(3) GDPR, request an extension to take a decision where necessary, and/or consult the competent DPA on the question.

As far as the obligation of **data protection by design and by default** is concerned, as well as general **security obligations**, it can be argued that intermediaries should design their services so as to ensure that the right to privacy and data protection of individuals is respected, considering *inter alia* the existing risk of online harassment via the services they offer. The requirements of data protection by design and default could play a vital role in preventing online harassment, as the implementation of a suitable design before launching an app, website or interface could significantly reduce such behaviours.¹⁴⁴⁴ Hence, when an intermediary offers a service which may directly allow individuals to share, publish or otherwise process personal data, and potentially to cause harm to third parties, the design of such services should be well thought-through, adapted and regularly updated so as to minimise the risks for the rights and freedoms of natural persons. The more important the intermediary is, the higher its level of responsibility would be under the GDPR, since the obligation of data protection by design and by default becomes stricter when the scope of the processing is large, and when the intermediary is able to afford the cost of implementation.¹⁴⁴⁵ Compliance with the obligation to ensure data protection by design and by default can be reached by adopting specific security or organisation measures, for example by requiring the identification of users prior to allowing them to share potentially sensitive or harmful information, or by screening specific type of content before their publication, when the absence of such measures could facilitate the unlawful processing of personal data in a way that would be overly detrimental for the rights and freedoms of data subjects concerned. As an illustration, in the Spanish case n°PS/00200/2021, it had been pointed out that allowing a random internet user to add a telephone number on a publicly accessible profile on an adult website, without putting measures in place to verify the correctness of this telephone number, breaches the principle of security of processing enshrined in Article 5(1)(f) GDPR. In this case, it can therefore be concluded that the intermediary had failed to ensure data protection by design and by default, and/or to adopt adequate security measures. At the level of big tech companies such as Meta or Google, these obligations could be interpreted in a way that would require from them to implement effective monitoring or reporting tools to prevent harassing behaviours such as doxing, impersonation or ‘revenge porn’.

There is, to date, an obvious lack of reliance of these alternative tools to combat various forms of online harassment. A review of the case-law of DPA and national

¹⁴⁴⁴ By analogy, see EDPB Guidelines 3/2022 on dark patterns, March 2022, available at https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf, p. 3.

¹⁴⁴⁵ Article 25(1) GDPR.

courts show indeed that the responsibility of the intermediaries is rarely engaged on the basis of their obligation to ensure data protection by design and by default, including by putting in place the necessary technical means to prevent or swiftly put an end to harassing behaviours. In the opinion of the author, the more these provisions will be put into motion to force intermediaries to adopt adequate security measures, offer effective reporting tools and better monitor the content on their website, the safer the digital sphere would become in general.

4.1.4.3. Concluding remarks on the functionality of the GDPR to combat online harassment

The above section has explored the functionality of the GDPR for protecting the right to privacy, data protection, human dignity, integrity, and freedom of expression of victims of online harassment. On the one side, it can be argued that the GDPR offers many functional tools in this respect. First, the broad meaning ascribed to the notion of 'personal data' and the restrictive interpretation given to the household exemption imply that almost all forms of online harassment fall within the scope of the GDPR. Second, the neutral stance of the GDPR allows data subjects to have recourse to these provisions without having to demonstrate the intention of the harassers to cause harm; the mere fact, for example, that sensitive personal data have been processed without the explicit consent of the data subject could render the processing unlawful by default. Third, the principle of accountability implies that it is for the concerned controllers to demonstrate that they have complied with the GDPR, rather than for the victim to prove that the processing of their personal data is unlawful. Fourth, the convenience with which data subjects may file a complaint with a DPA, and the investigative and corrective powers that the latter may use to stop and prevent further harassment, offer a clear advantage compared to more traditional ways for combatting harassment, such as filing a criminal complaint with the police force who still often lacks the necessary training and resources to fully apprehend this type of digital abuses. Fifth, in the event anonymity and/or the large number of harassers renders the identification and accountability of the harassers too difficult or laborious, data subjects have the possibility to address their request to the responsible intermediaries or file a complaint against them in the event they fail to react appropriately. The combined use of the GDPR and of the Digital Services Act may thus become particularly useful when combatting certain forms of harassment involving a multitude of individuals, such as online cyberbullying campaign or message bombing. Sixth, the GDPR offers various tools to foster the accountability of both harassers and intermediaries, from provisions on joint liability, to the obligation to ensure data protection by design and by default, to the existence of deterrent sanctions in the event of an infringement.

On the other side, the above section has also shown that some forms of harassment appear easier to combat by relying on the GDPR than others. In particular, the GDPR seems to offer more functional tools against 'one-to-one online harassment' where

the identity of the harasser is known. If sensitive personal data are being processed, the restrictive approach of Article 9 GDPR can also clearly facilitate the work of DPAs in holding the controller accountable for a breach. As a consequence, victims of online harassment may prefer relying on the GDPR rather than on provisions of criminal law in the context of 'one-to-one online harassment', as illustrated by the various harassment cases handled by the Icelandic, Spanish and Italian DPA analysed here above. The analysis of the case-law of DPAs involving harassing behaviours on the internet has also revealed that some DPAs appear more active than other in combatting this phenomenon through the application of data protection law. After having reviewed the entire corpus of these decisions, the author of this study noted that 90% of these cases had been handled by the Spanish DPA in particular, i.e., the AEDP. Nothing indicates however that online harassment would be more common in Spain than in the rest of the EU, or that data subjects located in Spain would be more aware of their rights under the GDPR than those located in other Member States. Hence, this high percentage is most likely the reflection of differing practices among DPAs. Once again, this seems to confirm that factors that are mainly external to the text of the GDPR, such as the resources, practices and legal culture of each DPA, may impact the manner in which the functionality of the GDPR is exploited and its FRO fulfilled. With a view of qualifying this finding, the functionality of the GDPR with respect to its FRO will once again be put to test in a second area: e-recruitment.

4.2. NON-DISCRIMINATION IN THE CONTEXT OF E-RECRUITING PRACTICES

From the screening algorithm of Saint George Hospital Medical School to *HireVue's* smart video interview software

In 1979, i.e., at a relatively early stage of the digitalisation of the European continent, St George Hospital Medical School¹⁴⁴⁶, an educational institute located in London, started using a computer algorithm to screen candidates for interviews. The algorithm had been developed by a member of St George's academic personnel in order to reduce the work of selecting applicants but also to eliminate any inconsistencies in the admission procedure of students. Seven years later, two senior lecturers at St George decided to review the corpus of decisions taken on the basis of the algorithm and found that the latter was discriminating against women and people with non-European sounding names, independently of any academic considerations.¹⁴⁴⁷ The algorithm had been originally developed and trained on the basis of admission data collected prior to 1979 at St George Hospital Medical School, at a time where a human panel was selecting the candidates. No change or correction were made in the data set on the basis of which the algorithm was developed. Hence, although the algorithm did not introduce any new bias, it reflected and systematised pre-existing human bias in the screening procedure. After

¹⁴⁴⁶ Now called St George's University of London (<https://www.sgul.ac.uk/>).

¹⁴⁴⁷ Lowry, S. I. & McPherson, G. (1988, March 5). A blot on the profession. *British Medical Journal*, 296(6623):657-658.

the two senior lecturers alerted the British Commission for Racial Equality on this issue¹⁴⁴⁸ and share with them their findings, St George was found guilty of practicing racial and sexual discrimination in its admission procedure, and the algorithm was never used again.¹⁴⁴⁹

This story shows that issues relating to so-called “*machine bias*”¹⁴⁵⁰ or “*algorithmic discrimination*”¹⁴⁵¹ in the field of recruitment are nothing new. Yet, as algorithms have become increasingly performant and now surpass humans in many fields when it comes to make complex decisions,¹⁴⁵² more and more companies are tempted to integrate them into their decision-making processes without always being aware of their inherent dangers in terms of systematised discrimination. As an illustration of a modern e-recruiting tool and the negative effects it can have, one may refer to *HireVue* video interview software and the criticism that it was already voiced with respect to its functioning.

HireVue, Inc. is a US company specialised in digital services for the purpose of recruitment. In 2009, *HireVue, Inc.* launched a video software with AI-elements for interviewing and evaluating job applicants.¹⁴⁵³ Candidates could download the HireVue app on their personal device, record a video in which they would answer several questions, and then submit their interview to the company offering the job position. One of the key features of *HireVue* video software was its complex algorithm which would analyse both the facial movement and speech of the interviewee. Each candidate would then receive an employability score on the basis of these elements before being ranked against other candidates. On their website, HireVue, Inc. claimed that this tool would help companies “*increase diversity and mitigate bias*” by using “*AI-driven predictions*”.¹⁴⁵⁴ Despite this, *HireVue* has been heavily criticised by researchers and journalists for calculating an “*unfounded blend of superficial measurements and arbitrary number-crunching that is not rooted in scientific facts.*”¹⁴⁵⁵ The company – for reasons relating to trade secret and intellectual property law – has never agreed to release the code of its video

¹⁴⁴⁸ The CRE was a publicly funded, non-governmental body set up under the Race Relations Act 1976 to tackle racial discrimination and promote racial equality. On 1 October 2007, the CRE was dissolved, and its functions taken over by the Equality and Human Rights Commission (EHRC). See <https://www.gov.uk/government/organisations/equality-and-human-rights-commission>.

¹⁴⁴⁹ For the full detailed story, please refer to the article by Lowry, S. I. & McPherson, G. (1988, March 5). *op. cit.*

¹⁴⁵⁰ Angwin, J., Larson, J., Mattu, S. & Kirchner, L. (2016, May 23). Machine Bias. There’s software used across the country to predict future criminals. And it’s biased against blacks. *ProPublica*. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

¹⁴⁵¹ Hacker, P. (2018). Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, 55(4):1143–1185.

¹⁴⁵² Bailey, R. (2019). Can Algorithms Run Things Better Than Humans? Welcome to the Rise of the Algocracy. *Reason Magazine*, 50(8):20-26; Brkan, M. (2019). Do Algorithms Rule the World? Algorithmic Decision-making and Data Protection in the Framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 27(2), p. 97.

¹⁴⁵³ The website of the company is accessible via <https://www.hirevue.com>.

¹⁴⁵⁴ Quote taken from HireVue website on 9.02.2021, <https://www.hirevue.com/employment-diversity-bias>.

¹⁴⁵⁵ Harwell, D. (2019, October 25). A face-scanning algorithm increasingly decides whether you deserve the job. *The Washington Post*. <https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/>.

interview software. Then, in 2019, the non-profit Electronic Privacy Information Center (EPIC) filed a complaint against the company with the US Federal Trade Commission alleging that HireVue's use of AI to assess job candidates constituted "unfair and deceptive trade practices." Because of this complaint and pressure from civil society, HireVue, Inc. eventually mandated ORCAA, a firm specialised in algorithmic auditing, to analyse and test its video interviewing software. Following that audit (whose results were probably negative), HireVue, Inc. ultimately announced on 12th January 2021 that it had decided to remove facial analysis from its video interviewing software.



In the opinion of the author, the case of Saint George Hospital Medical School and the criticism addressed to *HireVue* video interviewing software are both representative of how the use of algorithmic decision-making can potentially interfere with the right not to be discriminated in the field of recruitment, as further discussed below.

After defining 'e-recruitment' and highlighting the impact that these DDTs can have on the right not to be discriminated, the below sections will explore how the GDPR could be used as a tool to better monitor and regulate the effects of e-recruiting tools on data subjects' fundamental rights.

4.2.1. Defining e-recruitment or e-recruiting practices

From the outset, the author would like to make two important distinctions between online harassment (the first selected 'test area') and e-recruitment (the second 'test area'). First, while online harassment is considered negative by nature, e-recruitment is not. This is because e-recruitment, and more generally algorithmic decision-making, is not harmful as such. As a matter of facts, algorithms are made of mathematical formula which are neutral by nature, and which remain without any effects until an actual person puts them into motion. In many cases, relying on algorithmic decision-making can become a good method to combat discrimination traditionally stemming from human decision-making.¹⁴⁵⁶ In other cases, it may on the contrary negatively affect a particular group of individuals. In the end, whether

¹⁴⁵⁶ Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, 4(10):1572-1593, p. 1575.

an e-recruiting tool will have positive or negative effects for individuals' rights and freedoms will thus depend on how the underlying algorithms have been elaborated, and/or how the tool is used in practice. Keeping this in mind, the purpose of this section is not to advocate for the prohibition or prevention of e-recruiting practices in general as something systematically harmful for data subjects' fundamental rights and freedoms. Rather, this section will point out that e-recruiting tools can either have positive or negative effects for the rights and freedoms of individuals, highlight the importance of monitoring those effects, and suggest ways to prevent or combat potential discriminatory outcomes on the basis of EU data protection law.

Second, unlike the notion of online harassment, e-recruitment is explicitly mentioned by EU data protection law, and in particular by the GDPR. Recital 71 of the GDPR indeed refers to e-recruitment as a possible example of automated-individual decision making or 'AIDM'. AIDM has been defined by, and is subject to specific rules, set out in Article 22 of the GDPR. Taking this into consideration, this section will first define e-recruitment in general terms, and then more specifically in light of the notion of AIDM.

4.2.1.1. General e-recruiting practices: conceptualising the notion of 'e-recruitment'

E-recruitment has been defined as *"the use of any technology to attract, select or manage the recruitment process"*.¹⁴⁵⁷ E-recruitment can be conducted by actors from both the private or the public sector, for example by a public authority for hiring public officers, or by a company for identifying new recruits or offering a promotion to existing ones. Furthermore, e-recruitment is not limited to the field of employment as such, but can also extend to any fields where candidates are recruited on the basis of individual characteristics, including the field of education (e.g. selection of students by a University during the enrolment procedure), sport (e.g. recruitment of new players by a football club), professional occupation (e.g. promotional event by a law firm to hire high-performing graduates) or vocational training (e.g. selection of apprentices by a factory). The 'e' in e-recruitment indicates that part or all of the decision-making process is automated. Such automation usually derives from the use of algorithms that have been elaborated to support or replace human decision-making. Hence, e-recruiting practices¹⁴⁵⁸ must be understood as practices involving algorithmic decision-making to support or replace human decision-making with a view of identifying, evaluating and/or selecting individuals for a position or an advantage.

¹⁴⁵⁷ Giraed, A. & Fallery, B. (2009). E-recruitment: new practices, new issues, an exploratory study. *Proceedings of HRIS'2009 11th International Conference ICEIS in Human Resource Information System*, pp. 39-48. For similar definitions, see also: Parry, E. & Tyson, S. (2008). An analysis of the use and success of online recruitment methods in the UK. *Human Resource Management Journal*, 18(3):257-274; Holm, A. B. (2012). E-recruitment: the move towards a virtually organized recruitment process. De Juana-Espinosa, S., Fernandez-Sanchez, J.A., Manresa-Marhuenda, E. & Valdes-Conca, J. (eds). *Human Resource Management in the Digital Economy: Creating Synergy Between Competency Models and Information*. IGI Global, Hershey PA, p. 92.

¹⁴⁵⁸ In accordance with the expression used by Recital 71 of the GDPR.

The use of algorithms for the purpose of decision-making can take place at one or different stage(s) of the recruitment process. For the sake of clarity, and keeping in mind the various objectives that e-recruiting tools may fulfil, the author has identified three stages in particular:

- 1) Promotion:** at this stage, the recruiter may already rely on a e-recruiting tool to identify its target audience with a view of promoting a position or advantage, that is, to present them with an *opportunity to apply*.

E.g., a yoga school may be advertising a community manager position on LinkedIn by targeting female individuals between the age of 25 and 35 who have graduated from a marketing school and have already showed interest in sport and/or yoga;

- 2) Pre-selection:** at this stage, the recruiter may rely on an e-recruiting tool (for example, an online cognitive test) in order to evaluate the skills, competences or overall suitability of candidates in order to decide whether to pre-select them or not. Pre-selection supposes that, even if a candidate is successful, the latter is not yet granted a tangible offer or advantage, but rather an *opportunity to be selected* (for example, the candidate is shortlisted for a final interview). This stage may in itself be divided into multiple stages (for example, the cognitive test may be followed by two subsequent rounds of interviews).

E.g., a law firm may invite candidates who have applied for a position to take an online test in order to evaluate their oratory and writing skills (first pre-selection stage); depending on their performances, candidates may be invited to a interview (second pre-selection stage). If the candidates have been shortlisted, they will be invited for a final interview.

- 3) Selection:** at this stage, the recruiter may rely on an e-recruiting tool to evaluate the skills, competences or overall suitability of a candidate, with a view to present them with an actual *offer or advantage*.

E.g., a university could be relying on a smart algorithm to analyse the diploma and grades of candidates to determine which ones will be granted a spot within a specific master programme.

Some recruiters may not feel the need to promote and/or pre-select candidates, in which case they could immediately evaluate them with a view to either reject or select them for an actual position or advantage. The first and second stage of recruitment may thus be skipped if they are deemed unnecessary by the recruiter. Furthermore, e-recruiting tools can be used as an alternative to human decision-

making at one, two or all stages of the recruitment process. For example, a company could be looking for candidates by relying on a smart algorithm at the pre-selection stage (including, as the case may be, by using the search & match algorithm of recruitment platforms such as LinkedIn) before relying on its human resources department to actually evaluate and select the final candidates. Another company, by contrast, could be relying on a human panel to pre-select candidates for an interview, but then rely on a fully automated cognitive test to offer a position to the two best-performers. Finally, it must be noted that, within a single stage of the recruitment process, e-recruiting tools can be used either alone or in combination with human reviewers. For example, for the purpose of evaluating all candidates who have applied for a job position, a recruiter may request them to pass an online test, the results of which may in parallel be scrutinized or modified by a human reviewer.

4.2.1.2. E-recruitment practices qualifying as AIDM under Article 22 of the GDPR

Within algorithmic decision-making tools, two different types of tools can be distinguished in light of Article 22 GDPR. Indeed, this article provides that if a decision is *fully automated* and produces *legal or similarly significant effects* on an individual, this decision is the result of an *automated individual decision-making* or 'AIDM'. AIDM is specifically regulated under Article 22 of the GDPR, in the sense that more obligations are imposed on controllers and additional rights are granted to data subjects, as already discussed above (see Section 3.2.2.2(v)).

Some recruitment procedures involve a series of decisions which may or may not fall under Article 22 of the GDPR. For ensuring the correct application of the GDPR, it is thus primordial to analyse each decision separately to determine which ones could eventually qualify as an AIDM on its own. This should especially be the case for decision-making procedures involving both algorithms and humans. Whether a specific decision, at any stage of a recruitment procedure, qualifies as an AIDM regulated by Article 22 of the GDPR will depend, *inter alia*, on the oversight exercised by the human(s) involved in the overall procedure. To illustrate this, one may imagine a hypothetical recruitment process in the field of education, as developed here below.

In many Member States, higher education institutions, including universities, are facing an overwhelming amount of admission requests. Some faculties, however, only have a very limited number of available places in comparison to the number of applications. This is often the case, for example, for faculties of medicine. As it has

already been the case in such situations,¹⁴⁵⁹ the ministry of education of a Member State could thus be tempted to elaborate and implement a semi-automated decision-making procedure designed to fairly and timely allocate all available places within the faculties of medicine of that country. Such a procedure could be composed of the following steps:

- As a first step, the candidates wishing to study medicine must submit their high school diploma as evidence that they have satisfactorily completed secondary education – the overall average grade indicated on this diploma is calculated and confirmed by a human panel composed of their high school teachers;
- As a second step, an algorithm would calculate, based on the total number of places available in each university as well as the total number of candidates, the minimum average grade that a candidate must have obtained at the end of high school to be given the opportunity to study medicine; all candidates who do not fulfil this criterion would then automatically be informed that they have been excluded from the admission procedure;
- As a third step, the remaining candidates would be invited to submit an application form online. This would require them to fill in various personal data, such as name, age, gender, spoken languages and place of residence, and to select five universities where they would like to be admitted by order of preferences. Taking into consideration this wish list, the language requirements of the concerned universities, their respective level of popularity as well as their location, the algorithm would then automatically select three universities for each candidate and ranks those three establishments in accordance with a ‘suitability score’: A (best match), B (second best match) or C (third best match).
- As a fourth and final step, all the three selected universities would automatically receive access to the profile of the candidates with whom they have been matched. An admission panel within each university would then review those profiles and either accept or reject the concerned candidates, taking into account, *inter alia*, the ‘suitability score’ given by the algorithm. In the situation where multiple universities accept the application of the candidate, the latter could decide in which establishment they would like to study; if *only one* of the selected universities has accepted the application of a candidate, the latter would be invited to enrol in that university; finally, in the exceptional case where all three universities have rejected the

¹⁴⁵⁹ This algorithmic process is inspired by “Admission Post-bac”; an algorithmic process which was used by the Ministry of Education in France between 2009 and 2017 to allocate places within graduate schools, institutions or universities. It has been modified as from 2018 and is now known as “Parcoursup” (see <https://www.parcoursup.fr/>).

application of a candidate, the latter would be automatically admitted in the establishment with the best suitability score (this decision being binding on the concerned university).

If this entire procedure was considered as a single decision-making process, it would most probably not qualify as an AIDM under Article 22 of the GDPR since humans are being meaningfully involved at least at two moments of the procedure. Indeed, within the primary step, the overall grade obtained by each candidate at the end of high school is calculated and validated by a human panel composed of their high school teachers. Then, within the fourth step, it is once again a human panel within each selected university which formulates the decision to accept or reject a given application. At those two stages, the concerned panels have both the authority and the competence to take that decision. On this basis, it would be tempting to conclude that this selection procedure is not an AIDM in the sense of Article 22 GDPR. Yet, if one would identify each single decision made with respect to the candidates and assess whether each of these decisions could qualify as an AIDM on its own, this conclusion would largely differ. In this hypothetical example, four decisions in particular must be distinguished: (i) the decision to grant a high school diploma and the overall grade attached to it, as decided by a human panel; (ii) the automated decision to exclude some of the candidates from the admission procedure based on their average grade, as decided by the algorithm; (iii) the automated decision to select three universities from the wish list of each candidate and to rank these universities on the basis of a suitability score; and (iv) the decision taken by a human panel within each of the selected university to accept or reject the concerned candidates, taking into account, *inter alia*, the given suitability score.

From the outset, it must be noted that all these decisions could potentially have a direct influence on the final chances of admission of the candidates and could therefore be considered as significantly affecting the life of the candidate (although such considerations must be made on a case-by-case basis). The first decision – regarding whether the data subject is granted a high school diploma – has of course significant effects on the candidate since it will determine whether the latter is admissible to the procedure or not, with no other opportunity or alternative elsewhere. Because this decision is taken by a panel of high school teachers, however, it will not qualify as an AIDM under Article 22 GDPR. The second decision concerns the exclusion of candidates who are no longer admissible to the procedure because their overall grade is below the required average. Because this decision can have a significant impact on the life of the candidates and is taken *purely* by automated means, it can be argued that such a decision is regulated under Article 22 GDPR. Even when considering the recruitment procedure in its entirety, it must indeed be acknowledged that none of the human panels involved in the procedure has the capacity to review or depart from this exclusion decision. In particular, neither the high school teachers involved at the beginning of the procedure, nor the university panel involved at the end of the procedure, has the possibility to reverse

such a decision. For the same reason, the third (automated) decision through which three universities are selected and ranked on the basis of suitability score could also qualify as an AIDM, depending on the impact that such a decision can have on the life of the candidate. It can indeed be assumed that, in some instances, such a decision will significantly affect the life of the individuals concerned since it will *de facto* deprive them from the possibility to be considered by other universities (including, for example, universities located in the same city/region where the candidates already reside and where the costs of housing would thus not become a factor ultimately preventing them to enrol). Furthermore, this decision is taken *solely* by automated means, given that no human is involved at this stage of the process. At the end of the procedure, a fourth decision is taken by a human panel within each university; this panel can decide to accept or reject the application of the pre-selected candidates. If the 'suitability score' given by the algorithm is not blindly followed by this human panel, then, such a decision can be considered as being (at least partly) taken by humans and will thus not qualify as an AIDM. Looking at the overall procedure, it therefore appears that, while the first and last decisions are taken by humans, the second and third decisions could each be considered as an AIDM in the sense of Article 22 GDPR, with all the obligations that such characterization implies for the data controller. In the opinion of the author, the main reason why these two decisions should be considered distinctly from the rest of the procedure is that the humans involved at the beginning and at the end of the procedure are unable to meaningfully review, overturn or depart from such decisions.

The above section has showed that AIDM is a sub-type of ADM that is specifically regulated under Article 22 of the GDPR. Yet, even if a decision does not qualify as an AIDM under Article 22 of the GDPR, it may still interfere with the rights and freedoms of the data subjects, such as the right not to be discriminated. Hence, both possibilities will be considered and scrutinized within this section. From a terminological point of view, in the following sections and Chapters, each time the author will refer to 'AIDM', it should be understood as a fully automated decision-making process that has legal or similarly significant effects on the data subject, as defined and regulated under Article 22 of the GDPR. By contrast, when the author refers to ADM in general, it should be understood as comprising all types of automated decision-making, including those falling outside of the scope of Article 22 GDPR.

4.2.2. The nature and degree of impact of e-recruitment on non-discrimination

When reading on ADM, and on e-recruiting practices in particular, it quickly appears that, beyond privacy and data protection, most fears and concerns have crystallised around the impact that such practices could have on one important fundament right

in particular: non-discrimination.¹⁴⁶⁰ Hence, the below section will explore both the *nature* and the *degree* of impact of e-recruiting tools on non-discrimination.

First, with respect to the *nature* of such an impact, it will be shown that e-recruitment can either be positive or negative for the rights of candidates, as they can either prevent or contribute to discriminatory outcomes. Second, as far as the *degree* of this impact is concerned, it will be shown that e-recruiting tools can either have significant effects on individuals, or superficial effects on them, depending on the context.

Although the author will limit her analysis to the field of recruitment, the below considerations may also be applicable *mutatis mutandis* to ADM in other fields, such as criminal justice (e.g. automated 'risk score' attributed to defendants), banking (e.g. automated denial of a loan or closure of a bank account), public security (e.g. automated decision to deploy police forces within a specific neighbourhood), provision of goods and services (e.g. automated removal, by Airbnb, of reviews from guests that are deemed in violation of their Review Policy) or healthcare (e.g. automated triage of patients on the basis of their symptoms in the midst of a pandemic).

4.2.2.1. The nature of the impact of e-recruiting tools on non-discrimination: allies or trojan horses?

Algorithmic selection tools are normally primarily conceived with a view of ensuring more efficiency, accuracy, relevance and/or objectivity in the decision-making process. Unlike humans indeed, machines are able to simultaneously process and analyse large quantities of data on the basis of a comprehensive list of objective criteria, without any physical constraints or cognitive bias. Machines thus often outperform humans with respect to decision-making both in terms of quality and quantity because of their processing capacity and non-blooded intelligence. This is also the case in the field of recruitment where objectively analysing a large number of CVs and cover letters within a limited time frame may become challenging for the human mind. As an illustration, in 2014, the Harvard Business Review analysed seventeen different studies on the use of algorithmic tools for the purpose of recruitment and found that a simple algorithm usually outperforms human decisions by at least 25%, regardless of the nature of the job position.¹⁴⁶¹ Their conclusion was

¹⁴⁶⁰ For a systematic review of papers published with respect to algorithmic decision-making in the context of human resources management, see, in particular: Köchling, A. & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, 13:795-848. See also Council of Europe (2017). *op. cit.*, p. 26; Zuiderveen Borgesius, F. J. (2018), *op. cit.*

¹⁴⁶¹ Kuncel, N. R., Ones, D. S. & Klieger, D. M. (2014, May). In Hiring, Algorithms Beat Instinct. *Harvard Business Review*, 92(5):32.

that even recruiting experts would thus be better off leaving such selection to machines rather than trusting their own instincts or competences.¹⁴⁶²

Besides helping companies or institutions to find the 'right match' in a cost-effective manner, e-recruiting tools can also potentially enhance the respect of the rights and freedoms of candidates by preventing direct or indirect discrimination traditionally stemming from human bias. E-recruiting tools can indeed be programmed in a manner which may prevent direct forms of discrimination from occurring, such as when human recruiters tend to exclude potential female candidates because of gender bias, or when human recruiters reject applicants with foreign-sounding name because of racial prejudices.¹⁴⁶³ E-recruiting tools can also prevent more subtle or indirect forms of discrimination, such as the tendency of interviewers to hire 'mini-mes', i.e., candidates that resemble them.¹⁴⁶⁴ As far as e-recruiting tools are concerned, computer scientists have the possibility to open the code of an algorithm and work on it to determine and refine which attributes should or should not be taken into account by the algorithm when formulating a result, recommendation or decision. By contrast, it is not possible to open a human brain and get rid of existing mental bias. Altogether, there is thus no doubt that e-recruitment tools have the potential to become great allies not only for employers looking for the 'right match', but also for candidates who want their application to be objectively and fairly considered.¹⁴⁶⁵

As one could expect, most companies specialised in the development of e-recruiting tools actively advertise their products as increasing objectivity, reducing human bias and thus ensuring more diversity and/or fairness in the hiring process. This is the case, for example, for HireVue,¹⁴⁶⁶ Hiretual,¹⁴⁶⁷ Swyg,¹⁴⁶⁸ Modern Hire,¹⁴⁶⁹ or Mya

¹⁴⁶² *Ibid.*

¹⁴⁶³ Edo, A. (2013) *La Discrimination à l'embauche sur le Marché du Travail Français*. Paris: Éd. Rue D'Ulm; Bertrand, M. & Mullainathan, S. (2004). Are Emily and Greg more employable than Lakisha and Jamal? A field experiment on labor market discrimination. *Am. Econ. Rev.*, 94:991–1013.

¹⁴⁶⁴ In an interview given to the Washington Post, Unilever's chief human resource officer said that HireVue had helped steer managers away from hiring only "mini-mes" who look and act just like them, thereby (allegedly) boosting the company's "diversity hires" by about 16%. Source: Harwell, D. (2019). *op. cit.*

¹⁴⁶⁵ Hensler, J. (2019). Algorithms as Allies: Regulating New Technologies in the Fight for Workplace Equality. *Temple International & Comparative Law Journal*, 34(1):31-60.

¹⁴⁶⁶ HireVue, Inc. claims their software "increase diversity and mitigate bias", and that "HireVue's AI-driven approach mitigates bias by eliminating unreliable and inconsistent variables (...)". Source: <https://www.hirevue.com/employment-diversity-bias>. HireVue also published *AI ethical principles*. Source: <https://www.hirevue.com/why-hirevue/ai-ethics>.

¹⁴⁶⁷ On their website, Hiretual claims that using their products can "fill Existing Diversity Gaps" and leaves "no room for unconscious bias". They further invite their prospective clients to "Build an equal screening process with Blind Sourcing Mode by hiding names and images from profiles. Further, remove bias by sourcing from talent pools consisting of all underrepresented groups using Blind Diversity Sourcing.". Source: <https://hiretual.com/features/diversity-inclusion/>

¹⁴⁶⁸ On their homepage for recruiters, Swyg states: "Traditional CV screening and interviewing processes are biased. (...) Swyg solves this problem by soliciting reviews from multiple interviewers and by using A.I. technology. We actively detect and correct for bias." Source: <https://v1.swyg.com/employers/>.

¹⁴⁶⁹ On its website, Modern Hire states that their products promote "A transparent and candidate-centric recruiting process. (...) A transparent and candidate-centric digital recruitment process ensures fairness, helping you achieve the results and outcomes you require." Source: <https://modernhire.com/results/recruiter-experience/>. Modern Hire also promotes its AI tool, CognitiOn, as being built to reduce bias. Source: <https://modernhire.com/cognition/>.

Systems, Inc.¹⁴⁷⁰ Yet, whether e-recruiting tools truly increase fairness and equality in the hiring process ultimately depends on how well the underlying algorithms have been elaborated and how such tools are being implemented in practice. If poorly designed or improperly used by humans, algorithmic decision-making tools may indeed also create adverse effects for the interests, rights or freedoms of the data subjects concerned, as already exemplified by the case of Saint George Medical School. Of course, one may be tempted to think that the case of Saint-George Medical School is an isolated case from the past, and that such errors would no longer happen today based on the increased level of knowledge and technical abilities in the field of computer sciences. However, several recent cases have showed that the elaboration of flawless e-recruiting tools still represents a real challenge and may lead to discriminatory outcomes, as illustrated below.

4.2.2.2. The degree of impact of e-recruiting tools on non-discrimination: significant or superficial?

Besides the nature of the impact that e-recruitment can have on equality and non-discrimination (i.e., positive or negative), the degree of impact will also vary depending, *inter alia*, on the characteristic of each tool and the stage at which it is deployed. As a reminder, three stages can be distinguished in particular: (1) the promotion stage (where e-recruiting tools are used to target an audience with a view of promoting a position or advantage, for example showing a job advertising to a specific group on social media); (2) the pre-selection stage (where e-recruiting tools are used to evaluate the suitability of candidates for short-listing them, for example through a cognitive test); and (3) the selection stage (where e-recruiting tools are used to select candidates for presenting them with an actual job offer or advantage). To illustrate the varying degree of impact that e-recruiting tools can have depending on the stage at which they are deployed, two cases will be presented here below: one concerns an advertising tool offered by Google, while the second concerns a screening algorithm used by Amazon, Inc.

‘Google Search’ is the most popular online search engine in the world. Although using it is free, Google makes revenues by displaying ads within or along search results. In other words, companies are paying Google for displaying these ads on their behalf. Google started displaying paid ads in 2000 already. Google’s advertising system is based partly on cookies and partly on keywords determined by the companies paying for the ads. The algorithms undergirding this system have been refined over time, so as to show internet users increasingly relevant and individualised ads. These ads often promote goods or services, from a fashionable new pair of shoes to a trip to the Bahamas. However, they can also promote events or advantages, from music concerts to open job positions. In 2015, a study

¹⁴⁷⁰ On their website, the company claims that: “Choosing Mya means you’ve chosen an AI recruiting assistant that is optimized to prevent unconscious bias.” Source: <https://www.mya.com/blog/possible-prevent-unintentional-bias-in-ai/>.

conducted by two scholars from Carnegie Mellon University and a scholar from the International Computer Science Institute of Berkeley University shed light on the lack of transparency of Google advertising system. In particular, they found that this system was showing less ads for high-paid job to women than men.¹⁴⁷¹ It must be kept in mind however that it was still possible for these women to receive information or apply for these high-paid jobs via other channels. As such, not seeing an advertising for a job does not amount to the loss of an opportunity. Rather, it may deprive an individual from *having been made aware* of an opportunity.

The second case concerns an e-recruiting tool developed and used for several months by Amazon, Inc. The worldwide success of Amazon has largely been built on the use of automation for organising its giant warehouses, making fast purchasing decisions, as well as calculating and setting the price of goods on its various websites. Therefore, when Amazon announced that it had elaborated and used a smart hiring tool between 2014 and 2016 to recruit new qualified staff members, such revelation did not really come as a surprise.¹⁴⁷² This e-recruiting tool, undergirded by a smart algorithm capable of analysing candidates' CVs, was assigning a score ranging from one to five stars to each applicant, five being the maximum. However, the manner in which this score was actually being calculated by the algorithm remained opaque. As already mentioned above, lack of transparency is a common trait of smart algorithms. Indeed, when relying on machine-learning techniques for elaborating a performant predictive model, developers are unable to control from beginning to end the attributes or categories of data that the algorithm will ultimately favour for detecting and selecting the target variable (see above, Chapter 1, point A, Terminology). Hence, the quality of the tool can only be assessed *a posteriori* by analysing the quality of its output. In the case of Amazon's e-recruiting tool, for example, it was ultimately found that the algorithm had integrated pre-existing human bias against women and was replicating them when women were applying for developer and other 'tech' positions. The output data revealed indeed that qualified female candidates were often rejected or ranked below male candidates without any objective reason. This was most likely due to the fact that the dataset used to train the algorithm, i.e., the resumes submitted (mainly by men) for similar positions over a 10-year period, had misled the algorithm into concluding that being a woman was an adverse attribute for tech jobs. Excluding the gender of the applicants from the input data also proved to be insufficient to prevent such discriminatory outcomes, since other data correlating with gender could still be picked up by the algorithm. As reported by Reuters indeed, "*Amazon's system taught itself that male candidates were preferable. It penalized resumes that included the word "women's," [such] as in "women's chess club captain." And it downgraded graduates of two all-women's colleges (...).*"¹⁴⁷³ Given the difficulties or

¹⁴⁷¹ Datta, A. & Tschantz, M. (2015). Automated Experiments on Ad Privacy Settings. *Proceedings on Privacy Enhancing Technologies*. 1(10):1515.

¹⁴⁷² Dastin, J. (2018, October 11). Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*. [https:// www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G](https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G).

¹⁴⁷³ *Ibid.*

even impossibility to eliminate from the application documents all potential proxies correlating with gender, Amazon ultimately disbanded the project beginning of 2017 “because executives [had] lost hope for [it]”.¹⁴⁷⁴ According to Amazon Inc., human recruiters were not relying on this score as a conclusive factor in the hiring decision, but rather as a recommendation.¹⁴⁷⁵ Yet, this flawed e-recruiting tool was used for two years by Amazon recruiters before being abandoned, potentially depriving hundreds if not thousands of women from a fair assessment, and in some instances from an actual job.

These two examples show that, as a rule of thumb, a correlation can be found between the degree of potential individual harm caused by an e-recruiting tool and its complexity, as well as the stage at which it is deployed, and in particular whether it concerns a chance, an opportunity or an actual offer.

4.2.3. The sources of discrimination in the context of e-recruitment

Tackling discrimination arising from the use of ADM is an endeavour that appears all the more challenging when taking into account the many potential sources of such discriminatory outcomes. In a seminal paper, Barocas and Selbst – two American scholars – have distinguished five ways in which algorithmic decision-making can lead to discrimination:¹⁴⁷⁶ (a) the poor quality of the ‘target variable’ and ‘class labels’¹⁴⁷⁷ (e.g. in the field of recruitment, determining what looks or doesn’t look like the ‘sought recruit’); (b) the poor quality of the training data (e.g. training data supposed to provide examples of the ‘sought recruit’ can be incomplete or reflect pre-existing human bias); (c) the poor quality of the selected features (e.g. the features of a ‘sought recruit’ that were picked on by the e-recruiting tool can lack relevance or emphasize bias); (d) the existence of proxies (i.e., factors that are neutral in appearance but may lead to indirect discrimination) or (e) masking (i.e., when an algorithmic tool is used *on purpose* for discriminatory ends).

In the context of this study, the author would like to propose a more straightforward categorisation by distinguishing two types of situations in which e-recruiting tools may lead to direct or indirect discrimination: situations in which a discriminatory outcome stems from *the algorithm itself* because it has been poorly elaborated (inbuilt bias); and situations in which a discriminatory outcome stems from the *non-appropriate or malign use of the algorithmic tool by the data controller/processor*.¹⁴⁷⁸ Keeping this important distinction in mind, the below section will highlight the main

¹⁴⁷⁴ *Ibid.*

¹⁴⁷⁵ *Ibid.*

¹⁴⁷⁶ Barocas, S. & Selbst, A. D. (2016). *op. cit.*

¹⁴⁷⁷ *Ibid.*, p. 678: “While the target variable defines what data miners are looking for, “class labels” divide all possible values of the target variable into mutually exclusive categories.”

¹⁴⁷⁸ This would correspond to the issue of ‘masking’ according to the categorization proposed by Barocas and Selbst (2016).

risks that e-recruiting practices pose for data subject's fundamental rights, and in particular the right not to be discriminated.

4.2.3.1. Discrimination stemming from the poor design of e-recruiting tools

Research has already shown that algorithmic decision-making that is in appearance unbiased can lead to discriminatory models if they are poorly elaborated.¹⁴⁷⁹ In particular, lack of diligence in the collection and labelling of the training data or in determining the relevance of the data variables for the purpose of differentiating between individuals, may lead to unwanted inbuilt biases,¹⁴⁸⁰ where the algorithm itself becomes the problem.¹⁴⁸¹ To better understand this issue, it seems useful to distinguish between two forms of discrimination: (i) direct discrimination and (ii) indirect discrimination.

Direct discrimination occurs where a decision-maker bases a decision concerning an individual directly on criteria or factors which are regarded as unlawful because discriminatory.¹⁴⁸² Article 21 of the Charter cites the following factors as potential factors of discrimination: gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political opinion, national minority, property, birth, disability, age or sexual orientation. As an illustration, the decision of a recruiter to systematically reject women for managerial position because they might want to have children and thus take a maternity leave is a form of *direct* discrimination based on gender. Similarly, in the case of Saint-George Medical School or Amazon e-recruiting tool presented above, it was found out that both algorithms were excluding female applicants for no other apparent reason than their gender, thereby systematising a form of *direct* gender-based discrimination.¹⁴⁸³ As to the source of such inbuilt bias, it was found to stem from the training data themselves which embedded many pre-existing human biases against female and foreign applicants, which the algorithm merely reflected and systematized. As explained by Barocas and Selbst indeed, "*data is frequently imperfect in ways that allow these algorithms to inherit the prejudices of prior decision makers.*"¹⁴⁸⁴ Arguably, however, relying on properly elaborated algorithms rather than humans may ultimately be a more effective way to prevent direct discrimination. This is because, contrary to humans, algorithm can be specifically programmed so as to exclude or disregard

¹⁴⁷⁹ Custers, B., Calders, T., Schermer, B. & Zarsky, T. (2013). *Discrimination and Privacy in the Information Society*. SAPERE. Springer, pp. 43-57.

¹⁴⁸⁰ Jobin, A., Ienca, M. & Vayena, E. (2019, September 2). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9):389–399.

¹⁴⁸¹ Sandvig, C., Hamilton, K., Karahalios K. & Langbort, C. (2016). *op. cit.*, p. 4974.

¹⁴⁸² Council of Europe (2017), *op. cit.*, p. 26.

¹⁴⁸³ Gender and ethnicity are both recognized as potential factors of discrimination in Article 21 of the Charter as well as in the Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

¹⁴⁸⁴ Barocas, S. & Selbst, A. D. (2016). *op. cit.*, p. 671.

certain attributes associated with a risk of discrimination.¹⁴⁸⁵ When elaborating or training an e-recruiting tool, for example, it is in theory possible to delete any data relating to gender, race or nationality from the data set, and/or to exclude such data from the list of relevant variables that are analysed by the algorithm to take a decision. Forcing the human brain to exclude or fully disregard such information before taking a decision is, by contrast, impossible. Hence, in theory, algorithmic decision-making could annihilate direct discrimination in places where it is common, such as in the field of recruitment.¹⁴⁸⁶ In practice, however, it has been found that even algorithms that were designed so as to exclude or disregard discriminatory factors can still *indirectly* produce discriminatory outcomes, as explained below.

Indirect discrimination occurs where a decision-maker bases a decision on one or several criteria or factors which, in appearance, are both relevant and objective, but which, indirectly, lead to discrimination because of their high level of correlation or dependence with a protected characteristic, such as gender, ethnicity or sexual orientation.¹⁴⁸⁷ In the context of indirect discrimination, it is therefore not relevant whether the user of the algorithmic decision-making tool intended to discriminate or not; it is the effect of the practice that counts.¹⁴⁸⁸ As stated by the Advocate-General Maduro, “*this is the whole point of the prohibition of indirect discrimination: even neutral, innocent or good faith measures and policies adopted with no discriminatory intent whatsoever will be caught if their impact on persons who have a particular characteristic is greater than their impact on other persons.*”¹⁴⁸⁹

In the field of algorithmic decision-making, a factor or attribute which appears neutral in appearance, but which eventually leads to a discriminatory result, is usually referred to as a *proxy*,¹⁴⁹⁰ precisely because it acts as an *agent* or *proxy* for a discriminatory factor. For example, in the field of recruitment, the postal code of a candidate can become a proxy for discrimination because it may correlate with some protected characteristics, such as ethnicity.¹⁴⁹¹ Prima facie, postal codes appear as both neutral and relevant information for selecting candidates, as it may be objectively argued, for example, that employees having a shorter commuting time

¹⁴⁸⁵ Discriminatory factors are features relating to human identity which have been recognized by law as potential factors of unlawful discrimination. In light of Article 21 of the Charter, entitled ‘Non-discrimination’, discriminatory factors include: sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

¹⁴⁸⁶ Council of Europe (2017). *op. cit.*, p. 27.

¹⁴⁸⁷ *Ibid.*

¹⁴⁸⁸ Zuiderveen Borgesius, F. J. (2020). *op. cit.*, p. 1577.

¹⁴⁸⁹ CJEU, Opinion of AG Maduro of 31 January 2008, *Coleman*, Case C-303/06.

¹⁴⁹⁰ Zuiderveen Borgesius, F. J. (2018). *op. cit.*, p.13.

¹⁴⁹¹ Postal codes are often used as examples of factors that may lead to indirect discrimination. See, for example, Council of Europe (2018), *op. cit.*, p. 13 ; Barocas, S. & Selbst, A. D. (2016). *op. cit.*, p. 689; Kilbertus, N., Rojas-Carulla, M., Giambattista, P., Hardt, M., Janzing, D. & Schölkopf, B. (2017). Avoiding Discrimination through Causal Reasoning. *Advances in Neural Information Processing Systems*, 30:656-666; Zuiderveen Borgesius, F. J. (2020). *op. cit.*

tend to be more punctual and happier, and thus more productive at work.¹⁴⁹² Hence, a company whose offices are located in the centre of a big city may decide to favour CVs of applicants who live close-by. Yet, postal codes may indirectly lead to discriminate specific groups of individuals sharing the same protected characteristics, such as young workers from modest social origin who cannot afford housing in the city centre, or workers with an immigrant background who, for historical reasons, live in more distant and/or under-served areas. Hence, systematic reliance on postal codes to reject or select applicants could result into indirect discrimination on the basis of *ethnicity* or *social origin* – two recognised discriminatory factors under EU law.¹⁴⁹³ Barocas and Selbst offer another similar example in the field of education, where an “*enormous weight*” is usually assigned “*to the reputation of the college or university from which an applicant has graduated*”.¹⁴⁹⁴ Giving particular importance to such a factor can however be criticised for two reasons: first, for its poor relevance for selecting job applicants, since any correlation between the name of a university and the quality of a candidate results from a coarse generalisation according to which top-university graduates make better ‘employee material’, and this, even if they were actually at the bottom of their class.¹⁴⁹⁵ Second, and more alarmingly, systematically granting weight to such an attribute may sustain or even participate to the growth of an existing form of indirect discrimination on the basis of the social background and/or ethnic origin of individuals, since young people from poorer families, minority groups, and/or whose parents never graduated from higher education¹⁴⁹⁶ usually encounter more difficulties to enter universities in the first place (especially universities whose tuition fees are very high).¹⁴⁹⁷ These two examples show that e-recruiting tools, and in particular the selection of the attributes on the basis of which an algorithm is going to select or reject candidates, should be carefully designed, taking into consideration both direct and indirect forms of potential discrimination.

¹⁴⁹² See, for example, Rahman, A. N., Yusoff, Z., Aziz, I. S. & Omar, D. (2014). Reducing Employee Travelling Time through Smart Commuting. *Earth and Environmental Science*, 18(2014)012074; Svanberg, K. (2014). Decreased Commuting Time and Its Effects on Accessibility and Productivity. Master’s Thesis in Economics. Uppsala University Library.

¹⁴⁹³ Article 21 of the Charter.

¹⁴⁹⁴ Barocas, S. & Selbst, A. D. (2016). *op. cit.*, p. 689, referring to Richtel, M. (2013, April 28). How Big Data Is Playing Recruiter for Specialized Workers. The New York Times. <http://www.nytimes.com/2013/04/28/technology/how-big-data-is-playing-recruiter-for-specialized-workers.html>.

¹⁴⁹⁵ Or, in the words of Barocas and &, “*such reputations may communicate very little about the applicant’s job-related skills and competencies*” (Ibid.).

¹⁴⁹⁶ On this topic, see, among others, Brooks, R. (2018). Understanding the higher education student in Europe: a comparative analysis. *Compare: A Journal of Comparative and International Education*, 48:4:500-517; Wolter, A. (2015). Massification and diversity: Has the expansion of higher education led to a changing composition of the student body? European and German experiences. In P. Zgaga, U. Teichler, & H. G. Schuetze (Eds.). *Higher education research and policy. Higher education reform. Looking back – looking forward*. Frankfurt: Peter Lang GmbH, pp. 149–171.

¹⁴⁹⁷ High tuition fees are characteristic of most universities in the US and in the UK. In the rest of the EU in comparison, tuition fees remain relatively low, but the cost of studying may become substantial when one takes into account costs of living, and in particular accommodation costs in bigger EU cities. The 2019 College Admission Scandal in the US has shown, once again, that privileged wealthy people could, through networking and financial tactics, secure a spot at a top university for their children through the so-called “back door” (donations) or “side door” (bribery) (see, for example, The College Admission Scandal: Complete coverage of a brazen cheating scheme, series of articles published by the New York Time, available at <https://www.nytimes.com/news-event/college-admissions-scandal>).

4.2.3.2. Discrimination stemming from the misuse of e-recruiting tools by recruiters

The above section has shown how algorithmic decision-making tool could create discriminatory outcomes because of inbuilt bias. Inbuilt bias, as their name indicate, are internal technical flaws resulting from human errors or negligence at the moment of the elaboration of the algorithm (e.g., use of biased training dataset, poor selection of relevant attributes, or flawed determination of the target variable). Even if the design and architecture of an algorithm would be close to perfect, however, or even if the output of a smart algorithm would be closely and continuously reviewed so as to correct any unintended effects, there is still an external risk of discrimination. This external risk relates to the misuse of the algorithmic tool by natural or legal persons in the context of recruitment. This risk of misuse includes (i) masking, (ii) over-reliance, or (iii) *ex-ante* discrimination.

(i) Masking: the intentional use of e-recruiting tools to discriminate

Masking relates to the use of e-recruiting tools to hide intentional forms of discrimination. In the case of *HireVue* interview software for example, beyond the actual design of the algorithm, it was also the manner in which it could be used by some companies which sparked criticism. Presumably, some US companies could indeed implement the video interview software into their recruitment process to reach mandatory 'diversity quotas' among the interviewees, without having the intention to invite individuals from minority groups for a second interview and/or to hire them. If that would be true, the e-recruiting tool would thus be misused in order to circumvent legal requirements or guidelines aiming at increasing diversity and equality in the recruitment process. E-recruiting tools can thus potentially serve the malicious purpose of masking intentional discrimination.¹⁴⁹⁸

(ii) Over-reliance: when humans stop questioning automated results

Another type of misuse could take the form of over-reliance on automation, in the sense that individuals who are part of a semi-automated decision-making process gradually stop questioning the accuracy of the machine and start to (almost) systematically validate the automated results provided to them. Hence, even in instances where an e-recruiting tool would not be meant to take a decision but rather to formulate a recommendation, the humans in charge could end up blindly following the given result, without questioning them. Over-reliance on ADM could thus lead humans to disregard relevant factors which, if taken into account, would have changed the final decision.

¹⁴⁹⁸ Corresponding to the 'masking' strategy described by Barocas and Selbst (2016), *op. cit.*

In the sector of mobility, automation over-reliance is exemplified when aircraft pilots overthrust their automatic flight control system or when drivers blindly following their GPS, leading them to commit an error or accident which could have otherwise been avoided.¹⁴⁹⁹ In the healthcare sector, automation over-reliance can lead doctors to prescribe wrong medicines or clinicians to override their own correct decisions in favour of an erroneous automated result.¹⁵⁰⁰ Similarly, in the recruitment sector, HR professionals could disregard the CVs of qualified candidates because of negligence or complacency induced by overreliance on e-recruiting tools.¹⁵⁰¹

(iii) Ex-ante discrimination: when an e-recruiting tool is only used on specific groups of individuals in a discriminatory fashion

Another type of misuse could be the occurrence of an *ex-ante* discrimination with respect to *when or for whom* an algorithmic decision-making tool is being used, or not. As an illustration, one may refer to the SyRI case in the Netherlands. With a view of combatting fraud, the Dutch government had been relying on an algorithmic decision-making tool since 2008, first referred to as ‘Black Box’ and then as SyRI following a 2014 legislative reform (SyRI stands for ‘system risk indication’).¹⁵⁰² SyRI was being used to combat fraud, including social benefits fraud, by profiling citizens on the basis of various criteria, including peripheral criteria such as low water usage. Despite objections from the Dutch DPA and the Council of State, SyRI was implemented by a number of Dutch authorities. Following an information request by the Platform *Bescherming Burgerrechten*, it was found that SyRI had been primarily used in low-income neighbourhoods,¹⁵⁰³ thereby putting a higher pressure on less privileged individuals,¹⁵⁰⁴ despite fraud taking place across all social classes.¹⁵⁰⁵ This type of targeted application of an algorithmic system to a group of individuals based on their social status can thus be assimilated to an *ex-ante* form of discrimination due to the manner in which the tool is used.¹⁵⁰⁶ In the end, a complaint was filed

¹⁴⁹⁹ Wu, J., Thorne-Large, J. & Zhang, P. (2021). Safety first: The risk of over-reliance on technology in navigation. *Journal of Transportation Safety & Security*, 1(28); Hansen, L. (2015, January 9). Eight drivers who blindly followed their GPS into disaster. *The Week*. <https://theweek.com/articles/464674/8-drivers-who-blindly-followed-gps-into-disaster>.

¹⁵⁰⁰ Goddard, K., Roudsari, A. & Wyatt, J.C. (2014). Automation bias: empirical results assessing influencing factors. *Int J Med Inform*, 83(5):368-375; Parasuraman, R., Molloy, R. & Singh, I. L. (1993). Performance consequences of automation-induced “complacency.” *Int J Aviat Psychol*, 3(1):1–23.

¹⁵⁰¹ Lacroux, A. & Martin-Lacroux, C. (2022, July 6). Should I Trust the Artificial Intelligence to Recruit? Recruiters' Perceptions and Behavior When Faced With Algorithm-Based Recommendation Systems During Resume Screening. *Front Psychol.*, 6(13):895-997.

¹⁵⁰² van Dalen, S., Gilder, A., Hooydonk, E. & Ponsen, M. (2016, March 31). System Risk Indication: An Assessment of the Dutch Anti-Fraud System in the Context of Data Protection and Profiling. *PILP*.

¹⁵⁰³ Vervloesen, K. (2020, April 6). How Dutch activists got an invasive fraud detection algorithm banned. *Algorithm Watch*. <https://algorithmwatch.org/en/syri-netherlands-algorithm/>.

¹⁵⁰⁴ *Ibid.*

¹⁵⁰⁵ White, R. & Van der Velden, J. (1995). Class and Criminality. *Social Justice*, 22(1):51-74, p. 59; Henman, P. & Martson, G. (2008). The Social Division of Welfare Surveillance. *Journal of Social Policy*, 37(2):187-205.

¹⁵⁰⁶ In the end, a complaint was filed against the Dutch government, and the use of SyRI was ultimately abandoned after the Dutch District Court of the Hague ruled that such data processing practice was violating the right to privacy. The Hague District Court, Case number C/09/550982, Judgment of 5 February 2020, ECLI:NL:RBDHA:2020:1878.

against the Dutch government, and the use of SyRI was ultimately abandoned after the Dutch District Court of the Hague ruled that such data processing practice was violating the right to privacy.¹⁵⁰⁷ The same issue could arise in the field of e-recruitment. One could imagine, for example, a recruiter who would only require candidates above 50 to pass an online cognitive test, because the company would wrongly assume that people below 50 have less cognitive issues, thereby putting a higher pressure on older candidates.

In all the above-mentioned cases, the discriminatory output does not derive from an internal flaw in the algorithm itself but rather from the *manner in which it is used*. Hence, even when an e-recruiting tool has been carefully elaborated so as to mitigate any unintended effects, discrimination could still occur because of the unlawful, malign or negligent use of such tool by its users.

4.2.4. The scope of discrimination when using e-recruiting tools: focus on several phenomena that can exacerbate discriminatory outcomes

Besides their respective sources, the second main difference between algorithmic and human discrimination concerns their scope. E-recruiting tools may indeed drastically extend the scope of discrimination because of some characteristic phenomena pertaining to their use. These phenomena may be categorised as follows: (1) systematisation; (2) escalation; (3) dissimulation; and (4) feedback loops.

Unlike humans who may be inconstant in their decisions, change their mind, or unlearn some taught bias through conscientisation or interactions with other humans, algorithmic tools are mathematical formula which repeat the same model in a systematic fashion, and cannot change or evolve, unless specifically programmed to do so.¹⁵⁰⁸ A risk associated with the use of algorithmic-decision making is therefore the *systematisation* of discrimination. As an example, one may think of a female human recruiter who tends to hire ‘*mini-mes*’ (for example introvert, book-smart girls wearing glasses), to the detriment of extravert individuals, or male candidates. Although this tendency is real, it is unlikely to be systematic. Several times, this recruiter may indeed favour other factors and hire someone who does not resemble her at all. Furthermore, over time, this recruiter may become conscious of her own bias, and actively decide to fight it. By contrast, an algorithm will continue to apply the model that it was programmed to apply, in a systematic and continuous fashion. This issue may be referred to as **systematisation**.

¹⁵⁰⁷ The Hague District Court, Case number C/09/550982, Judgment of 5 February 2020, ECLI:NL:RBDHA:2020:1878.

¹⁵⁰⁸ One may refer, for example, to self-learning algorithm, although it may also be argued that self-learning algorithm are limited in their learning capabilities as well, depending on how they were initially programmed, as well as the input data that are fed to them.

Furthermore, unlike humans, e-recruiting tools may be infinitely duplicated, sold to different organisations, and simultaneously used on thousands of candidates, on a global scale. For example, the interview software developed by HireVue, Inc. has been adopted by groups of companies such as Unilever, KRAFT, DOW JONES, Randstad or Sodexo, to only name a few.¹⁵⁰⁹ On 23 March 2021, HireVue, Inc. even announced that it had completed “*its 20 millionth virtual interview*”.¹⁵¹⁰ Of course, if one assumes that HireVue interview software enables to efficiently and fairly assess the skills and competences of candidates, then one may argue that this e-recruiting tool has probably prevented many cases of human discrimination. For the same reason however, even a small unnoticed technical flaw in that software could grow into a worldwide source of discrimination for certain groups of individuals. In other words, the wider the application of one single e-recruiting tool is, the greater the scale of its effects becomes, including potential discriminatory effects. To further illustrate this, one may compare the biased decision of a human recruiter to only contact male candidates for a managerial position (i.e., one discriminatory behaviour relating to *one* job opportunity), to a search algorithm used on several recruiting platforms which systematically favours men over women for managerial positions because of an in-built bias (i.e., one flaw relating to *thousands* of jobs opportunities).¹⁵¹¹ This phenomenon which is characteristic of the use of e-recruiting tools can be referred to as **escalation**. Escalation is also one of the reasons why extra attention should be paid to the elaboration of such tools in the first place.

Third, discrimination stemming from the use of e-recruiting tools can also be enhanced due to the level of stealth of algorithmic decision-making. The automated decision to include or exclude individuals from the recruitment process (whether at the stage of promotion, pre-selection or selection) can indeed remain completely hidden from the public and even sometimes from the individuals who have been subject to such a decision. Before the advent of online recruitment, if a company, a university or another organisation wanted to hire new recruits, it mainly relied on public medium of promotion to do so, such as newspapers, specialised magazines or pamphlets.¹⁵¹² The ‘market of opportunities’¹⁵¹³ was thus relatively open or at least visible. Today, however, the situation has drastically changed, as recruiters increasingly rely on technical solutions and online strategies to fill in open positions.¹⁵¹⁴ Those online strategies may include the use of search & match algorithms or targeted job advertisement. Both types of tools are available on social media platforms such as LinkedIn or Facebook. The main issue with these tools is that they can lead to the intentional or accidental *upstream* exclusion of individuals, without the latter being even aware of it. Hence, the market of opportunities in the

¹⁵⁰⁹ Information available on www.hirevue.com on 15 April 2020.

¹⁵¹⁰ HireVue Press release, HireVue Completes its 20 Millionth Video Interview, available at <https://www.hirevue.com/press-release/hirevue-completes-its-20-millionth-video-interview>.

¹⁵¹¹ Datta, A. & al. (2015), *op. cit.*

¹⁵¹² Kim, P. T. (2020). Manipulating opportunity. *Virginia Law Review*, 106(4):867-875, p. 871.

¹⁵¹³ Following the expression used by Kim, P. T. (2020), *op. cit.*

¹⁵¹⁴ Caers, R. & Castelyns, V. (2011). LinkedIn and Facebook in Belgium: The Influences and Biases of Social Network Sites in Recruitment and Selection Procedures. *Social Science Computer Review*, 29:437-448.

field of recruitment may suffer from a new type of discrimination by stealth. In the study on Google advertising algorithm mentioned above, for example, one of the experiments conducted by the researchers showed that Google displayed advertising for a career coaching service for “\$200k+” executive jobs 1,852 times to the male group and only 318 times to the female group. Women whose profile had been excluded by Google algorithm remained of course unaware of that fact. It is highly probable that Google did not intend for its algorithm to be gender biased and was not aware of this flaw at that time. In other cases, however, recruiters could willingly discriminate on individuals, for example by setting the parameters of their research so as to discreetly exclude some individuals on the basis of gender, religion, ethnicity or handicap. The risk that recruiters, and more generally advertisers, could discriminate through the use of algorithmic decision-making became particularly apparent in October 2016, when ProPublica reported that Facebook allowed advertisers, including employers or landlords, to exclude individuals from their targeted adverts on the basis of ethnicity, handicap, age or other discriminatory criteria.¹⁵¹⁵ Facebook tried to defend itself by arguing that its tool was by nature neutral and that it could not be held accountable for its misuse by others.¹⁵¹⁶ Regardless of the question relating to the level of accountability of platform or advertisers, it must be acknowledged that the level of stealth offered by some e-recruiting tools can enable or even encourage recruiters to more frequently discriminate on candidates, knowing that the victims of such discrimination will not be able to notice it, contest it or report it. This characteristic which is specific to some algorithmic decision-making tools, and which is likely to enhance risks of discrimination, can be referred to as ‘**stealth**’ or ‘**dissimulation**’.

Another risk with respect to the enhancement of discriminatory outcomes through the use of algorithmic tools relate to so-called ‘**feedback loops**’. Feedback loops are the result of a statistical aggravation which may first reflect and then enhance overtime pre-existing human bias in any decision-making process.¹⁵¹⁷ For a feedback loop to emerge, a specific feature is initially given a reasonable weight within a predictive model to seek out a target variable (for example, ‘age group 45-55’ appears to make ‘punctual and reliable employees’). The predictive models can then be applied to real-life cases. The smart algorithm can then improve its predictive model with new data from recent experiences. If, within the data which is fed back to the algorithm, the given feature keeps on correlating with the sought target (for example, the newly hired employees between 45 and 55 are more punctual and reliable than other age groups), the algorithm is likely to enhance the importance of that specific feature. This phenomenon may continue in an exponential fashion which can ultimately create a dissonance between the predictive model and reality.

¹⁵¹⁵ Angwin J. & Parris T. (2016, October 28). Facebook Lets Advertisers Exclude Users by Race. *ProPublica*. <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>.

¹⁵¹⁶ See, e.g., Defendant’s Notice of Motion and Motion To Dismiss First Amended Complaint, *Onuoha*, 2017 BL 115835.

¹⁵¹⁷ Perry, W. L. & al. (2013). Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf

To illustrate this phenomenon, one may refer to a well-known example of feedback loops in the field of predictive policing or e-policing. In the US, several police departments in large cities have been experimenting predictive policing tools with a view to forecast and prevent criminal activity.¹⁵¹⁸ At the outset, an algorithm is programmed to find correlations between the frequency of an offence or crime (e.g., drug dealing) and specific neighbourhoods on the basis of large sets of data, including historical crime data. A predictive model is thereby created. In accordance with the recommendations made by the algorithm, police forces are then deployed in specific neighbourhoods at specific time of the day where an offence or crime is likely to occur, in order to prevent it and/or apprehend the offender. Quite logically, because of their accrued presence in certain neighbourhoods, the police forces are likely to register more offences or crimes in those particular places than elsewhere. And once these data are fed back to the algorithm, the latter will thus recommend more and more interventions in those neighbourhoods, where an increasing number of offences or crimes will be detected, thereby creating a feedback loop.¹⁵¹⁹ Feedback loops can either be considered as the result of an inbuilt flaw in the algorithmic tool, which has not been programmed to be critical about the data generated through its own predictive model, or it can be the result of a wrongful use of the algorithmic tool by its users. In the case of SyRI, for example, a feedback loop may have as well resulted from the decision of the Dutch authorities to almost always apply SyRI to poorer neighbourhoods, rather than equally using it in poor or wealthy neighbourhoods. As simply explained by Koen Vervloesem from the non-profit organization AlgorithmWatch, “*if the government only uses SyRI’s risk analysis in neighbourhoods that are already deemed high-risk, it is no wonder that it will find more high-risk citizens there*”.¹⁵²⁰ Depending on the perspective and course of actions, feedback loops may thus either be fuelled by a technical flaw in the algorithm itself (i.e., in-built bias), by its repetitive wrongful application by the users, or – potentially – by a combination of both.

Drawing from these considerations, it appears more clearly that human discrimination must be distinguished from algorithmic discrimination, given that both their sources and the scope of their effects are not identical. Those differences need to be kept in mind when aiming at tackling unfair treatment arising from the use of e-recruiting tools. In this perspective, the below section will provide a brief overview of existing instruments of soft and hard law whose object is to tackle discrimination. More specifically, light will be shed on the fact that some of these laws may be ill-fitted to address the modern challenges of algorithmic discrimination. In the following section, the author of this study will then assess

¹⁵¹⁸ *Ibid.*

¹⁵¹⁹ See also Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York University Press; Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, 4(10):1572-1593.

¹⁵²⁰ *Ibid.*

whether the GDPR could be used as a functional tool to ensure the responsible development and use of e-recruiting tools.

4.2.5. The regulation of e-recruitment practices in the EU through soft and binding law: a brief overview

The above section has revealed the main risks pertaining to the use of e-recruiting tools with respect to the fundamental rights and freedoms of individuals, and in particular non-discrimination. Despite the existence of these risks, and as long as algorithmic decision-making tools will outperform humans in terms of efficiency and accuracy, their use seems inevitable. Besides, considering the fact that human recruiters are prompt to discriminate or suffer from unconscious bias, the use of such e-recruiting tools may also be advisable, in the sense that it may prevent or decrease discriminatory outcomes. E-recruitment can thus be considered as a double-edged sword when it comes to protecting fairness and equality. On the one hand indeed, it cannot be denied that algorithmic decision-making tools have the potential to bring more fairness and prevent discriminatory outcomes in the field of recruitment – a field which has traditionally been plagued by human bias and discrimination.¹⁵²¹ On the other hand, it is essential to ensure that such tools remain allies and do not turn into Trojan horses, as it has already been the case. These two considerations should remain the cornerstone on the basis of which any (further) regulation in the field of e-recruitment should be thought. In particular, it seems important for such regulation to be able to accompany and frame the development of algorithmic decision-making tools for preventing any forms of discrimination, without nonetheless disproportionality hampering such development by establishing overly burdening rules.¹⁵²²

In Europe, many soft law instruments, including studies and guidelines, were published in this respect.¹⁵²³ One of the reference documents in the EU is currently the *Ethics Guidelines for Trustworthy AI* published by the European Commission's High Level Expert Group on Artificial Intelligence in April 2019.¹⁵²⁴ It advocates for a human-centric approach to AI which rests on seven key ethical requirements. These EU Guidelines further envisage the possibility to translate some of these ethical requirements into hard law, either by adopting new laws or amending existing

¹⁵²¹ Zuiderveen Borgesius, F. J. (2020). *op. cit.*, p. 1575.

¹⁵²² This is at least what an utilitarian or liberal-egalitarian approach would command to do, keeping in mind the objective to reduce the occurrence of unfair discrimination by humans as well.

¹⁵²³ In Europe, the Council of Europe, as well as each of the EU institutions involved in the legislative process have published their own study/guidelines. At the Member States level, data protection authorities or agencies have also participated to the debates. See, among the most recent examples: Council of Europe (2017). *op. cit.*; Madiega, T. (2019, September). *EU Guidelines on Ethics in Artificial Intelligence: context and implementation*. European Parliament, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI\(2019\)640163_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf); European Commission's High Level Expert Group on Artificial Intelligence (2019, April 8). *op. cit.*; CNIL (2017, December). *op. cit.*; Gutenachten der Datenethikkommission (October 2019) https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf.

¹⁵²⁴ The different language versions of these Guidelines are available at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

ones.¹⁵²⁵ In parallel, these Guidelines recognise that “*regulation to support AI’s trustworthiness already exists today*”, and explicitly mention product safety legislation, liability regimes, EU consumer protection regulations as well as the GDPR.¹⁵²⁶

Rather than analysing in depth the scope and content of all existing or future EU or Member States legislation aiming at tackling discrimination in the field of recruitment, this section will draw a general overview of the existing or proposed norms. Indeed, painting a detailed picture of the legislative landscape meant to tackle discrimination would fall far beyond the scope of this study. The below analysis is thus in no way meant to be comprehensive. Rather, it focuses on the main gaps and weaknesses of anti-discrimination legislation, as already identified by institutional actors or scholars, when it comes to regulating ADM, and e-recruitment in particular. This will in turn enable the author to show how using the functional nature of the GDPR could potentially fill these gaps or correct these flaws.

4.2.5.1. Self-regulation and soft law in the form of ethical standards for the development of e-recruiting tools

As expected, most of the companies active in the development and licensing of e-recruiting tools, such as HireVue and its competitors, claim to (regularly) review, audit and improve those tools in order to correct or prevent any inbuilt bias.¹⁵²⁷ These endeavours can in some instances be considered as self-regulatory efforts, similar to the one that all major internet operators such as Facebook or YouTube are deploying to prevent the proliferation of illegal or harmful behaviours on their platforms (see Section 4.1.3.1, above). It is also interesting to note in this respect that most of these companies are often praising the virtues of their e-recruiting tools by arguing *inter alia* that their application, beyond being both secure and legal, is also more *ethical* for the persons concerned. In line with the school of thoughts on the ethical aspects of AI, many authorities have also adopted soft law instruments designed to provide an ethical framework for the development and use of AI tools. One may refer, for example, to the OECD Recommendation on AI, to the Council of Europe Draft Recommendation on the Human Rights Impacts of Algorithmic Systems, or to the European Commission’s Ethics Guidelines on Trustworthy AI. When analysing the content of such soft law instrument, as well as the overlying

¹⁵²⁵ Ursula von der Leyden, President-elect of the European Commission, announced : “*In my first 100 days in office, I will put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence*”. Source: *Political Guidelines for the next Commission 2019 – 2024. A Union that Strives for More, My Agenda for the EU* (April 2019). https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

¹⁵²⁶ European Commission’s High Level Expert Group on Artificial Intelligence (2019, April 8). *op. cit.*, pp. 12, 16 and 17.

¹⁵²⁷ All the above-mentioned companies were indeed making these claims on their website at the time the author was researching on this topic. See also, Yeung, K., Howes A. & Pogrebna, G. (2019). Why Industry Self-regulation Will Not Deliver 'Ethical AI': A Call for Legally Mandated Techniques of 'Human Rights by Design'. Dubber and Pasquale (eds.). *The Oxford Handbook of AI Ethics*. Oxford University Press.

narrative accompanying self-regulatory efforts, it appears however that both private and public actors are sometimes resorting to a practice called ‘ethics washing’.

Ethics washing is an expression according to which the respect of ethical standards is presented as a substitute for regulation, or even, in some instances, a marketing argument.¹⁵²⁸ Ethics washing thus often emerges as a practice for compensating both the existence of public concerns and the simultaneous absence of legally binding rules. As far as e-recruiting tools are concerned, it can have the perverse effect of bringing more trust in the mind of the users or data subjects with respect to the fairness of these tools, while nothing guarantees that the allegations made by the companies concerned are true. On the website of Mya Systems Inc., for example, Ameya Deshmukh – presented as a member of the *Bias and Diversity* team of the company, explains: “At Mya, we tackled this problem [of algorithmic bias] early on by creating a strategy we call “Conversation Design”. For several years we’ve maintained a team of professional linguists and conversation reviewers. They are our Conversation Design Team and they prevent unconscious bias from impacting our AI’s questions, interpretations, and responses.”¹⁵²⁹ When looking for the composition or activities of this ‘Conversational Design Team’ however, no further information can be found on the website of the company. A quick search on LinkedIn further reveals that Mr. Deshmukh is actually not an expert in human resources or ethics, Inc. but a marketing graduate specialised in story-telling who was temporarily hired by the company between January and September 2020 as a Senior Content and Marketing Strategist.¹⁵³⁰ This example of ‘ethics washing’ shows that the desire of companies to brand their AI-products as ‘ethical’ may sometimes prevail over their desire to ensure the respect of ethical standards through concrete measures. Hence, ethical standards are to be considered with a certain degree of caution when it comes to their ability to ensure the respect of data subjects’ fundamental rights and freedoms. This does not mean, however, that soft law instruments or self-regulatory standards are worthless.

On the one hand indeed, self-regulation and soft law instruments appear desirable when their aim is to prevent harmful effects emanating from the use of new DDTs, including, for example, discriminatory outcomes through the use of e-recruiting tools. As explained by Zuiderveen Borgesius, “[i]t can hardly be denied that ethical AI is preferable over unethical AI. Self-regulation could help mitigate discrimination, and

¹⁵²⁸ Ethical AI can be seen as a marketing narrative. The use of such techniques is however not limited to the private sector. The European Commission has recently also been criticized for publishing its Ethical Guidelines on trustworthy AI. As argued by Thomas Metzinger, Professor of Theoretical Philosophy at the University of Mainz: “The underlying guiding idea of a “trustworthy AI” is, first and foremost, conceptual nonsense. Machines are not trustworthy; only humans can be trustworthy (or untrustworthy).” Source: <https://background.tagesspiegel.de/ethik-waschmaschinen-made-in-europe>.

¹⁵²⁹ Deshmukh, A. (2019, December 8). Is It Possible to Prevent Unintentional Bias in AI? Last updated on July 31, 2020. Mya blogonline publication. Source: <https://www.mya.com/blog/possible-prevent-unintentional-bias-in-ai/>

¹⁵³⁰ The LinkedIn profile of Mr. Ameya Deshmukh shows that he graduated in 2015 from San Jose University with a bachelor in Marketing and has since then worked for various companies as a marketing manager. Source: <https://www.linkedin.com/in/ameyadeshmukh10/>.

*could provide inspiration for legislators.”*¹⁵³¹ Furthermore, self-regulation and soft law instrument present many advantages for framing the development of fast-evolving DDTs, including, for example, the speediness with which they may be adopted (i.e., no lengthy legislative process), their adequacy or fitness (i.e., each company or authority may adjust those efforts or standards, taking into account risks that are specific to their sector/application) as well as their flexibility (i.e., they can quickly evolve along with further technological development and the emergence of new or unforeseen risks). On the other hand, claiming that self-regulation and soft law alone will suffice at preventing avoidable pitfalls and human rights violations would be naive. Among the weaknesses of soft law and self-regulation, one may cite the following three issues in particular: (i) such norms are non-binding, which typically leads to a total absence or at least a lack of enforcement when a real issue arises;¹⁵³² (ii) such norms are often vague, broadly worded and quite abstract, which makes them likely to be misinterpreted or distorted, usually so that their meaning fit the vision or objective of the person who abide to them or is invoking them;¹⁵³³ (iii) such norms may be interpreted as a compromise and ultimately delay the adoption of necessary binding rules.¹⁵³⁴

In view of these three weaknesses, self-regulation and ethical discourse – even if they may be desirable – will not be sufficient to protect the fundamental rights and freedoms of individuals against poorly elaborated or misused algorithmic tools. Hard law is needed. The below section will precisely aim at giving an overview of the existing laws that may be invoked to protect individuals against interferences with their right not to be discriminated in the context of e-recruitment.

4.2.5.2. EU anti-discrimination laws against discriminatory practices in the field of recruitment

EU primary and secondary law contains many norms aimed at combatting discrimination. Within EU primary law, non-discrimination is enshrined in Article 21 of the Charter, which is worded as follows:

*1. Any discrimination based on any ground such as **sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.***

2. Within the scope of application of the Treaty establishing the European [Union] and of the Treaty on European Union, and without prejudice to the

¹⁵³¹ Zuiderveen Borgesius, F. J. (2020), *op. cit.*, p. 1582.

¹⁵³² Gutierrez, C. I., Marchant, G. & Tournaso, L. (2020). Lessons for artificial intelligence from historical uses of soft law governance. *Jurimetrics Journal of Law, Science and Technology* 61(1):133.

¹⁵³³ As exemplified by the statements published on the websites of many companies in the field of e-recruitment, where they each argue to abide to ethical standards, although defined and implemented differently.

¹⁵³⁴ Zuiderveen Borgesius, F. J. (2020), *op. cit.*, p. 1582.

*special provisions of those Treaties, any discrimination on grounds of **nationality** shall be prohibited.*

The right to non-discrimination is further embedded in Article 10, as well as 18 and 19 of the TFEU, which respectively prohibit discrimination on grounds of nationality, and allow the EU to take appropriate action to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. On the basis of these competences, various EU legislative acts have been adopted to combat specific forms of discrimination. Today, one may refer, in particular, to the following instruments of EU secondary law:

- The Racial Equality Directive (Directive 2000/43/EC)¹⁵³⁵ – which prohibits discrimination on the grounds of **racial or ethnic origin** in the field of *employment or occupation* (both with respect to access and working conditions, vocational training, workers, employers or professionals' organisations), but also *social protection or advantages, education, and access goods and services available to the public*, such as housing;
- The Employment Equality Directive (Directive 2000/78/EC)¹⁵³⁶ – which prohibits discrimination on the grounds of **religion or belief, disability, age or sexual orientation** in the field of *employment or occupation*;
- The Equal Treatment of Men and Women Directive (Recast) (Directive 2006/54/EC)¹⁵³⁷ – which aims at preventing discrimination based on **gender** in the field of **employment or occupation** (including access, working conditions, and occupational social security schemes) ; and finally
- The Council Framework Decision of 2008 against racism and xenophobia¹⁵³⁸ – which aims at ensuring that **racist and xenophobic conducts** are sanctioned in all Member States by a minimum level of effective, proportionate and dissuasive criminal penalties.

The below section will briefly highlight the main weaknesses of each of these instruments when it comes to ensuring that e-recruiting tools do not produce discriminatory outcomes, starting with the Council Framework Decision.

¹⁵³⁵ Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

¹⁵³⁶ Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

¹⁵³⁷ Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), *OJ L 204, 26.7.2006, p. 23–36*.

¹⁵³⁸ Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, *OJ L 328, 6.12.2008, p. 55–58*.

(i) The limited scope of the Council Framework Decision of 2008 against racism and xenophobia

The Council Framework Decision of 2008 against racism and xenophobia was adopted mainly with a view to ensure that all Member States within the EU had the necessary legal arsenal to combat and punish certain forms and expressions of racism and xenophobia under criminal law, such as racist hate speech or denialism,¹⁵³⁹ or any other offence with underlying racist and xenophobic motivation.¹⁵⁴⁰ E-recruiting tools conceived with a view to exclude a group of individuals on the basis of racial or xenophobic motivation would thus fall within the scope of that Decision, including in instances where such tools have been elaborated and/or implemented by a *legal* person.¹⁵⁴¹

Beyond its broad personal scope, another positive aspect of this Decision is that Member States must ensure that investigations into or prosecution of such offences are not dependent on a report or an accusation made by a victim. A human right association, or a non-governmental organisation involved into algorithmic fairness or transparency – such as AlgorithmWatch in the EU,¹⁵⁴² could thus submit a complaint. A major limitation of this Framework Decision resides however in the fact that its scope is restricted to *intentional* harmful conducts. Article 4 of that Decision provides in particular: “(...) *Member States shall take the necessary measures to ensure that racist and xenophobic motivation is considered an aggravating circumstance, or, alternatively that such motivation may be taken into consideration by the courts in the determination of the penalties.*”

In the context of e-recruitment, the Council Framework Decision of 2008 would therefore only become relevant in cases where (i) an algorithmic tool is *intentionally* used for the purpose of discriminating candidates on the basis of *racial* or *ethnic* attributes, or (ii) where the user of an e-recruiting tool becomes aware of an unforeseen discriminatory outcome which puts certain racial or ethnic groups at a disadvantage, but *intentionally* decide to ignore this on the basis of *racist* or *xenophobic motivation*.¹⁵⁴³ In both cases, however, there must be a malicious

¹⁵³⁹ See Article 1 and 2 of the Council Framework Decision of 2008 against racism and xenophobia. The material scope of the Decision is principally focused on the following *intentional* conducts: “*publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin*” or “*publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes (...)*”. According to Article 3 of the same Decision, such offences must be punishable by “*effective, proportionate and dissuasive criminal penalties.*”

¹⁵⁴⁰ See Article 4 of the Council Framework Decision of 2008.

¹⁵⁴¹ Both natural and legal persons are concerned by this Framework Decision. In particular, Article 5(1) of the Council Framework Decision of 2008 against racism and xenophobia provides: “*Each Member State shall take the necessary measures to ensure that a legal person can be held liable for the conduct referred to in Articles 1 and 2, committed for its benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person (...)*”.

¹⁵⁴² According to a statement on their website, **AlgorithmWatch is a non-profit research and advocacy organization committed to evaluating and shedding light on algorithmic decision-making processes used either to predict or prescribe human action or to make decisions automatically.** Source: <https://algorithmwatch.org/en/about-en-alt/>

¹⁵⁴³ Article 4 of Council Framework Decision of 2008 against racism and xenophobia.

intention on the part of the user of the e-recruiting tool, and such intention must be established. On the one hand, it can be argued that malicious intention when using e-recruiting tools is likely to become apparent through the selection of discriminatory 'attributes' or 'characteristics' by the users, which can often not be hidden because of lack of ownership or control over these tools. As an example, when landlords or housing companies started using Facebook advertising system in a discriminatory manner, for example by excluding from the targeted public individuals whose Facebook profile included discriminatory attributes such as 'African-American', such behaviours became apparent precisely because these characteristics *had* been selected. In particular, the *possibility* to discriminate was visible to anyone using that tool and the manner in which landlords or housing companies were discriminating could be established on the basis of Facebook entry logs. On the other hand, the malicious use of e-recruiting tool may also remain completely hidden if the recruiter has total control over the tool and no obligation of disclosure in this respect. In that case, an e-recruiting tool could be maliciously used to discriminate on the basis of racist or xenophobic motivation, while potentially masking those racist or xenophobic intentions under the objective appearance of algorithmic decision-making system. In the EU however, the instrumentalization of e-recruiting tools for the purpose of intentionally discriminating individuals is not a very plausible scenario given that transparency rules exist under EU data protection law. Instead, as discussed above, the main risks pertaining to e-recruitment is the occurrence of *accidental* (indirect) forms of discrimination, for example because of the poor quality of the original dataset or the existence of proxies within the algorithmic model.¹⁵⁴⁴ Keeping this in mind, the relevance of the Council Framework Decision of 2008 is thus likely to remain peripheral in the context of e-recruiting practices. Yet, this Decision may still have the overall beneficial impact of prompting Member States to adopt more stringent sanctions against discriminatory behaviours in general, including non-intentional (indirect) forms of discrimination.

(ii) The fragmented transposition of the EU directives combatting discrimination

By contrast to the Council Framework Decision of 2008, the three above-listed directives combatting discrimination do not focus on *intentional* behaviours. Rather, they focus on the existence of a discriminatory outcome, regardless of whether such discrimination would be direct or indirect, whether it would be human, institutional or machine-based, or whether it would be intentional or accidental. This is of course very important in the context of e-recruitment practices, since *accidental* forms of *indirect* discrimination (for example, through proxies) are more likely to occur than intentional forms of direct discrimination. Furthermore, these directives have a broader material scope in the sense that they cover more forms of discrimination. Taken together indeed, these directives cover (1) discrimination on the grounds of

¹⁵⁴⁴ Council of Europe (2018). *op. cit.*, p. 19.

racial or ethnic origin in the field of *education, employment or occupation, social protection or advantages* as well as *provision of goods and services*; and (2) discrimination on the grounds of **gender, religion/belief, disability, age or sexual orientation** in the field of *employment or occupation*. Those directives could thus effectively apply in situations where the use of e-recruiting tools leads to unforeseen forms of indirect discrimination against women, individuals with a handicap, elderly people, or members of a specific ethnic group. Similarly, the Racial Equality Directive could apply to unforeseen forms of indirect discrimination on grounds of racial or ethnic origin in the field of healthcare, insurance or housing (i.e., ‘services available to the public’), arising from the use of e-health, e-insurance or e-housing tools.

Another advantage of these directives is that they have adapted and harmonised across the EU the applicable rules relating to burden of proof in a way that is favourable for victims of discrimination, in accordance with the case-law of the CJEU in that field. According to these rules indeed, where evidence of a *prima facie* case of discrimination is brought by the claimant, the burden of proof is shift back to the respondent who is given the responsibility to demonstrate that, contrary to the established presumption of discrimination, the principle of equal treatment has been respected.¹⁵⁴⁵ One may imagine, for example, that, over a two-years period, the input data fed to a screening algorithm would show that an almost equal numbers of men and women having similar competences have applied for managerial positions, while the output data would show that 75% of the candidates selected by the algorithms for an interview were men. This could constitute a *prima facie* case of gender-based discrimination that is contrary to the Equal Treatment of Men and Women Directive. It would then be for the employer to prove that the e-recruiting tool in question is not discriminating against women. Because of those protective rules, e-recruiting tools elaborated on the basis of strong transparency requirements could thus (if anything) *reduce* the amount of unperceivable and thus unreported cases of discrimination and simultaneously *increase* the level of accountability of employers with respect to equal treatment.¹⁵⁴⁶

Although EU anti-discrimination law could become instrumental in the fight against discrimination arising from the use of e-recruiting tools, an analysis of the implementation of such legislation into national law, as well as its enforcement at the national level, have revealed several weaknesses, as explained below.

First of all, it must be noted that the above-mentioned anti-discrimination legislation only prohibits discrimination on the basis of specific grounds, also called protected characteristics. These grounds can be summarised as follows: (1) gender (*limited however to the binary distinction between male or female*); (2) racial or ethnic origin;

¹⁵⁴⁵ Article 8 of the Racial Equality Directive ; Article 10 of the Employment Equality Directive; Article 19 of the Equal Treatment of Men and Women Directive.

¹⁵⁴⁶ Rai, A. (2020). Explainable AI: from black box to glass box. *Journal of the Academy of Marketing Science* volume, 48:137–141.

(2) religion or belief, (3) disability, (4) age or (5) sexual orientation. Although some Member States have included other protected characteristics under their national anti-discrimination law,¹⁵⁴⁷ most legislation only focus on these primary characteristics.¹⁵⁴⁸ Hence, anti-discrimination laws often leave important gaps.¹⁵⁴⁹ As an illustration, an interview video software similar to the one developed by HireVue, Inc. could favour candidates who are thin over candidates who are fat, without such a data being considered as a protected characteristic under the applicable anti-discrimination law.

Second, despite the fact that the above-mentioned directives formally prohibit *indirect* discrimination, the definition set by EU law in this respect does not set any clear or easily applicable rules.¹⁵⁵⁰ For example, Article 2(2)(b) of the Racial Equality Directive provides for the following typical definition:

“Indirect discrimination shall be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary (...)” (emphasis added).

The notion of ‘practical disadvantage’ is often considered as relatively vague. For example, it may be unclear for a court to determine whether being excluded from seeing a job advert on a social media platform consists into a ‘particular disadvantage’ or not. More generally, it is unclear whether the loss of an opportunity could translate into the loss of a ‘practical advantage’. If not, EU anti-discrimination law would not apply to cases where categories of individuals are excluded at the stage of promotion or pre-selection because of a protected characteristic. On top of that, the disadvantage suffered by the discriminated group must be established in comparison to the treatment reserved for other groups. For this purpose, sound statistical evidence is usually required.¹⁵⁵¹ The CJEU has ruled in particular that the statistics on which indirect discrimination is based must be valid. This is understood as meaning that these statistics must cover enough individuals, must not illustrate purely fortuitous or short-term phenomena, and appear, in general, to be

¹⁵⁴⁷ For example, Belgian law also prohibits discrimination in the grounds of civil status, birth, wealth, political conviction, trade union membership or conviction, language, current or future health condition, a physical or genetic characteristic or social origin (see Article 4, 4° of the Loi du 10 Mai 2007 tendant à lutter contre certaines formes de discrimination, 30-05-2007).

¹⁵⁴⁸ The Luxembourg law transposing the anti-discrimination for example, does not provide for any additional protected characteristics (see Loi du 28 Novembre 2006 portant sur transposition de la directive 2000/43/CE (...), Memorial A, N° 207).

¹⁵⁴⁹ Council of Europe (2018). *op. cit.*, p. 20.

¹⁵⁵⁰ *Ibid.*, referring to Sunstein, C. R. (1995). Problems with Rules. *California Law Review*, 83(953); Baldwin, R., Cave, M. & Lodge, M. (2011). *Understanding Regulation: Theory, Strategy, and Practice*. Oxford Academic.

¹⁵⁵¹ Council of Europe (2018), *op. cit.*, p. 20.

significant.¹⁵⁵² Meeting this threshold of evidence can be difficult as it would require access to a significant amount of output data generated by the e-recruiting tool. Usually, however, only the recruiters have access to this output data.

Third, although the applicable rules on burden of proof enable victims to bring a claim based on a *prima facie* case of discrimination, bringing such *prima facie* evidence can still be difficult. This is the case whether e-recruiting tools are used or not, although some evidence may even be harder to obtain when e-recruiting practices are at stake. Among obstacles that are common to all types of discrimination, the most common is that offenders will usually attempt to deny or hide their discriminatory behaviour. Another common obstacle is the fact that victims do not have a general overview of the situation and may thus be unaware that candidates having a similar characteristic have systematically been rejected in the past. For example, if a recruiter turns down five candidates on the basis their skin colour while formally giving them another reason, it will be difficult for each victim to realise – and even harder to prove – that such a rejection was motivated by a racial prejudice. Similarly, if a video interview software is flawed and tends to give to female candidates a poorer employability score than to male candidates, such flaw is not perceptible for each female candidate individually, since the discrimination is taking place “*screen by screen*”.¹⁵⁵³ This lack of overview and/or access to the output data is therefore an obstacle which makes it difficult to detect the existence of accidental or intentional discrimination, and thus to bring evidence of a *prima facie* case of discrimination. Furthermore, among obstacles that are specific to e-recruiting tools, one must refer to the fact that algorithmic decision-making can exclude categories of individuals without them being aware that they were even part of a decision-making process. In particular, the fact that some profiles can be rejected by a pre-selection algorithm without the individuals concerned even being aware of it make it impossible for them to question or contest such a decision.¹⁵⁵⁴ Yet, many e-recruiting tools used at the stage of promotion and pre-selection, such as LinkedIn Recruiter¹⁵⁵⁵ as well as Facebook or Google advertising system, operate on this basis. This issue directly relates to the stealth or dissimulation phenomenon discussed above, which is characteristic of most e-recruiting tools.

Finally, it must be noted that according to a third report from the Commission, the general implementation of these directives at the national level still suffers from

¹⁵⁵² See Case C-127/92 *Enderby v Frenchay Health Authority and Secretary of State for Health* [1993] ECR I-5535 and Case C-226/98 *Jørgensen v Foreningen af Speciallæger and Sygesikringens Forhandlingsudvalg* [2000] ECR I-2447.

¹⁵⁵³ Zeynep Tufekci in the 2020 documentary ‘Coded biases’, directed by Shalini Kantayya.

¹⁵⁵⁴ Larson & al. (2017, December 19). These Are the Job Ads You Can’t See on Facebook If You’re Older. *The New York Times*. <https://projects.propublica.org/graphics/facebook-job-ads>.

¹⁵⁵⁵ LinkedIn Recruiter is the name given by LinkedIn Ireland Unlimited Company to its main e-recruiting tool; a search and match algorithm aimed at finding candidates corresponding to the profile sought by a recruiter among the profiles of LinkedIn members. <https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions/products/pdfs/linkedin-recruiter-tipsheet-en-us.pdf>

many other social obstacles and structural weaknesses. There are, among others, low and diverging levels of compensation across the EU; fear or distrust on the part of victims with respect to reporting incidents of discrimination; and little awareness of rights and support mechanisms by victims or witnesses.¹⁵⁵⁶

Keeping in mind these gaps and weaknesses, the next section will focus on how EU data protection law could complement EU anti-discrimination legislation or be used as an alternative for protecting individuals against algorithmic decision-making tools with discriminatory effects.

4.2.6. Exploiting the functionality of the GDPR for combatting discrimination in the context of e-recruitment

The hypothesis developed at the beginning of this study was that EU data protection law is a multi-functional framework for the defence of data subjects' fundamental rights. Such multi-functionality would derive from various internal factors, specific to the scope, the substance and the system of supervisory mechanisms and sanctions of EU data protection law. The possibility exists, however, that such a multi-functionality would be to a large extent illusory or underexploited, especially considering the low number of cases at the CJEU level where the GDPR has been interpreted for the defence of (a) fundamental right(s) *other* than privacy or personal data protection. Hence, to test the hypothesis of this study, the below section will apply EU data protection law to cases of discrimination arising from the use of e-recruiting tools – the second 'test area' of this study.

The GDPR contains many provisions relating to data subjects' rights, controllers' obligations and DPAs' prerogatives that could be relevant to combat discrimination in the context of e-recruitment. It would be quite cumbersome however to discuss each of these provisions in details. Hence, keeping the purpose of this study in mind, only the most relevant provisions of the GDPR will be discussed in the following subsections. To make this discussion more vivid, the provisions of the GDPR will be applied to various types of e-recruiting practices at the promotion, pre-selection or selection stage.

4.2.6.1. Rights which can be actioned by the data subjects in the context of e-recruitment to combat discriminatory outcomes

The GDPR has conferred on data subjects an array of rights with a view of providing them with additional control over their personal data. This section will highlight the main rights that individuals can actioned when their personal data are being

¹⁵⁵⁶ Commission third report of 19 March 2021 on the application of the Racial Equality Directive (Directive 2000/43/EC) and the Employment Equality Directive (Directive 2000/78/EC).

processed for the purpose of jobs advertisement (stage 1), or for the purpose of assessing their suitability for a given position (stage 2 and/or 3).

(i) Right to be informed about the processing of personal data: a steppingstone towards more transparency in e-recruitment

Under Articles 12 to 14 of the GDPR, data subjects have the right to be informed about ‘how, why and by whom’ their personal data are being processed. Any data subject¹⁵⁵⁷ whose personal data are processed in the context of e-recruitment should receive information about, *inter alia*, the identity of the data controller, the purpose of the processing, the legal basis of such processing, the period during which the personal data are going to be kept or the existence of an AIDM. The right to information can thus serve as a steppingstone for data subjects to become aware of potential discrimination arising from the use of e-recruiting tools. This presupposes, however, that the data subjects are aware of this processing activity. Indeed, individuals who remain unaware of the e-recruiting practice cannot question it, or exercise any of their other data protection rights, such as asking for the correction of their personal data or contest the outcome of a fully automated decision (see below).

One of the main flaws of this right to information, especially in relation to stage 1 or 2 of e-recruitment, is that companies do not have to actively inform candidates each time their profile is being processed. Hence, most of these processing activities may remain under the radar. As an illustration, after creating a profile on a platform such as LinkedIn, individuals are not systematically notified each time a recruiter operates an automated screening of their profile, which may lead to their inclusion or exclusion from a recruitment procedure.¹⁵⁵⁸ Usually, providing a one-time notice is considered sufficient to comply with the transparency obligations of controllers – for example, at the time the individual registers on a given website.¹⁵⁵⁹ Similarly, if a company decides to advertise a job position on the internet, and defines a target audience for that purpose (for example, a project manager located in a specific city, and having 5 to 7 years of experience), individuals who have been included or excluded from this advertisement campaign will not be actively notified by it. Due to

¹⁵⁵⁷ Be it understood as any living individual located in the EU whose personal data are being processed by a company located in the EU, or even by a company located *outside* of the EU when the latter is profiling that individual or offering him goods or services (including, as the case may be, liaison services with potential recruiters).

¹⁵⁵⁸ The possibility for users to see when and by whom their profile has been viewed is possible, but the detail of the search remains mostly hidden even when the data subject has subscribed to a LinkedIn Premium account. See <https://premium.linkedin.com/>.

¹⁵⁵⁹ In LinkedIn Privacy Policy, for example, the following information is provided under the section ‘Career’: “We will use your data to recommend jobs to you and you to recruiters. We may use automated systems to provide content and recommendations to help make our Services more relevant to our Members, Visitors and customers. Keeping your profile accurate and up-to-date may help you better connect to others and to opportunities through our Services.” See <https://www.linkedin.com/legal/privacy-policy#use>, last accessed on 21/05/2021.

the lack of visibility of some e-recruiting tools, especially those commonly deployed in stage 1 or stage 2 of the recruitment process, a large amount of potentially discriminatory outcomes can thus be left unnoticed. This is the reason why providing data subjects with rights alone would not be enough to make of the GDPR an effective framework in this context; only the obligations imposed on controllers (see section 4.2.6.2, below) as well as the investigative powers of DPAs (see section 4.2.6.3, below) can compensate for the fragility of these rights against hidden e-recruiting practices.

Once a company decides to contact candidates in the context of stage 2 or 3 of the recruitment process, the processing of their personal data necessarily becomes apparent to them, since the data subjects will be invited to actively confirm or share additional information about them. If a company relies on a smart video interviewing software to rank candidates, for example, those data subjects will be aware that a certain type of processing is taking place, since they will actively take part in the interview. At this stage, the right to information becomes truly relevant, as the candidates could require from the company additional details on the nature of the processing, including on the existence, logics and consequences of an AIDM. Having access to this information (or, on the contrary, being denied such access) may trigger additional actions on the part of the data subject who can then become an active actor in the defence of his data protection and related rights, as further explored below.

(ii) Right to access and rectification under Article 15 and 16 of the GDPR: a window of opportunity for spotting discriminatory outcomes

Once candidates are aware of the fact that an e-recruiting tool was used to process their personal data, they may require the company to be granted access to those personal data under Article 15 of the GDPR.¹⁵⁶⁰ This right to access includes in particular the right to obtain “*a copy of the personal data undergoing processing*”.¹⁵⁶¹ At this stage, the candidates can thus have a clearer picture of the different data that a recruiter is using, and may critically assess their accuracy or relevance, but also notice – as the case may be – errors, missing data or inconsistencies.

Following the entry into force of the GDPR, most of the major social or professional networking platforms such as LinkedIn started offering the possibility for each user to obtain a copy of their personal data by logging into their account and downloading one or different data packages. As far as LinkedIn is concerned, the downloadable data are organised in more than 20 folders or excel tables with

¹⁵⁶⁰ Article 15 of the GDPR.

¹⁵⁶¹ Article 15(3) of the GDPR.

different titles, such as ‘ad_targeting’, ‘Company Follows’ or ‘Phone Numbers’.¹⁵⁶² The ‘ad_targeting’ table shows, for example, which recruiters have included one’s profile in an advertising campaign conducted on LinkedIn.¹⁵⁶³ It is however difficult for a person who is not an expert in data analysis to decrypt what the information in each of these columns or rows actually mean. Furthermore, it would require hours of careful investigation to spot eventual mistakes, errors or inconsistencies. Finally, and most importantly with respect to the scenario at stake, LinkedIn does not offer any clear overview of the type of personal data on the basis of which a user’s profile has been included in or excluded from specific search by recruiters. As a consequence, it is almost impossible for data subjects to critically assess whether the personal data composing their public profile has been subject to a type of processing that may have deprived them from a job opportunity on the basis of a protected characteristic or a proxy.¹⁵⁶⁴ In theory, the data subject could contact the controller to request additional information so as to potentially detect or confirm an anomaly in the processing or a violation of the GDPR. If the response is not provided in due time, is incomplete or unintelligible, the data subject may further involve the competent DPA by invoking a breach of the principle of transparency and the non-respect of their right to information on the processing. It is undeniable that the existence of a clear deadline for the controller to respond to such a request, and the fact that a complaint can be filed with the competent DPA at no cost, make the GDPR particularly convenient in this respect.

If the response is provided in due time, and if the data subject is able to notice an error or mistake in the data (for example, missing years of experience), the right to rectification enables them to obtain from the controller rectification of inaccurate or incomplete personal data, including by means of “*providing a supplementary statement*”.¹⁵⁶⁵ Hence, if – but only if – the information provided to the data subject enables them to critically assess whether the e-recruiting tool may have been biased on the basis of erroneous, irrelevant or flagrantly discriminatory input data, then the right to rectification may provide a concrete mean to correct the result. One can imagine, for example, that a candidate receives a disappointing employability score from a video interviewing software and decides to ask the recruiter to have access to the report generated by this software. If this report is clear and comprehensive

¹⁵⁶² On 20/05/2021, the author of this article used the download option available on her own LinkedIn profile in order to have an overview of the personal data that are automatically made available to data subjects when requesting access.

¹⁵⁶³ In the Excel table provided by LinkedIn, names of various companies and institutions are listed, after or before a list of attributes corresponding to one’s profile (such as age group or degrees), without however the possibility to see which attributes served those companies or institutions to target’s one profile. The content and nature of the advertising themselves remain also unknown. (Information based on the author’s own experience after having downloaded her data and analysed the ‘ad_targeting’ folder).

¹⁵⁶⁴ On this topic, please see, inter alia: González Fuster, G. (2018). Transparency As Translation in Data Protection. Emre Bayamlioglu, Irina Baraliuc, Liisa Albertha Wilhelmina Janssens and Mireille Hildebrandt (eds). *Being Profiled: Cogitas Ergo Sum*. Amsterdam: Amsterdam University Press, pp. 52-55; Goodman, B. & Flaxman, S. (2017). *op. cit.*; Wachter S., Mittelstadt, B. & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2):76–99.

¹⁵⁶⁵ Article 16 of the GDPR.

enough (which greatly depends on the diligence of the controller, as discussed below), the data subject may notice a mistake; for example, the algorithm may have wrongfully concluded that this person used injurious terms multiple times during the interview and therefore downgraded their overall employability score by mistake. In line with Article 16 of the GDPR, the data subject could then ask for a rectification and could, at the end of the day, obtain a better employability score and be considered as one of final contenders for the position. The cause behind such an error may however remain obscure. It may be the case, for example, that the algorithm was not properly trained to recognise different accents, thereby wrongfully detecting slurs in the voice of some candidates because of their accent. Beyond its cause, the *scope* of the issue may also remain hidden from the eyes of data subjects. Indeed, since each applicant is only aware of their own result, one data subject cannot know whether hundreds of applicants were downgraded for the same reason or not. In other words, data subjects themselves may lack the necessary insight that would allow them to have a general picture of the situation and eventually spot the origin of this mistake.¹⁵⁶⁶ Hence, data subjects can hardly contest the general functioning or performances of e-recruiting tools. Once again, the lack of transparency or the opacity of some e-recruiting tools may thus defeat the purpose of the right to information and access. This is why obligations imposed on controllers (see section 4.2.6.2, below) as well as the investigative powers of DPAs (see section 4.2.6.3, below) are equally essential tools for combatting discriminatory outcomes arising from the use of e-recruiting tools.

(iii) The right to obtain a human intervention and be informed about the logics of an e-recruiting tool involving an AIDM

Prior to the adoption of the GDPR, a lot of ink had already been shed on the increasing risks that profiling and automated individual decision-making could pose for data subjects' rights and freedoms, and in particular non-discrimination.¹⁵⁶⁷ It is thus not a coincidence if the EU legislator decided to further define and regulate AIDM under the GDPR, and to reinforce the rights of data subjects in this specific context.¹⁵⁶⁸

As already explained above, if a decision by an e-recruiting tool is *fully automated* and produces *legal or similarly significant effects* on the concerned individuals, this

¹⁵⁶⁶ As explained by Zeynep Tufekci in the 2020 documentary 'Coded biases' (director: Shalini Kantayya), an obstacle in holding controllers accountable for relying on discriminatory algorithmic tools is the fact that discrimination may occur "screen by screen" and may thus remain imperceptible for the group as a whole.

¹⁵⁶⁷ Hildebrandt, M. & Gutwirth, S. (2008). *Profiling the European Citizen Cross-Disciplinary Perspectives*. SpringerLink; Council of Europe (2010), *The protection of individuals with regard to automatic processing of personal data in the context of profiling*, Recommendation and explanatory memorandum (CM/Rec (2010)13).

¹⁵⁶⁸ The Commission draft proposal for the GDPR stresses the fact in particular that provisions on automated individual decision-making "builds on, with modifications and additional safeguards, Article 15(1) of Directive 95/46 on automated individual decisions, and takes account of the Council of Europe's recommendation on profiling".

decision will qualify as an AIDM under Article 22 GDPR. Regarding the first criteria, the existence of a legal effect suggests “*a processing activity that has an impact on someone’s legal rights,*”¹⁵⁶⁹ such as the freedom to associate with others, to enter into an employment contract, or to receive a financial advantage. Hence, if an e-recruiting tool is used by a company to determine the amount of the end-of-the-year bonus given to its managers, for example, these decisions can be considered as producing legal effects on the individual and will thus most likely qualify as a regulated AIDM under Article 22 GDPR. By contrast, if an e-recruiting tool is used to profile internet users to show them advertising for a job or an educational programme based on their interests and location (without any certainty to be selected), such a decision is less likely to be regulated under Article 22 GDPR. It must be stressed however that, even if an automated decision does not produce any legal effect, it can still qualify as an AIDM if it “*similarly significantly affects*” the individual concerned. This calls for a distinction between significant and less significant decisions in the context of e-recruitment. On the basis of this distinction, it can be argued that e-recruiting tools used at the promotion stage (for example, for advertising purpose) are less likely to qualify as a regulated AIDM since they merely concern a remote possibility rather than a real opportunity or an actual offer.

To be able to appreciate the severity of the impact of an automated decision on a given data subject, such impact should always be appreciated *in concreto*, taking into account all the relevant circumstances of the case. For example, if an employee fills in an online survey entitled ‘*How good of a manager you really are?*’ out of curiosity, and is characterized as a ‘mediocre manager’, this result will not be considered as an AIDM in the sense of Article 22 GDPR, since it will not have any legal or similarly significant effects on that employee (at most, the result of the survey may slightly influence his mood for the rest of the day but it will certainly not put into question his position as a manager). By contrast, if the same software is used by a company to test the skills of all its employees with a view of calculating their end-of-year bonus or assessing their level of suitability for a newly opened managerial position, such a software would most probably qualify as an AIDM under Article 22 of the GDPR.

The production of legal effects or similarly significant effects on the data subject is not the only requirement that an e-recruiting tool must fulfil to qualify as a regulated AIDM under Article 22 GDPR. On top of that, it must also be shown that the decision is *fully automated*. According to this second criteria, a process will thus only qualify as an AIDM if the decision concerning the data subject is taken solely on the basis of automated means, in the sense that no human is involved in the decision-making process. Hence, if an e-recruiting tool is used in the framework of a recruitment process to elaborate a profile or formulate a recommendation which will then serve as a basis for a human person to take a final decision concerning a candidate, the

¹⁵⁶⁹ *Ibid.*, p. 9.

procedure will most likely not qualify as an AIDM under Article 22 GDPR.¹⁵⁷⁰ Keeping this second criterium in mind, it could therefore be argued that an e-recruiting tool such as the one developed by Amazon (as presented above)¹⁵⁷¹ would have *not* fallen within the scope of Article 22 GDPR since, according to Amazon' declarations, the recruiters were only looking at that score as a recommendation but did not rely on it as a conclusive factor in the hiring decision.¹⁵⁷²

The obvious pitfall of this system is that an unscrupulous recruiter could be tempted to circumvent Article 22 GDPR by asking a straw man – such as an obedient or unqualified employee – to (pretend to) review the automated decisions taken by an e-recruiting tool, and approve them without ever departing from them, so that they would no longer appear fully automated. In this respect, the EDPB already made clear that controllers should not fabricate human involvement.¹⁵⁷³ Hence, for the human involvement to be considered as sufficiently meaningful, the human(s) involved in the decision-making should at least have the authority and competence to review and/or depart from the automated decision.¹⁵⁷⁴ For example, if someone would “*routinely*”¹⁵⁷⁵ rely on results generated by automated means to take a decision regarding data subjects without having the possibility or competence to consider any other factors, such person would have no actual influence on the decision, and the human involvement would thus not be considered meaningful enough. Because of the issue of *over-reliance on automation* pointed above, and the difficulty in bringing evidence thereof, the additional layer of protection offered by Article 22 GDPR could easily be compromised if recruiters do not ensure that automated decisions are meaningfully assessed, nuanced, and corrected when need be. Data subjects, however, have little means to challenge the seriousness of the human involvement put in place by the controllers, since most decision-making procedure take place behind closed doors. Keeping this in mind, it clearly appears that the investigative and corrective powers of DPAs are an essential complement to the rights of data subjects under Article 22, as the latter may not suffice to bring to light a violation of the GDPR.

When it is established that an automated decision qualifies as an AIDM, then the data subjects whose personal data have been processed are granted important additional rights, such as the right to obtain human intervention, to express their point of view and to contest the decision.¹⁵⁷⁶ Most importantly, the data subjects may request from the controller “*meaningful information about the logic involved*” as well as “*the significance and the envisaged consequences of such processing for the*

¹⁵⁷⁰ WP 251, *op. cit.*, p. 9.

¹⁵⁷¹ See section 4.2.2.2, above.

¹⁵⁷² WP 251, *op. cit.*, p. 9.

¹⁵⁷³ *Ibid.*, p. 10.

¹⁵⁷⁴ *Ibid.*

¹⁵⁷⁵ *Ibid.*, p. 21.

¹⁵⁷⁶ Article 22(3) of the GDPR.

data subject."¹⁵⁷⁷ Theoretically, this means that each candidate could for example require information about how a video interviewing software has come to give them a certain employability score. This, in turn, would require from the recruiter the capacity to provide this information. If Article 22 of the GDPR is interpreted and applied strictly (which is still to be seen), self-learning e-recruiting tools that consist in algorithmic 'black boxes' would then, in theory, not be compliant with EU data protection law since, by definition, neither the recruiter nor the developer would be able to provide information about the logic(s) involved.¹⁵⁷⁸ It is undeniable that these additional rights confer to the data subjects additional leverage to suspect, notice and/or contest potential sources of discrimination arising from the use of e-recruiting tools qualifying as an AIDM under Article 22 of the GDPR. Yet, recruiters may not always (be able to) reveal the truth about the logic(s) involved or admit their ignorance thereof. Because of this, the investigative and corrective powers of data protection authorities are essential for reviewing the use of e-recruiting tools qualifying as an AIDM under Article 22 of the GDPR, for prohibiting such use when the tools concerned turn out to be algorithmic black boxes, or for detecting and combatting discriminatory outcomes potentially arising from the use of such tools.

4.2.6.2. Main obligations of controllers that may prevent algorithmic discrimination: data protection by design and by default, DPIA, appointment of a DPO and the necessity to have a valid legal basis

It has been shown that data subjects, although benefitting from some rights that may help them combatting unfair e-recruiting practices, are not in a position to establish the rules of the game. Like David against Goliath, candidates are often at the mercy of the will of recruiters. This is all the truer when considering the imbalance of powers that characterizes the relationship between job seekers and job providers, and between internet users and giant professional networking platforms. Hence, the protection of the rights and freedoms of data subjects also largely depends on the diligence of controllers in actively seeking to comply with the GDPR, as well as the supervision and enforcement actions conducted by DPAs. This section will focus in particular on the second layer of the GDPR-shield: the obligations of controllers in the context of e-recruitment.

Preventing discriminatory effects arising from the use of e-recruiting tools will not be a successful endeavour without imposing on the licensors and licensees of such tools strict obligations aiming at ensuring the respect of the rights and freedoms of candidates. Besides the anti-discrimination laws discussed above, the GDPR contains multiple provisions that can be invoked to foster the accountability of recruiters and licensors with respect to development or use of e-recruiting tools. In particular, one

¹⁵⁷⁷ Art. 13(2)(f) of the GDPR.

¹⁵⁷⁸ See, in this respect, Wachter, S., Mittelstadt, B. & Floridi, L. (2017). *op. cit.*

may refer to (i) the obligation to ensure data protection by design and by default; (ii) the obligation of data controllers to conduct a DPIA where a type of processing using new technologies, including reliance on a e-recruiting tool, is likely to result in a high risk to the rights and freedoms of natural persons;¹⁵⁷⁹ (iii) the obligation to consult the competent DPA in the event the result of a DPIA indicate that the processing at stake would *still* entail high risks, despite the implementation of several safeguards; (iv)¹⁵⁸⁰ the obligation for major companies in the sector of recruitment to hire a Data Protection Officer (DPO), the latter having the duty to monitor compliance by its company with the GDPR and, where necessary, issue internal warnings if an e-recruiting tool produces discriminatory outcomes or represents a risk in this respect;¹⁵⁸¹ or, more generally (v) the obligation of controllers and processors to have a valid legal basis when processing personal data for the purpose of recruitment, including, as the case may be, the consent of the data subjects when special categories of data such as data on ethnic origin, political opinions or sexual orientation are being processed.¹⁵⁸²

In the opinion of the author, the obligation of data protection by design and by default, combined with the obligation to conduct a DPIA where a processing activity represents a 'high risk' to the rights and freedoms of natural persons, as already both discussed above (see Section 3.2.2.2(iv)), are particularly relevant in the context of e-recruitment, as it could prevent in many instances the offer on the market or the use by recruiters of poorly elaborated e-recruiting tools producing discriminatory outcomes.¹⁵⁸³ According to article 35(3) of the GDPR, a processing activity is likely to "*result in high risks*" and therefore requires a DPIA when it involves "*a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*".¹⁵⁸⁴ In other words, e-recruiting tools qualifying as AIDM under Article 22 of the GDPR would in any case require the controllers to conduct a DPIA *prior* to the implementation of the e-recruiting tool. Referring to the example provided above, a company wishing to implement a video interviewing software similar to HireVue will thus most likely fall under the obligation to conduct a DPIA, with a view of identifying and mitigating the risks that such an e-recruiting tool could represent for the rights and freedoms of data subjects, including the right to non-discrimination. The obligation to conduct a DPIA implies that the recruiter has to describe the processing activity that it intends to put in place, including the technologies involved, assess its necessity and proportionality,

¹⁵⁷⁹ Art. 35 of the GDPR.

¹⁵⁸⁰ Art. 36 of the GDPR.

¹⁵⁸¹ Art. 37-39 of the GDPR, and in particular 39(1)(a) and (b).

¹⁵⁸² Article 9(2)(a) of the GDPR.

¹⁵⁸³ As an indication that this provision may work as intended, most of the companies that are offering 'smart' e-recruiting tools are located in the US, as well as their clients. It may be the case that EU actors subject to the GPR are more careful towards the effects of these technologies in general, including due to their compliance obligations in the field of EU data protection law.

¹⁵⁸⁴ Point (a) of Art. 35(3) of the GDPR.

identify all the risks associated with it for data subjects, and find manners to mitigate those risks.¹⁵⁸⁵

DPIAs must be formalised in writing, usually in the form of a report, to ensure compliance with the principle of accountability (recruiters could indeed be required by the competent DPA to share a copy of this report). As highlighted by the EDPB,¹⁵⁸⁶ DPIAs are thus important tools for accountability, as they require from controllers not only to take concrete steps to comply with the GDPR, but also to demonstrate that these steps have been taken to ensure compliance with EU data protection law.¹⁵⁸⁷ As far as e-recruitment is concerned, one may think of multiple safeguards to mitigate existing risks of discrimination, such as carefully selecting the input data, consistently monitoring the output data, mandating an external audit before starting to use the e-recruiting tool, and/or ensuring that candidates can always contest the decision and be granted a swift and comprehensive human review of their case when requested. Once again, however, the success of this provision is largely dependent on the interpretation that will be made of it by recruiters, as well as their level of diligence when implementing such tools. On the positive side, the fact that most major companies active in the recruitment sector¹⁵⁸⁸ would normally also be subject to the obligation to appoint a DPO¹⁵⁸⁹ may enhance compliance with this obligation, as DPOs would normally alert the management on the need to conduct a DPIA prior to the implementation or offering of an e-recruiting tool. Not all recruiters however must appoint a DPO (see Section 3.2.2.2(iii), above).¹⁵⁹⁰

More generally, the obligation for controllers to have a valid legal basis prior to processing personal data, read in light of the principle of lawfulness, fairness and transparency, can also prevent the use of e-recruiting tools or practices leading to potential discrimination. As discussed above, the GDPR provides for two separate set of legal bases depending on whether the personal data are considered sensitive or not under Article 6 and Articles 9 and 10, respectively (see Section 3.2.2.1 and 3.2.2.2(i), above). As a rule of thumb, the processing of sensitive data by an e-recruiting tool, such as data relating to the health, religion, sexual orientation, or political opinion, is more likely to lead to discriminatory outcomes precisely because of the sensitive nature of such data. It is thus essential to ensure that the processing of these data for recruitment purposes is adequately regulated. Under Article 9 GDPR, it appears that recruiters could rely on two legal bases to process such data as

¹⁵⁸⁵ See Art. 35 of the GDPR and Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, WP 248 rev.01 (13 October 2017).

¹⁵⁸⁶ Previously known as the Article 29 Working Party.

¹⁵⁸⁷ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, WP 248 rev.01 (13 October 2017).

¹⁵⁸⁸ Including professional networking platforms such as Monster or LinkedIn.

¹⁵⁸⁹ Most recruitment agencies and professional networking platforms would indeed fall within the scope of Article 37(1)(b).

¹⁵⁹⁰ In particular, a majority of private recruiters would not need to appoint a DPO since their HR activities remain in principle peripheral to their core activities. By contrast, public authorities must always appoint a DPO (cf. Art. 37(1)(a) GDPR).

part of a e-recruitment procedure: either the “*explicit consent*” of the data subject (Article 9(1)(a) GDPR, or the fact that the data have already been made “*manifestly public*” by the data subject (Article 9(1)(e) GDPR). As far as consent is concerned, the latter should not only be explicit to be valid, but must also be specific, informed, unambiguous and “*freely given*”.¹⁵⁹¹ Therefore, if a recruiter intends to rely on the explicit consent of each candidate to process their sensitive data in the context of an e-recruitment procedure, there still exists a risk that such a consent would not be valid, given the imbalance of power that characterizes the relation between candidates and recruiters, or between employees and employers.¹⁵⁹² As noted by the EDPB, indeed, “*employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Unless in exceptional situations, employers will have to rely on another legal ground than consent (...)*”.¹⁵⁹³ Hence, candidates could challenge the processing of sensitive personal data by an e-recruiting tool, even if they had previously ticked a box or otherwise agreed to the processing of such data in the first place. Article 9 GDPR, read in combination with Article 4(11) and 7 on the condition for consent, could thus be particularly functional in preventing the discriminatory processing of sensitive personal data by recruiters, even when candidates have agreed to it. Another legal ground that recruiters could invoke is the fact that the sensitive data in question were made “*manifestly public*” by the data subject. It may be the case, indeed, that an individual has willingly and publicly shared information on his/her ethnicity, religion, sexual orientation, or political opinion on a LinkedIn profile, for example. As far as ethnicity and religion are concerned, such information could also be inferred from a profile picture. Even if the processing of such sensitive data could be justified on that ground, however, the processing must in all case remain fair, in accordance with Article 5(1)(a) GDPR. Hence, if it is found that an e-recruiting tool produces discriminatory outcomes by rejecting candidates on the basis of sensitive personal data – even when such data were made manifestly public by the data subjects concerned – the recruiter could still be held liable for a breach of the GDPR and be ordered to put an end to such a practice. An interesting point in this respect is that the notion of ‘sensitive data’ does not strictly correspond to the notion of protected characteristics under EU anti-discrimination law. Both notions may thus complement each other when assessing, on the one side, the lawfulness of the processing, and on the other side, the fairness of the processing. In particular, data relating to one’s religion or beliefs, handicap or disability, sexual orientation, or race or ethnicity, both qualify as sensitive personal data and protected characteristics under EU law. Yet, the notion of sensitive data also extends to data relating to health, genetics, criminal offences, political opinions, or trade union membership. By contrast, the notion of sensitive data does *not* include data relating to one’s gender or age, while these two elements are considered as potential discriminatory factors

¹⁵⁹¹ Article 4(11) GDPR.

¹⁵⁹² WP29, Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, p. 6, available at <https://ec.europa.eu/newsroom/article29/redirection/document/51030>.

¹⁵⁹³ WP29, Opinion 2/2017 on data processing at work, adopted on 8 June 2017, p. 4, available at https://ec.europa.eu/newsroom/document.cfm?doc_id=45631.

under EU anti-discrimination law. To give a visual overview of this, the below table shows which characteristics qualify as ‘protected’ under EU anti-discrimination laws and/or as ‘sensitive’ under data protection law.

TABLE 11

The below table provides an overview of human characteristics that are considered as ‘protected’ under anti-discrimination law and/or as sensitive personal data under Articles 9-10 GDPR, and show that the explicit scope of the GDPR is larger than of the explicit scope of anti-discrimination law.

	Protected characteristic under EU anti-discrimination law	Sensitive data under the GDPR (Articles 9 and 10)
Religion or philosophical beliefs	✓	✓
Handicap or disability	✓	✓
Sexual orientation	✓	✓
Race or ethnicity	✓	✓
Physical or mental handicap	✓	✓
Health (beyond handicap)	X	✓
Genetics	X	✓
Criminal offence	X	✓
Political opinions	X	✓
Trade union membership	X	✓
Gender	✓	X
Age	✓	X

Even if a personal data does not qualify as ‘sensitive’, however, controllers must still have a valid legal basis to process them for the purpose of recruitment under Article 6 GDPR. In line with the principle of lawfulness, fairness and transparency, such a processing cannot lead to the unfair exclusion of candidates on illegitimate grounds, such as their gender or age, for example, as this would arguably violate Article 5(1)(a) and/or 6(1)(f) GDPR. In the opinion of the author, the flexibility of interpretation pertaining to the principle of lawfulness and fairness may thus become particularly functional for combatting discriminatory outcomes in instances where a recruiter has a valid legal basis for the processing their data under Article 6 or 9 GDPR but does not process these data in a manner which is lawful or fair for the concerned candidates, also in light of the principle of non-discrimination enshrined in Article 21 of the Charter and in EU secondary law.

Although each of the above-mentioned obligations cannot guarantee alone the proper elaboration and use of e-recruiting tools, they nonetheless provide a regulatory framework which binds recruiters and licensors of e-recruiting tools operating on the EU market. Those obligations, each in their own way, should thus help to ensure the quality and reliability of e-recruiting tools, and encourage recruiters to continuously monitor their effects, with a view of preventing or swiftly correcting any potential discriminatory outcomes. For such obligations to have a truly beneficial effect, however, one has no choice but to count on the diligence of recruiters and licensors. Some of them might make of compliance with EU data protection law a priority with a view of gaining a competitive advantage on the EU market, and thus invest in the development of compliant e-recruiting tools. Some others, however, may be primarily driven by other incentive, such as cost-effectiveness and profits. Hence, it is crucial that data subjects actively use their rights, as discussed above, and that DPAs exercise their investigative powers to monitor compliance with and enforce EU data protection law, as discussed below. It has been shown above indeed that the functionality of the GDPR principally derive from the interactions of the various panels of the PRO-triptych, as supported by the supervisory and corrective powers of DPAs. For example, if a recruiter seeks to hire a French and Dutch-speaking receptionist having five years of experiences, and uses for that purpose a screening algorithms that automatically rejects the CVs of candidates below 26 years of age, it could be argued that such a processing is in breach of Article 5(1)(a) GDPR because of the lack of fairness of such an excluding factor, even if the candidates in question have consented to the processing of their personal data, including their date of birth, when uploading their CV. A candidate could request a controller to provide additional information on the processing, and in particular information on the logics involved behind the automated decision on the basis of Article 13(2)(f) GDPR. If it is later found that the algorithm was systematically considering that candidates below 26 years of age did not satisfy the requirement of five years of experience, while this is an obviously wrong assumption, the recruiter could then be held liable for having failed to identify this error and the risk of unfair discrimination attached to it when conducting the required DPIA. Under EU anti-discrimination laws, indeed, age is considered a protected characteristic. Through this example, one can thus appreciate how the various panels of the PRO-triptych form together a legal sequence which, once read together with EU anti-discrimination laws, form a stronger narrative for the defence of data subjects' rights and freedoms, and in particular their right not to be discriminated.

4.2.6.3. Investigative and corrective powers of DPAs as essential tools to combat the inbuilt bias or the misuse of e-recruiting tools

The supervision and sanction system of the GDPR is the third pillar of functionality of EU data protection law. As already argued above, it is also one of the most essential

pillars when it comes to ensuring the robustness of the entire framework with respect to its FRO. A welcomed development in this respect is that the GDPR has broadened the competences and tasks of DPAs and considerably increased their investigative and corrective powers (see Section 3.3.1, above). Among these powers, one may refer, in particular to their investigative powers in the form of data protection audits; their power to force controllers to comply with requests from data subjects; to impose ban of processing activities (including, as the case may be, on the use of a certain e-recruiting practices or tools) and, of course; to apply deterrent sanctions, up to 4% of the total worldwide annual turnover of the controller or 20 million euros, whichever the higher.¹⁵⁹⁴

As discussed above, the negative effects that e-recruiting tools can have on data subjects may not always be obvious because of the opacity of most e-recruiting tools, or because discrimination may be conducted by stealth (see Section 4.2.4, above). As a result, discriminatory outcomes arising from the use of e-recruiting tools could not only be significant in terms of scope but also long-lasting. Indeed, it is not possible to put an end to a breach when such a breach remains out-of-sight. In this context, the proactive role that DPAs can play in uncovering breaches appears more important than ever. In order to concretely illustrate how the GDPR, and the investigative and corrective powers of DPAs in particular, are essential tools to prevent discriminatory outcomes in the field of e-recruitment, the author will refer to a decision rendered by the Italian DPA (the '*Garante per la Protezione dei Dati Personali*' or '*Garante*') in June 2021 against the food delivery company Foodinho.¹⁵⁹⁵

Foodinho operates a digital platform for on-demand food delivery in the Italian city of Milan.¹⁵⁹⁶ Individuals can use Foodinho website or app to order food from various Milanese restaurants and get it delivered at their house, office, or another location. Foodinho contracts with self-employed individuals to ensure the picking up and delivery of the food, usually by bike. These individuals (hereafter, 'bikers') are paid based on the number of completed deliveries. To be able to take orders, Foodinho bikers must first install a special app on their smartphone and select, for each day of the week, different time slots of one hour each during which they are willing to work. Not all timeslots are available to all bikers; rather, certain time slots are made available to bikers depending on their past performances. Once one or multiple time slots have been booked, the biker can open the app on the selected days and hours and confirm availability to start receiving orders. To avoid 'cherry-picking', Foodinho does not share upfront the collection and delivery addresses of each food order with

¹⁵⁹⁴ With the caveat that a majority of Member States have excluded the possibility for DPAs to fine public authorities in breach of EU data protection law. In some instances, however, depending on the implementation that was made of the GDPR in each Member State, it may be the case that public authorities, when searching to hire new recruits, would be considered as acting outside of the scope of their public tasks and could thus be subject to such fines. See Article 83 of the GDPR and in particular Article 83(7) of the GDPR.

¹⁵⁹⁵ Garante per la Protezione dei Dati Personali, Ordinanza ingiunzione nei confronti di Foodinho s.r.l., n° 9675440, 10 June 2021, available at <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440>.

¹⁵⁹⁶ See Foodinho company profile via <https://www.linkedin.com/company/foodinho>.

its bikers. Rather, the location of the collection point is only communicated after a biker has accepted the order. Then, once the food has been collected from the restaurant, Foodinho shares the precise delivery address. Bikers can therefore not accept or decline orders based on the location of the collection or delivery point. As far as remuneration is concerned, bikers can see the maximum amount that will be paid before accepting an order. This amount is a variable value calculated at Foodinho's discretion based on three elements: (1) a basic fee (2) a fixed compensation per kilometer; and (3) five cents for each minute of waiting after the first 10 to 15 minutes at the restaurant. Bonuses can also be provided at the discretion of Foodinho depending on the performances of the bikers and the weather conditions (for example, in case of rain). Bikers are also assigned a score based on their performances (e.g., how many deliveries have been completed on time or abandoned) and the reviews received from restaurants and customers. Poor performances and negative reviews can decrease their overall score, while good performances and positive reviews can increase it. According to the explanations provided by Foodinho to the *Garante*, this performance score mainly serves as a reference point for assigning time slots to bikers. A higher score gives bikers the opportunity to view the calendar with the different available time slots in advance of other bikers, and thus select their favorite time slots. As a consequence, bikers with a poor performance score may not be able to work during their preferred or time slots or may not be able to work at all. In line with the definition provided in this study, this type of processing can thus be considered as an e-recruiting practice at the third stage of recruitment – i.e., the selection stage – since data subjects are provided by automated means with an actual offer or advantage (in this case, the opportunity to work and be remunerated).

On 16 and 17 July 2019, the *Garante* launched an *ex officio* investigation into Foodinho data processing practices. This procedure was launched as part of a joint operation with the Spanish DPA who had decided to investigate the processing practices of Foodinho's holding company, GlovoApp23.¹⁵⁹⁷ Both DPAs were indeed sharing similar concerns with respect to the use by these companies of AIDM to micromanage their deliverers. On the Italian side of the procedure, the *Garante* made use of its investigative power to conduct an on-site inspection at the registered office of Foodinho in Milan in order to collect evidence of its data processing practices. At the time the investigation was carried out, 18,684 bikers were registered with Foodinho. During the investigation, Foodinho shared some information with the *Garante* as to the functioning of its algorithms for organizing its food delivery services. It was clarified, in particular, that the performance score assigned to the bikers was fully automated, without prejudice to the possibility for Foodinho to change this score manually. After considering all the collected evidence and the additional information provided by Foodinho, the *Garante* found several breaches of the GDPR.

¹⁵⁹⁷ Glovoapp23 S. L. is a software development company based in Barcelona, Spain. It is principally now for its food delivery app 'Glovo'. See company profile at <https://www.linkedin.com/company/glovoapp23-s.l>.

First, the Garante found that Foodinho had failed to properly inform the bikers in accordance with the principle of transparency enshrined in Article 5(1)(a) and its information obligation under Article 13 GDPR. In accordance with Article 13(1)(c) and 2(f) GDPR, bikers should have been clearly informed about the purposes and legal basis of the processing of their personal data, as well as the existence of an automated decision-making based on profiling. Given the existence of an AIDM in the sense of Article 22 GDPR, the bikers should also have been provided with “*meaningful information*” about the logic of the e-recruiting tool, as well as the significance and the envisaged consequences of such processing in terms of job opportunities, as required by Article 13(2)(f) GDPR. The Garante noted however that the data protection policy available via the bikers’ app, and the additional fragmented information provided to the bikers during the recruitment process, was too unorganized, unprecise or vague for bikers to be properly informed about the essential elements of such a complex processing activity. In particular, the Garante found that Foodinho had failed to clearly inform the bikers about the constant tracking of bikers’ live location while on duty, about the automated assessments of their performances, and about the influence of their assigned score on future job opportunities. The Garante therefore concluded that Foodinho had breached its transparency obligations under Article 5(1)(a) and 13 GDPR.

Secondly, the *Garante* found that the automated processing of bikers’ personal data for assigning them a performance score qualified as an AIDM regulated under Article 22 of the GDPR, given that such scores were determined *fully by automated means*, and had *significant effects* on the bikers. The fact that Foodinho could potentially correct this score manually did not change the finding that the scores were ‘fully automated’, since the possibility to intervene does not amount to an actual human intervention. As to the significance of the effects on the concerned data subjects, it was pointed out that a poor performance score could lead to the exclusion of bikers from actual job opportunities and thus significantly affect their revenues. Hence, the Garante concluded that Article 22 GDPR was applicable to the e-recruiting tool used by Foodinho. With respect to the legal basis for such a processing, the Garante conceded that the necessity of the performance of the contract envisaged under Article 22(2)(a) GDPR could justify the automated assignment of scores to determine which bikers could book time slots in advance of others. However, the Garante noted that Foodinho had failed to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests against discriminatory outcomes. In particular, the *Garante* considered that the possibility for bikers to report issues through internal channels (for example, via email or a chat available on the application) did not amount to ‘suitable measures’ that would *de facto* allow bikers to obtain a human intervention, to express their opinion, or to contest the score assigned to them by the e-recruiting tool (i.e., the three rights guaranteed under Article 22(3) GDPR). Furthermore, the fact that bikers had not even been informed of their rights in this respect was perceived as an aggravating factor by the Garante. In assessing the gravity of the breach of Article 22(3) GDPR, the Garante

also explicitly stressed the risk of discrimination arising from the use of such an e-recruiting tool. Most interestingly, the Garante stressed that e-recruiting tools relying on machine-learning, if not sufficiently transparent and robust, could reproduce and amplify human biases. Hence, Foodinho and its holding company should have adopted some form of ‘algorithmic vigilance’¹⁵⁹⁸ to prevent interferences with the principle of non-discrimination and the dignity of deliverers. Regarding this risk of discrimination, the Garante expressed particular concerns over the fact that restaurants and customers’ reviews determined 20% of a biker’ overall score, and that Foodinho had not adopted appropriate measures to avoid improper or discriminatory use of such feedback mechanism.¹⁵⁹⁹

The Garante also identified a number of other breaches which had probably led to these unlawful processing practices, including the fact that Foodinho had failed to conduct a proper DPIA, had not respected its obligation of data protection by design and by default (notably, by failing to prevent discriminatory outcomes through the use of their algorithm) and had failed to appoint a DPO as from the entry into force of the GDPR. As discussed above (see Section 3.2.2), these obligations of a preventive nature – if respected – can consist in several safeguards allowing software developers or recruiters to spot a discriminatory issue before an e-recruiting tool is even put to use.

Based on the above considerations, the Garante ultimately held that Foodinho had violated the GDPR¹⁶⁰⁰ and imposed a fine of €2,600,000 on the company, taking into account, inter alia, the severity of the breaches, the lack of cooperation of Foodinho during the investigation, and the large number of bikers who were registered on the platform and whose rights had been violated. In addition, the Garante issued an injunction ordering Foodinho to bring its processing operations into compliance with the GDPR, notably by adopting new measures for preventing any discriminatory effects arising from the use of its automated scoring system for the attribution of job opportunities.¹⁶⁰¹

In the opinion of the author, this decision shows that, on paper as in practice, DPAs have an incredible arsenal of means to ensure that the rights and freedoms of data subjects are respected in the context of the processing of personal data for recruitment, employment or occupational purpose. It also illustrates the importance of the third pillar of the GDPR, and of its multi-actor enforcement system in particular, in ensuring the robustness and functionality of the entire framework. In

¹⁵⁹⁸ The Garante used that term by referring to the OECD Guidelines on Artificial Intelligence and Data Protection, adopted by the Consultative Committee of Convention 108 on 25 January 2019, available at <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>.

¹⁵⁹⁹ In original language: “*Con riferimento, infine, al meccanismo di feedback, che determina il 20% del punteggio di eccellenza, non risulta che la società abbia adottato misure appropriate per evitare usi impropri o discriminatori dei meccanismi reputazionali basati sui feedback.*” (see point 3.3.6., para. 11 of the ordinance n° 9675440 of the Garante).

¹⁶⁰⁰ And in particular Articles 5(1)(a), (c) and (e), 13, 22, 25, 30, 32, 35 and 37 of the GDPR.

¹⁶⁰¹ See points 5 and 6 of the ordinance n° 9675440 of the Garante.

this case indeed, Foodinho's bikers themselves were largely unaware of the existence or full extent of these breaches because of the opacity of the algorithm, and the failure on the part of Foodinho to properly inform them about the existence and impact of its scoring system. Hence, despite the very large number of bikers being registered with Foodinho at the time (around 19.000), the investigation into Foodinho's processing practices was not triggered by a data subject's complaint, but rather by the *Garante* itself, who decided to conduct an investigation of its own volition. This corresponds to the chain of enforcement n°4 in the graphic presented under Section 3.3.3. In other words, the multi-actor enforcement system established under the GDPR, and the proactive stance of the *Garante* in particular, allowed to support the first and second pillar of the GDPR in order to release its full potential.

4.2.6.4. Concluding remarks on the functionality of the GDPR to combat the harmful effects of e-recruitment on equality and non-discrimination

Algorithmic decision-making has revolutionised the recruitment sector and will probably continue to do so, as increasingly sophisticated tools are being developed to improve the cost-effectiveness of recruitment. Depending on how the industry is regulated and controlled, e-recruitment may either bring more fairness and objectivity in the recruiting process or, on the contrary, produce or amplify inequalities and discriminatory outcomes. In this respect, understanding the differences between human and algorithmic discrimination in the context of recruitment is essential for developing appropriate regulatory and enforcement practices. In particular, phenomena pertaining to the use of algorithmic decision-making tools, such as systematisation, escalation, dissimulation or feedback loops, should be seriously monitored, as they may drastically enhance inequalities which, depending on their nature, could escape the scope of more traditional anti-discrimination laws adopted to prevent human discrimination. In this context, the GDPR could be used as a functional framework that is able to combat these new types of discriminatory outcomes.

The above section has showed that EU data protection law, and the GDPR in particular, offers a promising regulatory framework to prevent or combat discriminatory outcomes arising from the use of e-recruiting tools in a preventive and corrective manner. Although the author has limited her analysis to the field of recruitment, the same considerations may also apply *mutatis mutandis* to ADM in other fields, such as criminal justice (e.g. automated 'risk score' attributed to defendants), banking (e.g. automated denial of a loan or closure of a bank account), public security (e.g. automated decision to deploy police forces within a specific neighbourhood), provision of goods and services (e.g. approval of bookings on platform such as Airbnb) or healthcare (e.g. automated triage of patients on the basis of their symptoms in the midst of a pandemic).

Among the internal factors of functionality of EU data protection law, it is argued that the success of the GDPR as a shield to protect the rights and freedoms of data subjects largely depends on the solidity and proper imbrication of its different layers of rights, obligations and supervisory mechanisms. In particular, it seems that the rights of the data subjects – although seemingly functional to bring more transparency into e-recruitment, could be easily defeated without diligence on the part of recruiters. Similarly, although it is true that many obligations stemming from the GDPR should encourage the development and monitoring of compliant e-recruiting tools by software developers and recruiters (such as controllers' obligations in relation to DPIA and AIDM), only effective supervision from the competent authorities may prevent less diligent actors from violating these rules and introducing discriminatory e-recruiting tools on the market. In particular, because of the dissimulation phenomenon discussed above, discrimination arising from e-recruiting tools could go unnoticed for a long time if not properly investigated. Hence, it is essential that DPAs make use of their investigative powers to supervise both the development and the application of e-recruiting tools at all stages of the process, from promotion to selection. The proactive stance of some DPAs such as the Garante or the AEDP is a positive sign that the multi-functionality of the GDPR can be put into action to protect data subjects from unfair or potentially discriminatory e-recruiting practices. Other DPAs should follow this model in the future, so as to ensure that e-recruiting tools do not unduly discriminate data subjects but live up to their promises to increase objectivity and fairness in the recruitment process.

CHAPTER 5 – SUMMARY FINDINGS, RECOMMENDATIONS & CONCLUSIONS

This study has conceptualised the notion of the functionality of the law, before assessing whether EU data protection law, and the GDPR in particular, could be considered as a multi-functional framework for the defence of data subjects' fundamental rights and freedoms against the negative effects of novel DDTs or modern data processing practices. As part of this assessment, a distinction has been drawn between the primary functionality of EU data protection (i.e., when the rules are applied for the defence of data subjects' rights to privacy and personal data protection) and the secondary functionality of EU data protection law (i.e., when these rules are applied for the defence of other fundamental rights and freedoms, referred to as 'DFR').

Building on the previous Chapters of this study, the author will, first, provide a **summary of her findings** regarding the main factors of (multi-)functionality of the GDPR, and provide **her recommendations** on how to further preserve and enhance such (multi-)functionality in the future (Section 5.15.1.1). The author will then present **her final reflections and conclusions** on the causes behind the apparent **shortfall** of the secondary functionality of the GDPR, as well as the **desirability** and **legitimacy** of further exploiting such a secondary functionality for combatting the negative effects of novel DDTs or data processing practices on DFR (Section 5.2).

For the sake of clarity, this final Chapter will be structured around the following questions in particular:

- *What* are the main factors of multi-functionality of the GDPR for the defence of data subjects' fundamental rights and freedoms, and *how* to further preserve and enhance such multi-functionality? (i.e., summary findings and recommendations);
- *What* can explain the apparent shortfall in the secondary functionality of the GDPR, and *should* this secondary multifunctionality be used more often for the defence of DFR? (i.e., final reflections and conclusions).

5.1. SUMMARY FINDINGS AND RECOMMENDATIONS REGARDING THE MAIN FACTORS OF MULTI-FUNCTIONALITY OF THE GDPR WITH RESPECT TO ITS FUNDAMENTAL RIGHT OBJECTIVE

For the sake of consistency and clarity, the summary findings and recommendations of the author of this study will be structured around the three structural pillars of the GDPR, i.e., its Scope, its Substance, and its Supervision and sanction system.

5.1.1. Summary findings regarding the main factors of multi-functionality of the GDPR

5.1.1.1. With respect to the scope of the GDPR

As far as the scope of the GDPR is concerned, the following internal factors in particular have been identified as contributing to the overall multi-functionality of the GDPR:

- a) As far as the **material scope** of the GDPR is concerned:
 - i. The material scope of the GDPR is not limited to ‘privacy matters’; rather, the GDPR applies when personal data are being processed, without the need to demonstrate that the processing operation at stake has interfered with the fundamental right to privacy or personal data protection of the data subjects concerned. This rational approach grounded in the objective notions of ‘processing’ and ‘personal data’ facilitates the application and enforcement of the GDPR for the benefit of a wide range of interests, rights and freedoms.
 - ii. The notions of ‘processing’ and of ‘personal data’ have been ascribed a broad meaning in the legislation and the case-law of the CJEU, thereby bringing many situations in the scope of the GDPR; this broad material scope of the GDPR is further enhanced by multiple phenomena, such as the Negroponte shift, the tensions between anonymisation and de-anonymisation techniques, and the contamination theory. As a result, the GDPR is encompassing a growing number of processing operations.
 - iii. The material scope of the GDPR includes both processing of personal data by automated means and manual processing when the data form part of a filing system. As far as processing by automated means is concerned, the material scope of the GDPR is not limited to a particular type of technology. Hence, the GDPR can apply regardless of the DDT that is being used. As far as manual processing is concerned, the non-restrictive interpretation given by the CJEU to the notion of ‘filing system’ has enabled to include a wide variety of non-automated processing operations within the scope of the GDPR, for the benefit of data subjects’ rights, freedoms and interests.
 - iv. There is no quantitative condition attached to the notion of ‘processing’ or the notion of ‘personal data’ (i.e., no *de minimis* rule applies under EU data protection law); this means, in particular, that the processing of even

one type of personal data for a very limited amount of time can trigger the application of EU data protection law.

- v. Although the GDPR does not apply to the processing of personal data by individuals in the context of purely personal or domestic activities, in case of mixed processing, where part of the processing is directed outwards from the private setting of an individual, the GDPR applies. As a result, data subjects can rely on the GDPR even in situations where their personal data are being processed by other individuals in a semi-private context.

b) As far as the **territorial scope** of the GDPR is concerned:

- i. The territorial scope of the GDPR is not limited to the EU but is construed around the borderless effects that processing activities can have on the rights and freedoms of data subjects, regardless of where the processing is taking place. Hence, the GDPR has a wide territorial reach which also protects the rights and freedoms of data subjects located *outside of the EU* when their data are being processed by an EU controller, and data subjects located *in the EU* when their personal data are processed by a non-EU controller for monitoring purposes or for the purpose of providing them with goods or services. As a result, data subjects are not deprived of their data protection rights by the mere fact that they are not resident of an EU Member State, or by the mere fact that the processing would not take place in the EU.
- ii. The integrity of the territorial scope of the GDPR is protected by several safeguards to ensure that the level of protection of the rights and freedoms of data subjects do not diminish once their personal data are being transferred abroad. These special safeguards include the obligation for non-EU controllers to establish a representative in the EU, the obligation to abide to specific transfer mechanisms, the obligation of controllers to enter into data processing agreements with processors, and international cooperation mechanisms. These safeguards increase the convenience with which data subjects may hold EU or non-EU controllers or processors accountable for their actions, including when located abroad.

c) As far as the **personal scope** of the GDPR is concerned:

- i. The personal scope of the GDPR is grounded in the notion of 'personal data' and does not require the fulfilment by right holders of any additional condition to be recognised as such (no condition of citizenship, nationality, age or *compos mentis*).

- ii. The personal scope of the GDPR is also broad as far as duty bearers are concerned, in the sense that any person processing personal data will necessarily be either a controller or a processor, regardless of whether that person is a natural or a legal person, or whether it is acting in a private or public capacity. This means, for example, that the GDPR can also be used against public authorities in combination with or in a manner that serve the right to access administrative documents or the right to a good administration.
- iii. The GDPR embraces a unitary approach to the notions of 'controller' and 'processor', including when multiple controllers, processors and sub-processors are involved in shared processing activities, which facilitates the exercise of data protection rights by data subjects, and in particular the possibility to hold one or multiple party/parties accountable for their actions or omissions under EU data protection law, without having to identify or file a claim against all the actors involved.
- iv. The GDPR allows data subjects to be represented by not-for-profit entities that are knowledgeable and experienced in the field of human rights and/or IT law, thereby facilitating the filing of complaints, including in cases where a group of (non-identified) data subjects is affected by the same alleged breach(es) of the GDPR.

Because of the above, it can be argued that the GDPR has a particularly broad material, territorial and personal scope that facilitate its use in a variety of situations. In particular, data processing practices that interfere with a fundamental right or freedom can be challenged on the basis of the GDPR, regardless of the nature of the right or freedom at stake, the voluntary or accidental nature of the processing, the amount of data that is being processed, the duration of the processing, the qualification of the data subject, or the identity of the controller. Moreover, to ensure that the level of protection established under the GDPR is not undermined by data transfers, and to avoid situations where controllers/processors would be able to circumvent the applicable rules by outsourcing their processing activities, the territorial scope of the GDPR has been stretched to processing activities taking place outside of the EU, as long as a link still exists between this processing activity and the EU territory (either because the controller/processor is located in the EU, or because the data subjects are). All these elements pertaining to the scope of the GDPR can thus be considered as factors which makes it particularly functional for the defense of data subjects' rights and freedoms, in the sense that the actors willing to rely on to GDPR will be able to do so in a wide range of situations, without having to deal with burdensome limitations or restrictions as to the scope of the legislation. As illustrated in Chapter 4, this allows the GDPR to be used, for example, to defend the right to dignity, integrity or freedom of expression of data subjects who are victims

of online harassment, or to protect data subjects from undue discrimination in the context of e-recruitment.

Because of this broad scope and the parallel 'datafication' of human activities, the GDPR is sometimes being labelled as "*the law of everything*"¹⁶⁰² – a label that could be considered as problematic if, indeed, the rules that it contains would become unbearable or unworkable for its addressees. To counterbalance the dysfunctional effects of an all-encompassing scope, however, the GDPR also contains clear exceptions and exemptions that create spaces of data processing-freedoms for individuals and Member States. These provisions also put emphasis on the need to appreciate the factual circumstances in which the processing is taking place. Based on this contextual approach, the scope of the GDPR can be envisaged in a functional manner in light of the facts of each case. This, in turn, allow DPAs and the CJEU to interpret and apply the GDPR in a meaningful way, taking into account all the relevant circumstances. As a result, a balance can be maintained between the FRO and IMO of the GDPR, as well as between private and public interests. It is the conclusion of the author that the provisions on the scope of the GDPR, as well as its limitations, enable the competent authorities to both preserve and reinforce the functionality of EU data protection law.

5.1.1.2. With respect to the substance of the GDPR

As discussed in Section 3.2 of this study, the substance of the GDPR is composed of three main panels: (1) the principles of data processing; (2) the rights of the data subjects; and (3) the obligations of controllers. Each of these panels contain different provisions that allow data subjects, DPAs or other concerned actors to enforce the FRO of the GDPR in a manner that can be considered particularly convenient. This high level of convenience stems from the following factors in particular:

- a) As far the **principles of data processing** are concerned:
 - i. The key principles of data processing are broadly phrased, which allow for **interpretative flexibility** when assessing whether a data processing practice or a DDT may be violating the rights and freedoms of data subjects. Such interpretative flexibility is undeniably an advantage for combatting a wide range of potentially harmful data processing practices or DDTs whose effects cannot be directly addressed through the prism of more specific provisions of the GDPR.
 - ii. The principles of lawfulness, fairness and transparency, of purpose limitation, of data minimisation, of data security and of accountability have primarily at heart the protection of the interests, rights and

¹⁶⁰² Purtova, N. (2018). *op. cit.*

freedoms of the data subjects. By contrast, none of these principles is primarily concerned with the facilitation of data flows among EU Member States. The principle of fairness, in particular, is attached to the reasonable expectations of data subjects, and can thus be used for combatting processing practices that could appear compliant in theory but still affect data subjects in a way that is not considered 'fair' in practice, taking into account the relevant circumstances of each case, including the imbalance of powers that often characterizes relations between data subjects and controllers. These principles were thus primarily **designed to contribute to the fulfilment of the FRO** of EU data protection law rather than its IMO.

- iii. The function of these principles is **not limited to ensuring the respect of the right to privacy or data protection of individuals** but extends to other rights and freedoms. These principles thus contribute to the inherent *multi*-functionality of data protection law. The principle of data minimisation, for example, may prevent controllers from collecting and processing unnecessary data, including data on gender, religion or sexual orientation, which may both benefit the right to privacy of individuals, as well as their right not to be discriminated on the basis of protected characteristics.
 - iv. Among these principles, the principle of accountability, which obliges controllers and processors to be able to demonstrate compliance with EU data protection law, is particularly functional, in the sense that it shifts the **burden of proof** of a potential violation from the data subjects to the controllers and processors themselves.
- b) As far as the **rights of the data subjects** are concerned, although it is undeniable that each right increases the effectiveness of data protection law by empowering individuals against controllers and processors, they could have become dysfunctional if difficult or inconvenient to exercise in practice. Several provisions of the GDPR contribute to the functionality of these rights in the following ways:
- i. By default, **no formal requirements** may be imposed on the data subjects by controllers or processors when the former exercise their rights; a simple email, letter or even an oral request can suffice to exercise these rights, without the need to fulfil any formal requirement or pay a fee upfront.
 - ii. There is **no substantial requirement** that could bar data subjects from exercising their rights vis-à-vis a controller or processor. In particular,

data subjects can exercise their rights without having to prove any particular harm caused by a processing activity or justify their action; an alleged lack of compliance suffices. From the perspective of the FRO of the GDPR, this can be considered as an important factor of functionality, in the sense that data subjects can activate any of their data protection right without having to provide any *prima facie* evidence of an interference with their interests, rights or freedoms.

- iii. Data subjects can exercise their rights without having to be knowledgeable about the applicable law. There is, so to say, **no need to be an expert**. In particular, data subjects can object to the processing of their personal data, request their erasure or ask for information about an AIDM (among others) without having to refer to the applicable GDPR article. Controllers, on the other side, have to facilitate the exercise by data subjects of their rights, for example by providing them with a standardised form or by ensuring that a direct communication channel exists between the data subjects or their DPO.
- iv. The **right to information** can be particularly convenient, as it allows data subjects to gather additional information on the nature and extent of the processing activity conducted by the controller or processor, thereby allowing the data subjects or their representatives to conduct **mini-fishing expeditions**. In addition, a lack of clear and complete information or a disappointing answer from a controller can in itself give rise to a claim.
- v. Where a data subject submits a request by electronic means, the answer from the controller should also be given by electronic means, unless otherwise requested by the data subject. This guarantees both the **convenience and promptness of the communications** between the data subject and the controller, which in turn increases the ease with which data subjects can exercise their rights.
- vi. As a general rule, all communications and any actions taken by a controller following a data subject's request must be provided **free of charge**. Data subjects can thus exercise their right to information, access, rectification, erasure, objection, or even their right to a human intervention without being charged for the associated services. This also increases the functionality of the framework since it allows data subjects to exercise their rights whenever they see fit, without being deterred by the cost that this could imply for them in the future.
- vii. Controllers are obliged to provide data subjects with information on the action that they will take without undue delay and in any event within

one month of receipt of the request. If the request is particularly complex, the controller is allowed to extend that period by two further months but must inform the data subject of this delay, together with its reasons. These **strict deadlines** increase the functionality of the GDPR by forcing a reaction on the part of the controller – even if it leads to the rejection of the request, and the potential intervention of a DPA.

- viii. In the event the controller is of the opinion that it cannot respond positively to the request of a data subject, it must inform the latter of their **right to lodge a complaint** with a DPA. Data subjects are thereby aware that they may challenge the decision of the controller through the intervention of a DPA, i.e., without any substantial personal investment in terms of time or financial resources. This mandatory mention can be seen as another factor of functionality of the GDPR, given that investing additional time or money could otherwise deter many individuals from pursuing their claim.
- c) As far **the obligations of controllers and processors** are concerned, the following provisions in particular can be seen as actively contributing to the multi-functionality of the GDPR for the fulfilment of its FRO, as they put at their heart the need to prevent violations of the fundamental rights and freedoms of data subjects:
- i. With respect to the **lawfulness of the processing**, the fact that controllers may not process personal data when necessary for the purposes of their own interests – even if legitimate – where these interests are overridden by the rights and freedoms of the data subjects (without such interests, rights or freedoms being limited to privacy matters).
 - ii. The fact that most controllers undertaking significant processing activities have to appoint an internal compliance officer, i.e., **a DPO**, and the fact that the supervisory and advisory role of DPOs is accentuated in all situations where the fundamental rights and freedoms of data subjects (including non-privacy related rights) could be threatened by a new DDT or processing practice.
 - iii. The fact that controllers must maintain an up-to-date **record of processing activities**, in line with the principle of accountability, which increases the **convenience** with which DPAs may review these activities and ensure their compliance, including where it appears that a data processing activity could be detrimental to the interests, rights or freedoms of data subjects.

- iv. The fact that controllers must, when implementing any new processing activity, consider all alternatives to ensure **data protection by design and by default**, so as to **prevent any harmful effects** on the interests, rights and freedoms of data subjects (without such interests, rights or freedoms being limited to privacy matters).
- v. The fact that controllers must conduct a **DPIA** every time that an envisaged data processing practice, especially those using a novel DDT, *is likely* to result in a high risk to the rights and freedoms of the data subjects, and the fact that controllers must consult the competent DPA if it appears from the results of the DPIA that the absence of mitigating measures *would* result in a high risk, without this risk being confined to a interference with the right to privacy or data protection *per se*.
- vi. The fact that **AIDM** is more strictly regulated under the GDPR because of the potential harmful effects that fully automated decisions can have on the interests, rights and freedoms of data subjects, and the fact that controllers have additional obligations if an AIDM is taking place, including the obligation to highlight the existence of this AIDM, the obligation to inform the data subjects about the logic and consequences of the automated decision, and the obligation to provide them with the opportunity to express their point of view or obtain a human intervention, among others.
- vii. The fact that the **relations between joint-controllers, controllers and processors**, and the **transfers of personal data outside of the EU/EEA** are regulated with the specific aim of avoiding a dilution of responsibility across the processing chain and maintaining an adequate level of protection of the fundamental rights and freedoms of data subject in the context of the processing of their personal data, regardless of the jurisdiction concerned.

It is undeniable that each of these principles, rights and obligations contribute to the fulfilment of the FRO of the GDPR both in a preventive and corrective manner. *On the preventive side*, many of these provisions indeed put controllers and processors under the obligation to ensure that the processing activities that they envisage to conduct do not create interferences with the rights and freedoms of data subjects, and that the level of protection guaranteed by the GDPR does not diminish in the event personal data are being transferred, or part or whole of the processing activities are being delegated to third parties. *On the corrective side*, many of these provisions can also be leveraged by data subjects, DPAs, not-for-profit entities or competent authorities *a posteriori* to force controllers and processors either to put an end to unlawful data processing practices, or to adjust them so that they become

compliant with the GDPR, i.e., so that they do not disproportionately interfere with data subjects' interests, rights or freedoms.

The GDPR does not limit the applicability of these rules to concerns over privacy, but refer to the interests, rights and freedoms of data subjects in general. As a consequence, these rules are multi-functional in the sense that they can be invoked in a wide variety of situations, including against unlawful e-recruiting practices that can lead to discrimination, or against harassing behaviours on the internet that can harm the dignity or mental integrity of the victim(s), as explored in Chapter 4.

In parallel, many safeguards and facilitation mechanisms provided under the GDPR have been specifically designed to increase the convenience with which the framework can be used, including, in particular, the principle of accountability that puts the burden of proof on controllers, the deadlines imposed on controllers to address data subjects' requests, the possibility for data subjects to file a complaint with their DPA at no cost, or the possibility for NGOs to bring a claim on behalf of data subjects, to name a few. Overall, it is undeniable that these safeguards and facilitation mechanisms make EU data protection law particularly convenient to use for defending data subjects' fundamental rights and freedoms against potentially harmful DDTs or data processing practices.

It has also been found that, if each of these provisions were to be considered alone, they may not be sufficient in ensuring the effective protection of data subjects' rights and freedoms in a functional way. As illustrated through various examples in this thesis, however, a key-factor of the functionality of the GDPR resides in the fact that these principles, rights and obligations can be combined to form together a solid triptych, with each panel reinforcing the two others. The legal narrative that derives from this triptych is itself deeply embedded in the FRO of EU data protection law. This is particularly reflected in the fact that most of these provisions are primarily concerned with the protection of the fundamental rights and freedoms of data subjects, rather than the free flows of personal data. Combining different provisions of this PRO-triptych, read in light with the Charter, can further contribute to the unwinding of additional rights or obligations, and thus enhance the overall level of protection of data subjects, as illustrated by the *Google Spain* case, where the CJEU concluded that data subjects had a 'right to be forgotten' against search engines, based on the principle of storage limitation read together with the right to have incorrect data erased. Hence, it is the concluding opinion of the author of this study that the creative combination of various provisions of the PRO-triptych, read in light of the Charter, has the potential to further unlock the full multifunctionality of the GDPR, for the benefit of various fundamental rights and freedoms in the digital sphere, regardless of the sectors or areas concerned. This would include the assemblage of provisions for combatting various novel and sometimes harmful DDTs or data processing practices, such as online harassment, unlawful surveillance,

opaque profiling techniques, or undue discrimination arising from the use of DDTs in various fields, such as e-recruitment, e-justice or e-banking, to name a few.

5.1.1.3. With respect to the supervision and sanction system of the GDPR

Within the third pillar of functionality of the GDPR, it is concluded that the following provisions in particular contribute to the overall convenience of the framework by facilitating the detection of violations and the enforcement of data protection rights, to the benefit of the FRO of EU data protection law:

- i. The facts that data subjects may trigger an enforcement chain by bringing a violation to the attention of a DPO, a not-for-profit entity or a DPA, without having to invest any significant personal resources (Article 77 and 80 GDPR).
- ii. The fact that data subjects may choose between lodging a complaint with a DPA in the Member State of their habitual residence, place of work or place of the alleged infringement (Article 77(1) GDPR).
- iii. The fact that DPAs are under the obligation to facilitate the filing of complaints, for example by providing an online form on their website for that purpose (Recital 141 and Article 57(2) GDPR).
- iv. The fact that DPOs, despite being subject to strict obligations of confidentiality and secrecy with respect to the data processing practices of their controller or processor, may still address their concerns to a DPA in the event their recommendations or opinions are being disregarded, and can therefore play the role of compliance informers (Article 39(1)(e) GDPR).
- v. The fact that not-for-profit entities – especially entities already specialised in the protection of fundamental rights and freedoms – may be mandated by data subjects in the context of a representative collective action to put an end to a violation (Article 80(1) GDPR).
- vi. The fact that not-for-profit entities can also decide to act against a violation of the rights of data subjects, independently from any specific mandate, in any Member State providing for this possibility (Article 80(2) GDPR).
- vii. The fact that DPAs have been given extensive investigative and corrective powers to fulfil their main task, which has been explicitly spelled out as ensuring the protection of *“the fundamental rights and freedoms of natural persons in relation to processing”*, including DFR (Article 51(1) GDPR).

- viii. The fact that data subjects or not-for-profit entities can bring an action against a DPA that would not properly fulfil its tasks, so that DPAs are being held accountable for their (lack of) actions (Article 78 GDPR).
- ix. The fact that data subjects, or a not-for-profit entity on their behalf, may decide to submit a case before the courts of the Member State where the controller or processor has an establishment or where the data subject has his, her or their habitual residence (Article 79(2) GDPR), either before, during or after the intervention of a DPA.
- x. The fact that co-controllers are considered jointly liable before national courts and may each be ordered to compensate the data subject(s) in full (Article 82(4) GDPR), thereby facilitating the right to an effective remedy of data subjects.

Once again, the facilitation mechanisms provided under the GDPR to challenge potentially harmful data processing practices undoubtedly contribute to the functionality of the framework. More generally, it must be noted that EU data protection law is characterised by the diversity of the actors that can take an active role for ensuring compliance. A violation may indeed be picked up by a data subject, a DPO, a not-for-profit entity, a DPA or any other competent authority. The more actors are involved, the greater the chances of infringements being detected.

In parallel, the fact that these actors may choose between different enforcement paths (mainly, (i) addressing a request directly to a controller or a DPO on the basis of data subjects' rights, (ii) filing a complaint with a DPA, or (iii) bringing a violation to the attention of national courts) allow them to strategically opt for the most convenient and/or adequate path, depending on the circumstances of the case. Strategic enforcement may include different considerations, such as costs, speediness, likelihood of an amicable settlement, benefit of involving a not-for-profit, etc., to increase the chances of a successful outcome. Hence, the decentralised enforcement system of the GDPR does not only increase the chances of detecting a violation, but also the chances of having it fixed. For all these reasons, this multi-actor decentralised enforcement system can be considered as a horizontal factor of the effectiveness and functionality of the GDPR with respect to its FRO.

Yet, it must be acknowledged that exercising and enforcing data protection rights can remain a challenge in practice, mainly due to external factors impeding the effective enforcement of the GDPR at the national level, such as the lack of human and financial resources of DPAs, as well as diverging national procedural rules, which also render the cooperation among DPAs in cross-border cases particularly difficult, among others. All these issues are accentuated by the general slow pace of the

administrative and judicial system of Member States, which contrasts with the fast changes in data processing practices and DDTs.¹⁶⁰³

Although the scope of this study is limited to the identification of *internal* factors of (dys)functionality at the EU level with respect to its FRO, it has been showed that some of the gaps left by the GDPR can in some instances be regarded as *semi-internal* factors of dysfunctionality. Thus, the author will still spell out some specific recommendations on how to fill these gaps to further enhance the multi-functional nature of the GDPR, here below.

5.1.2. Summary recommendations on how to preserve and further enhance the multi-functionality of the GDPR

This study has shown that the GDPR contains many multi-functional provisions designed to serve the fulfilment of its broad FRO. Yet, the author of this study has also identified specific elements within these provisions that could, overall, hinder the overall functionality of the GDPR with respect to its FRO. This Section will recall the main factors of potential dysfunctionality of the GDPR, as identified throughout this study, and summarise the recommendations made in this respect, with a view of preserving or enhancing the effectiveness and the multi-functional nature of the GDPR.

For the sake of clarity and conciseness, these twelve recommendations will be presented in the form of a table. The table itself will be structured around the three structural pillars of the GDPR: its scope, its substance and its supervision & sanction system.

TABLE 12

Summary of the recommendations of the author as to the measures to adopt or maintain to further consolidate the effectiveness and functionality of EU data protection law in the future, including its secondary functionality.

N°	Matter	Description of the issue	Recommendations
I. Regarding the scope of the GDPR			

¹⁶⁰³ See in particular, Massé Estelle (2022). Four years under the EU GDPR. How to fix its enforcement. Access Now. <https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf>

1.	Material scope of the GDPR - Potential merger of Article 7 and 8 of the Charter	The quest for consistency between the ECHR and the Charter may lead to a merger of Article 7 and 8 of the Charter and restrict the application of Article 8 of the Charter to situations where the right to privacy of individuals would be infringed. This, in turn, would prevent the CJEU from interpreting or appreciating the validity of EU law in light of Article 8 of the Charter in an autonomous way, and restrict the scope-extending dialogue that exists between EU primary and secondary law.	The CJEU should clearly distinguish the scope of Article 7 and 8 of the Charter and recognize that Article 8 ECH has not one but two distinct equivalent provisions under the Charter. This would enable the CJEU to continue appreciating the validity or interpreting EU law in light of Article 8 of the Charter in an autonomous manner, i.e., without having to appreciate whether the right to privacy of an individual has also been interfered with. That way, the dialogue between the Charter and EU secondary law can continue reinforcing the scope of data protection-related legislation, put limit to interferences with the fundamental rights of data subjects, and reveal the existence of associated rights, as the case may be (e.g., the right to be forgotten).
2.	Material scope of the GDPR - Unclear borders of the household exemption in the context of semi-private processing	Cyberbullying, online defamation, doxing, revenge porn, and other types of harmful processing are proliferating on the internet. Because of the (partly) inter-personal nature of some of these processing practices, it can be difficult to determine whether the GDPR applies to them or whether the household exemption brings them outside of its scope. In particular, some DPAs appear reluctant to handle cases where the processing is conducted by individuals in a semi-private context.	The borders of the household exemptions should be further clarified with respect to semi-private processing of personal data. In particular, due regard should be paid to the following elements: (1) whether the personal data were made (at least partially) public or shared with individuals that are not part of the private sphere of the controller; (2) whether there was an absence of relation and/or communication between the controller and the victim prior to the litigious processing; (3) whether the controller allowed or encouraged individuals within his/her private sphere to spread the data beyond his/her private sphere. If the answer to one or more of these questions is positive, it should be considered that the household exemption does not apply, thereby allowing the data subject to hold the controller accountable for his or her action under the GDPR.
3.	Material scope – Unclear borders of the exception for matters falling outside of EU law	Some DPAs or courts tend to question the applicability of the GDPR to the processing of personal data in the context of activities that <i>relate</i> to the organization of the state, public security, defense or State security based on Article 2(2)(a) GDPR (i.e., matters	The public law exception provided in Article 2(2)(a) GDPR should be interpreted restrictively, in line with the case-law of the CJEU, so as not to deprive data subjects from the protective scope of the GDPR. To determine whether a processing practice falls outside of EU law because conducted for the purpose of

		falling outside of the scope of EU law), including, for example, when private actors are processing personal data that could later be used or serve a public interest.	public security, defense or State security, the factual elements of the case should be considered. In particular, the two following elements should in any case <i>prevent</i> Article 2(2)(a) GDPR from applying: (1) when private actors that were not specifically mandated by state authorities are processing personal data, even if such processing relates to a public matter (e.g. elections) or could (later) serve a public interest (e.g. information gathering for surveillance purpose) (2) when the processing in question was not specifically initiated <i>for the purpose</i> of public security or defense by a state authority, but is or could be extended to that purpose.
4.	Extra-territorial scope of the GDPR - No designation of an EU representative by foreign controllers	<p>Foreign controllers that offer goods and services to data subjects located in the EU or monitor their behaviors fall within the territorial scope of the GDPR and must normally designate a representative in the EU to facilitate the communication between them and data subjects/DPAs.</p> <p>If this obligation is not respected, however, it becomes difficult for DPAs to enforce the GDPR against a foreign controller conducting unlawful processing practices. The GDPR could become dysfunctional if foreign controllers completely disregard these rules and consider themselves beyond of the reach of EU law/DPAs.</p>	<p>For controllers offering goods and services to data subjects in the EU, DPAs should further encourage the development of certification mechanisms, data protection seals or marks specifically designed to encourage compliance by foreign controllers. Such certification would only be delivered if it is proven that the foreign controller has indeed established a representative in the EU, as required by the GDPR. This would also allow data subjects to quickly assess the level of data protection of relevant products and services offered by foreign controllers, while providing a competitive advantage to foreign controllers that have designated a representative in the EU. DPAs should promote and raise awareness on these data protection certification, marks or seals in information campaigns targeted at data subjects. In the long term, this could prevent situations where a DPA would have to initiate (costly) proceedings against a controller in a foreign jurisdiction because the latter would have failed to establish a representative in the EU, does not respond to the DPA or fails to respect its injunctions in this respect (e.g. injunction to the foreign controller to provide information and/or to establish an EU representative).</p> <p>For foreign controllers that are monitoring the behavior of data</p>

			<p>subjects in the EU but have failed to appoint a representative, and do not respond to the requests or injunctions of DPAs, the latter should also adopt a strict approach based on transparency, consisting in issuing a warning against the concerned controllers, publicizing such warning (for example, on their website) and raising awareness among data subjects on the risk associated with sharing data with these controllers. Black-listed controllers would lose in credibility and be more pressured to comply. This “name, blame and shame” strategy should not prevent DPAs to also initiate proceedings against non-compliant foreign controllers directly in the jurisdiction where the latter are established.</p>
II. Regarding the substance of the GDPR			
5.	Lawfulness – legal basis – self-imposed or construed ‘contractual necessity’	<p>The notion of contractual necessity is often appreciated based on the contractual terms unilaterally defined by controllers. The issue is that controllers often put in place data processing practices that allow them to fulfill their contractual obligations in a cost-effective manner, with little or no regard for data subjects’ rights or interests. If this approach is not questioned, any type of processing operation could be regarded as lawful simply because it would facilitate the conclusion or performance of contracts by controllers. This could lead to situations where controller can artificially create a situation of contractual necessity, to the detriment of the rights or freedoms of data subjects, including consumer protection.</p>	<p>Contractual necessity should be appreciated based on objective criteria rather than the economic interest or the subjective appreciation of controllers. For that purpose, DPAs should analyze whether the processing operation at stake is truly a condition <i>sine qua non</i> for the conclusion or performance of a contract, or whether less intrusive alternatives would exist, keeping in mind the FRO of the GDPR. For example, an insurance company should not be able to rely on contractual necessity to justify the use of an AIDM simply because it would facilitate the conclusion or performance of insurance contracts or decrease their operational costs. Should there be a doubt as to the true ‘necessity’ of a processing operation for the performance of a contract, controllers should rely on another legal basis, such as the consent of the data subjects.</p>
6.	Lawfulness – legal basis – application of Article 6 GDPR instead of Article 9 GDPR	<p>When various personal data are being processed, the lawfulness of such processing operation is sometimes appreciated on the basis of Article 6 GDPR, although the dataset also includes (a</p>	<p>When DPAs, national courts and other competent authorities are requested to appreciate the lawfulness of a processing operation on a specific dataset, they should first determine whether the dataset in question may not include <i>sensitive</i> personal data, in</p>

		minority of) sensitive data. When a DPA overlooks the presence of sensitive data within a dataset, individuals are deprived from the higher level of protection foreseen by Article 9 GDPR for the processing of sensitive data.	accordance with the interpretation given by the CJEU. If that is the case, Article 9 GDPR should be applied to the entirety of the dataset, or at least to the portion of the dataset that includes sensitive personal data, if the latter may be distinguished.
7.	AIDM – obligation to understand and be able to explain the logics of the algorithm	More and more DDTs relying on self-learning algorithms are being used in various sectors. The opacity of self-learning algorithms may however lead to situations where a controller is unable to explain how or why a certain automated decision was taken about a data subject. This could lead to situations where data subjects are unaware or unable to understand automated decisions taken about them or challenge their accuracy or fairness. This would also imply a breach of the principle of transparency and of the obligation of controllers to inform data subjects about the logic involved in an AIDM pursuant to Article 13(2)(f) GDPR.	DPAs should adopt a strict reading of Article 13(2)(f) of the GDPR and require controllers to only use self-learning algorithms or similar DDTs when the algorithmic process in question can be analyzed, and when its logic can be explained to the data subjects. Even if such a strict reading may prevent the use of some DDTs under the GDPR in the short term, this would steer transparency-oriented technological developments in the long-term, for the benefit of data subjects’ rights and freedoms.
III. Regarding the supervision and sanction system of the GDPR			
8.	Perceived lack of competence or proficiency of DPAs to handle data protection cases with fundamental rights issues	Some DPAs seem reluctant to handle complaints or issue binding decisions with respect to disputes where multiple fundamental rights and freedoms conflict with each other. For example, in a case of online defamation on social media, the Icelandic DPA preferred to dismiss the complaint and refer the concerned parties to the national courts, despite having confirmed that the GDPR was applicable to the litigious processing, because it did not consider itself competent to rule on a case where the right to data protection of the complainant was conflicting with the freedom of	As far as competence is concerned, DPAs should be under the obligation to make full use of their investigative and corrective powers <i>especially</i> in cases where fundamental rights issues arise. This is in line with their competence and explicit tasks as defined in the GDPR. National law should not restrict but rather confirm their competence in this respect. DPAs remain in any case subject to the scrutiny of national courts, including their Member State’s constitutional court, as the case may be. As far as proficiency is concerned, in order to be able to deal with complex cases where multiple fundamental rights or freedoms conflict with each other, the permanent staff of DPAs should include experts in the field of data protection law and fundamental

		expression of the controller.	rights law. The permanent staff of DPAs should also receive regular training on important aspects of data protection law and fundamental rights law for the purpose of enforcement.
9.	Lack of human and financial resources of DPAs	A general issue that impacts both the effectiveness and functionality of data protection law in practice is the lack of human and financial resources allocated to DPAs to handle complaints and fulfill their other tasks. This issue is likely to be aggravated if the secondary functionality of EU data protection law is exploited to its fullest extent, as this could lead to a drastic surge in data protection cases in the future.	Member States should provide DPAs with additional financial and human resources, so as to allow them to effectively fulfill their tasks, including for conducting investigation, handling complaints and adopting corrective measures against controllers as necessary and within a reasonable time. Whether the required financial or human resources have been allocated to DPAs should be appreciated on the basis of their annual report, and in particular on the basis of the ratio of cases that have been effectively handled by them (i.e., cases for which a binding decision <i>other</i> than a rejection or a dismissal has been issued).
10.	Lack of proactive investigation into hidden data processing practices	Because of various phenomena or characteristics inherent to data processing practices or DDTs, such as <i>dissimulation</i> , <i>escalation</i> or the <i>opacity of algorithmic tools</i> , unlawful processing practices can remain hidden from the public eye despite having a deep impact on society. Only proactive investigations into these practices would allow DPAs to uncover potential infringements. This is particularly the case with respect to data processing practices that do not require the active input of data subjects (and may thus remain hidden from them), as well as with respect to complex algorithmic decision-making tools (whose functioning, scope or impact may not be perceivable for each data subject individually).	DPAs should be aware of this issue and use their powers to regularly start ex-officio investigations in order to uncover and assess the lawfulness of otherwise hidden data processing practices. In order to capitalize on their efforts, a sector-oriented approach should be adopted (e.g., investigative campaign into e-recruiting tools; investigative campaign into automated moderation system on social media; investigative campaign on the use of biometric identification system by banks for AML purpose; etc.).
11.	Absence of clear and mandatory communication channel	DPOs have no coercive power and can thus not force organizations to adopt their advice or recommendations with a view of complying with	A safe channel of communication should be established between DPOs and DPAs, so that DPOs may turn to DPAs in the event their organization repetitively ignores their advice and

	between DPAs and DPOs	the GDPR. This may lead to situations where the advice or opinions of DPOs could be systematically disregarded even when the latter would have pointed out serious infringements of the GDPR and suggested solutions.	knowingly continues to act in breach of the GDPR. For more certainty, this safe channel of communication should be accompanied by an obligation for DPOs to submit a report to the competent DPA each time a processing activity is put in place or maintained by their organization <i>despite</i> their explicit contrary opinion (e.g. AIDM having discriminatory effects ; intrusive tracking of customers without proper information notice; etc.), or each time an organization fails to take a certain action despite the advice of their DPO (e.g. failure to report a data breach; failure to include the DPO in project management meetings; etc.).
12.	Divergences in procedural rules	Another general issue that negatively impacts the effective enforcement of EU data protection law is the existence of divergences in national (procedural) law. The gaps left by the GDPR in this respect may be considered as semi-internal factors of dysfunctionality. Guidelines published by the EDPB with a view of improving enforcement at the national level are non-binding and can thus be disregarded by national DPAs. As a result, the enforcement of the GDPR remains sub-optimal and unequal across the EU, which is detrimental to the FRO of the GDPR in general.	Clearer and harmonized procedural rules should be adopted at the EU level to better frame enforcement at the national level. This would include, in particular, the harmonization of the following procedural aspects: (1) maximal admissibility requirements for complaints lodged with a DPA (e.g. no statute of limitation ; no formal requirement with respect to the signature of the complaint; etc.) ; (2) a clear obligation to issue a binding decision for every complaint, regardless of the nature of the decision (dismissal, reception or acceptance of the complaint in part or in whole); (3) stricter procedural deadlines to (i) declare a decision admissible, (ii) decide whether it is necessary to conduct an investigation, and (iii) issue a binding decision; (4) specific procedural rules to improve the communication and inclusion of DPAs in the context of the OSS mechanism; (5) the determination of specific procedural rights that must be granted to data subjects and controllers throughout the procedure, such as the right to be heard and the right to access file documents.

5.2. FINAL REFLECTIONS AND CONCLUSIONS ON THE APPARENT SHORTFALL, LEGITIMACY AND DESIRABILITY OF THE SECONDARY FUNCTIONALITY OF EU DATA PROTECTION LAW

The author of this study will now present her final conclusions with respect to the apparent shortfall of the secondary functionality of EU data protection law, and on

whether exploiting the secondary functionality of the GDPR should be regarded as legitimate and/or desirable for the future.

5.2.1. Final reflection and conclusion on the apparent shortfall of the secondary functionality of EU data protection law in light of the case-law of the CJEU

The broad scope, convenient safeguards and facilitation mechanisms available under the GDPR contribute to its functionality, which may in turn explain why the GDPR is being so popular among data subjects, not-for-profit entities or legal professionals for defending a multiplicity of interests, rights and freedoms. This can also explain why the GDPR is increasingly being relied on to address various concerns, including non-privacy-related concerns that had not been specifically foreseen by the EU legislator back in 1995. The two cases discussed in the Introduction of this study (one involving a conflict between a bank and a former client regarding access to documents; the other regarding a conflict between two UBOs and the Luxembourg financial authority regarding the publication of their home address in a public register), as well as the various cases discussed in the fourth Chapter of this study (in particular with respect to combatting some forms of online harassment or e-recruiting practices) are illustrative of this almost 'enthusiastic' use of the GDPR, and the diversity of fundamental rights and freedoms that can benefit from it. Many other areas could have further been explored to test the multi-functionality of the GDPR. The conclusion would however remain the same: overall, there is no doubt that, as soon as a DDT is being used, or as soon as a practice involves the processing of personal data, such DDT or practice will most likely fall under the scope of the GDPR, have to comply with its high standards in terms of fundamental rights protection, and be subject to the scrutiny of the various actors having an interest in ensuring its enforcement.

This conclusion could however be questioned in light of the case-law of the CJEU, which tends to show that EU data protection law is still mainly being interpreted or applied for the benefit of the right to privacy and the right to personal data protection. Indeed, as summarised in the table under Section 2.3.4.1, Articles 7 and 8 of the Charter have so far undeniably been the main beneficiaries of this framework, with a large majority of CJEU judgments being expressly concerned with the right to privacy and/or data protection. One could thus conclude that, while the primary functionality of EU data protection law has already been evidenced at the EU level, its secondary functionality remains mostly theoretical.

In light of the various harmful data processing practices that proliferate in the digital sphere, it would be difficult to argue however that the main cause behind this shortfall would be the quasi-absence of violation of DFR in the context of data processing. Indeed, this study has shown that modern data processing practices are so widespread and diverse in today's society that they can virtually affect *all* the

fundamental rights and freedoms of the data subjects. In the opinion of the author, the fact that the case-law of the CJEU in the field of data protection still appears narrowly focused on the need to protect privacy and data protection is thus primarily a reflection of the past, or rather of the slow pace of justice in general. This delay is more logically significant in the field of data protection, given that the rapidity of technological developments notably contrasts with the slow pace of the judicial system. The GDPR itself acknowledges that “[r]apid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.”¹⁶⁰⁴ Among these rapid technological developments, one may cite, for example, the rise of social media and the development of smart algorithms to support or replace human decision-making. These processing practices that were not technically possible ten years ago have now become (almost) common – and so are their consequences for individuals’ rights and freedoms.

In parallel, one must also admit that the world did not turn into a dystopian reality ruled by technology, as pictured in many apocalyptic discourses, ominous declarations or works of fiction.¹⁶⁰⁵ Reliance on algorithmic system such as COMPAS or HireVue video interviewing software, for example, is far from being generalised, and has altogether engendered more mistrust than enthusiasm for novel DDTs. Journalists and scholars in particular are keen to analyse and highlight any adverse consequence or negative impact that technology can have on individuals, as highlighted by most of the references of this study. Although it is important to discuss and palliate the risks posed by futuristic or novel DDT, one must not forget that, in today’s world, the main risks that exist in relation to data processing are still mainly privacy-related risks. As a result, it is likely that the primary functionality of the GDPR will remain more apparent than its secondary functionality. This situation may however evolve in the future, as already reflected in the growing number of cases at the level of the CJEU where EU data protection law is being interpreted for the benefit of a DFR, such as non-discrimination, freedom of expression or the right to an effective judicial remedy (cf. Section 2.3.4.1).

Finally, another element which may explain the perceived shortfall of the secondary functionality of EU data protection law is the enforcement practices of DPAs. As illustrated in the fourth Chapter of this study, while some DPAs do not hesitate to rely on the GDPR to protect DFR (for example, to protect data subjects against algorithmic discrimination or online defamation), others seem reluctant to do so, usually because of factors that are *external* to the text of the GDPR itself (for example, lack of resources; privacy-oriented enforcement culture; lack of legitimacy

¹⁶⁰⁴ Recital 6 of the GDPR.

¹⁶⁰⁵ One may refer, inter alia, to George Orwell’s book “1984”, Isaac Asimov’s “Three laws of robotics”, movies such as “A.I.”, “I, Robot” or “The Matrix”, and series such as “Love, Death + Robots” or “Dark Mirror”.

under national law; etc.).

Against this background, it is argued that the perceived shortfall in the secondary functionality of EU data protection law does not imply that EU data protection law is ill-fitted for the defence of DFR. Rather, this shortfall may be explained by the following three causes: (i) the slow pace of the judicial process against the rapid development of novel DDTs; (ii) the fact that data processing practices are still mainly posing concerns for the right to privacy and data protection, even if these concerns are increasingly extending to DFR; (iii) the fact that the enforcement and judicial culture of the various bodies in charge of combatting these violations must still evolve and adapt to the broad FRO of EU data protection law. In the opinion of the author of this study, this also means that the secondary functionality of the GDPR is likely to be increasingly exploited in the coming years at the national level, which should in turn render it more apparent at the EU level.

5.2.2. Final reflection and conclusion on the desirability and legitimacy of the secondary functionality of EU data protection law

Throughout this study, the secondary functionality of EU data protection law has been conceptualised and regarded as an inherently positive characteristic, which should be further preserved and enhanced for the benefit of data subjects' rights and freedoms. While some concerns over the far-reaching scope of the GDPR have already been addressed in this study (cf. Section 3.1.1.2, above), the author would like to present her final reflections and conclusions on why it would be both desirable and legitimate to exploit the secondary functionality of EU data protection law to its fullest extent.

As far as **desirability** is concerned, the author of this study believes that exploiting the secondary functionality of the GDPR is not only sensible but also advisable in light of the technological and social developments that took place during the last decade, and their impact on the fundamental rights and freedoms of individuals. Since March 2020 in particular, the COVID-19 pandemic and the repeated lockdowns that it triggered seem to have accentuated the Negroponte shift: many human activities that used to take place in the material world migrated to the digital sphere, mainly because of the necessity to reduce physical contacts. This also encouraged the creation of new DDTs and the forming of new institutional practices and social habits, from the development of contact tracing apps to the wide-spread use of video-conferencing software. In the private sphere, individuals had often no choice but to rely on social media and messaging apps to interact with family and friends. The pandemic was also more generally accompanied by an increased consumption of online services, such as online shopping, banking, coaching, booking, gaming or

streaming services for entertainment purpose.¹⁶⁰⁶ As far as education and employment are concerned, pupils and students made increased use of e-learning tools while employees and other professionals relied on various connected solutions to be able to work from home. In the public sphere, various authorities have also been adopting digital solutions to be able to perform their tasks; many procedures, such as for the issuance of permits or other official documents, the allocation of social allowances, the notification of judgments, or the reimbursement of healthcare costs have been gradually digitalised, in whole or in part.¹⁶⁰⁷ Even after the pandemic, many of these new digital habits have persisted. As a result, the information society has gained considerable ground these last two years.

Besides these horizontal developments, which concern a majority of the population in the EU and have set new standards for everyday life, various ‘niche’ DDTs with AI-components have also been developed along technological innovations in the field of computer sciences. The effects of these niche DDTs on the rights and freedoms of data subjects can be adverse if they are not kept in check. Among these niche DDTs, one may mention, for example, smart algorithms used for screening prospective clients or employees, or for the allocation of work in the gig economy, ‘deep fake’ videos used to spread misinformation or blackmail individuals, wearable biometric monitoring devices for health prevention, anti-fraud detection algorithms in the financial or insurance sectors, or any software or hardware technologies related to the so-called metaverse.¹⁶⁰⁸ Although the use of these niche DDTs has not yet been generalised, they can have a much deeper impact on the data subjects concerned, precisely because of their level of sophistication and novelty. The need to regulate high-impact technologies is reflected in the provisions of the GDPR regulating the use of AIDM and requiring controllers to conduct a DPIA when a processing practice relies on a new technology that can put at risk the fundamental rights and freedoms of the data subjects.

All in all, whether niche or generalised, it cannot be denied that DDTs have become an integral part of the private and professional life of individuals in the EU. This has reinforced both the importance and the vulnerability of digital identities. Or as summarised by Eurostat in their latest report, *“digital solutions can enrich our lives in many ways. But the benefits arising from digital technologies do not come without risks or costs. Some people no longer feel in control over what happens with their personal data and are increasingly overloaded by digital solicitations for their attention. Furthermore, malicious cyberactivity may threaten personal well-being or*

¹⁶⁰⁶ Eurostat. Regional Yearbook. Digital society statistics at regional level. Data extracted in May 2022. Source: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_society_statistics_at_regional_level.

¹⁶⁰⁷ *Ibid.*

¹⁶⁰⁸ Metaverse is a word formed from the contraction of the terms “meta” and “universe”. It either refers to a hypothetical iteration of the Internet as a single, universal and immersive virtual world, or to an interconnected network of different 3D worlds, that individuals can access by wearing virtual reality (VR) or augmented reality (AR) wearable devices, such as headsets. See Ball, M. (2022). *The Metaverse: and how it will revolutionize everything*. Liveright.

*disrupt critical infrastructures and wider security interests.”*¹⁶⁰⁹ It is thus only logical to accompany these changes by keeping in check the impact of these DDTs on individuals with available regulatory tools. The GDPR – mainly because of its broad scope and human-centric approach – has been able to encompass this evolution. Of course, the acceleration of the Negroponte shift also means that the GDPR is likely to apply to a growing number of past, present or future DDTs and data processing practices, which may in turn lead to a sudden surge in complaints against controllers at the national and EU level. As a result, enforcement authorities may soon be overwhelmed in the accomplishment of their tasks if their human, technical and financial resources are not rapidly being increased in line with these changes. Yet, claiming that the secondary functionality of the GDPR is not desirable because of the widespread use of DDTs would be like claiming that traffic rules have become less desirable since more and more people drive a car. In the opinion of author, the opposite is true.

As far as **legitimacy** is concerned, one may further question whether exploiting the secondary functionality of the GDPR is truly legitimate to regulate all types of DDTs or data processing practices, including in situations where *non-privacy* related rights are affected, and/or in situations traditionally envisaged through the prism of criminal law or other legislations (e.g., online harassment, discriminatory e-recruitment, etc.). The perception that EU data protection law may lack the necessary legitimacy to infiltrate these spheres seems to mainly derive from the fact that the EU legislator might have not anticipated or foreseen these situations. As a result, the application of the GDPR to these situations may appear surprising, unintended or non-consensual, and thus illegitimate.

According to the deliberative ideal developed by Jürgen Habermas, the legitimacy of social or legal norms can be appreciated on the basis of the consensus that has led to their adoption or that supports their actual application to specific cases.¹⁶¹⁰ The legitimacy of norms would thus primarily derive from the consent of those governed by them. When the norm in question qualifies as a legal norm, particular attention should therefore be given to the legislative process which has led to its adoption. Without entering the debate on the so-called ‘democratic deficit’ of the EU,¹⁶¹¹ it is generally accepted that EU law is the product of a democratic process, considering, in particular, the fact that most EU directives and regulations are adopted through a

¹⁶⁰⁹ Eurostat. Regional Yearbook. Digital society statistics at regional level. Data extracted in May 2022. Source: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_society_statistics_at_regional_level.

¹⁶¹⁰ Habermas, J. (1996). *Between facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Translated by William Rehg. Oxford: Polity.

¹⁶¹¹ Demetriou, K. (2015). *The European Union in Crisis. Explorations in Representation and Democratic Legitimacy*. SpringerLink; Majone, G. (1998). Europe’s Democratic Deficit. *European Law Journal*, 4:1; Moravcsik, A. (2002). In Defence of the “Democratic Deficit”: Reassessing the Legitimacy of the European Union. *Journal of Common Market Studies*, 40(4):603-634. Follesdal, A. & Hix, S. (2006). Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik. *Journal of Common Market Studies*, 44(3):533-562.

legislative procedure requiring the approval of the European Parliament.¹⁶¹² The democratic debates that precede the adoption of a law, and the representative function of the legislator in that respect, are thus essential components of the legitimacy of legal norms. By analogy, once a law has been adopted, the legitimate use and enforcement of that law in a given situation can be appreciated on the basis of the *express objective* of that law, as spelled out by the legislator, as well as the *acceptance* by the actors concerned of the actual application that is made of the law in practice and over time. In other words, if a law is interpreted, applied or enforced in a manner that contributes to its democratically-defined objective, and in a manner that remains acceptable for a majority of the persons subject to it, it can be assumed that its use is legitimate.

As far as EU data protection law is concerned, it has been shown in the second Chapter of this study that the protection of the fundamental rights of the data subjects is part of the DNA of European data protection law. While, in the 70s, this objective was often narrowly focused on the need to protect the right to privacy of citizens against the processing practices of public authorities, it was gradually extended by national legislators to the private sector, including with a view to protect DFR (cf. Sections 2.1.2 and 2.1.5). In 1995, when the EU legislator adopted its first comprehensive act in the field of data protection, the explicit objective of that act was to *“protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”*¹⁶¹³ Taking this objective into account, it may thus reasonably be argued that, although the right to privacy was indeed envisaged as the main beneficiary of the 1995 Data Protection Directive, the EU legislator had already opened the door to a broader use of that legislation for the purpose of defending other important rights and freedoms against harmful data processing practices. With the adoption of the GDPR, this broad FRO was confirmed in the following terms: *“This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.”*¹⁶¹⁴ Once again, these rules were thus envisaged as a mean to protect the fundamental rights and freedoms of data subjects in general. Several recitals of the GDPR further refer to important social and economic rights that ought to be protected against intrusive or potentially harmful DDTs, thereby confirming that these rules are not exclusively privacy-oriented.¹⁶¹⁵ In the opinion of the author, the broad explicit FRO of the GDPR therefore justifies the use of that legislation any time a data processing practice interferes with an important interest, right or freedom, even when such an interest, right or freedom is not narrowly focused on the right to privacy of the individuals concerned. In other words, the author of this study believes that data subjects can *legitimately* rely on the GDPR to assert various rights and freedoms beyond privacy or data protection, including those supporting

¹⁶¹² As foreseen in Article 294 TFEU.

¹⁶¹³ Article 1(1) of the 1995 Data Protection Directive.

¹⁶¹⁴ Article 2(1) GDPR.

¹⁶¹⁵ Recital 71, 75 and 85 GDPR.

economic, social or personal interests, given that such a use is in line with the explicit objective of that regulation.

As far as consensus is concerned, one must admit however that not all DPAs seem to fully support the secondary functionality of the GDPR. The fourth Chapter of this study has shown in particular the reluctance of some DPAs to handle cases where freedom of expression could be impacted. This reluctance seems grounded in the self-perceived lack of legitimacy of DPAs to impose limitations on constitutional rights. In light of Habermas' theory, the secondary functionality of the GDPR could thus suffer from a shortfall because of the absence of consensus among the actors concerned in this respect, including DPAs. This reluctance is however not generalised. In France, Italy or Spain, for example, the CNIL, the *Garante* and the AEDP are regularly handling requests of victims of online harassment. The Icelandic DPA, by contrast, does not seem to consider itself competent to tackle these types of complaints (Section 4.1.4.2 above). In the opinion of the author, this calls for additional discussions and harmonisation on how DPAs should embrace and rely on the secondary functionality of EU data protection law for handling complaints that are not exclusively concerned with the fundamental right to privacy or data protection. This also calls for a better understanding, by DPAs, of their important role with respect to fundamental rights protection, as well as additional expert knowledge in that field among the staff of DPAs. In other words, for the secondary functionality of the GDPR to further gain in legitimacy, it is important that DPAs understand and reach a consensus on how to best exploit this secondary functionality in line with the FRO and IMO of the GDPR, together with other public actors, as the case may be. The recommendations spelled out here above with respect to enforcement (Section 5.1.1.3) precisely aim at encouraging such developments.

The notion of legitimacy of the law can also be understood in opposition to the notion of abuse of the law. In its common sense, the term 'abuse' is defined as the use of something for the wrong purpose, in a way that is harmful or morally wrong.¹⁶¹⁶ In legal terms, an abuse of law or abusive practices (in French, "*abus de droit*"; in German, "*Rechtsmissbrauch*") is more specifically understood as any "*acts or omissions which do not appear to be unlawful in formal terms but defeat the object or the purpose of the law.*"¹⁶¹⁷ Once again, the notion of abuse must thus be appreciated in light of the objective of the law and its intended effects. For example, one may wonder whether the colleagues of Mrs Lindqvist did not 'abuse' of their right to object to the processing of their personal data by requesting Mrs Lindqvist to delete several pages of her blog. Similarly, one may wonder whether Maximilian Schrems did not abuse of his data protection rights to oppose the transfer of his personal data by Facebook from the EU to the US, which led to the invalidation of

¹⁶¹⁶ See the definitions provided by the online Cambridge dictionary or Merriam-Webster dictionary.

¹⁶¹⁷ As defined under the Proposal for an EU Directive on the protection of persons reporting on breaches of Union law (COM(2018)218 final).

the Safe Harbour and Privacy Shield adequacy decisions. More recently, one may wonder whether gig workers should be able to exercise their right to information or their right to a human intervention to question the manner in which their employer organises their schedule or allocate work to them by relying on algorithmic tools. In the same line, one may question whether wealthy individuals who qualify as UBOs of an investment fund are not abusing of their right to erasure when requiring a public authority to delete their personal address from a public register, with the alleged purpose to ensure the safety of their family. While the first two cases primarily relate to an interference with the right to privacy of the individuals concerned, the two other cases are primarily concerned with fair working conditions, on the one side, and the right to the integrity of the person, on the other side. In the opinion of the author, however, the common element between all these cases is that each time the processing activity at stake was causing an interference with a right or freedom in a way that could arguably be considered as disproportionate by the data subjects concerned. Since the objective of the GDPR is precisely to protect individuals against such disproportionate interferences, it can be considered that invoking its rules was a legitimate attempt by these data subjects.

Ultimately, in order to safeguard the legitimacy of the framework, it is for DPAs and national courts to determine, in each case, how to concretely interpret and apply EU data protection law in line with its dual objective.¹⁶¹⁸ In this respect, the author of this study fully agrees with the opinion of Hielke Hijmans, according to which “[s]uccessful data protection requires effective [DPAs] working in a legitimate manner”.¹⁶¹⁹ In the accomplishment of their long list of tasks, DPAs must thus preserve their independence while seeking to reconcile the IMO and FRO of EU data protection law.¹⁶²⁰ This study has precisely shown that the GDPR leaves room for DPAs to balance the sometimes diverging rights and interests of data subjects and controllers, without giving an absolute or disproportionate weight to one or the other. Indeed, it must be acknowledged that invoking the GDPR will not systematically lead to a situation where the rights and freedoms of the data subjects will prevail over the rights, freedoms or interests of the controllers or processors facing them. There exists, indeed, no radical prohibition or obligation in the GDPR; rather, compliance with general principles or specific obligations must be appreciated on a case-by-case basis, while none of the rights of the data subjects can be considered as absolute. As a result, one can hardly assimilate the GDPR to a weapon of massive destruction,¹⁶²¹ whose use against controllers or processors would be so fatal that its legitimacy could be questioned. Rather, the GDPR can be seen as a toolbox that various actors may decide to open in an attempt to fix or calibrate the scales in which conflicting interests or rights are being weighed.

¹⁶¹⁸ Hijmans, H. (2014). *op. cit.*, pp. 1-2.

¹⁶¹⁹ Hijmans, H. (2018). *op. cit.*, p. 80.

¹⁶²⁰ *Ibid.*

¹⁶²¹ In reference to O’Neil, C. (2016). *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*. Crown Books.

For all these reasons, the author of this study believes that the secondary functionality of the GDPR *can* be exploited and *should* be exploited, in the sense that it is both *desirable* and *legitimate* to explore the many tools that the GDPR has to offer to protect individuals' rights and freedoms, including human dignity, integrity, freedom of expression or non-discrimination, against (potentially) harmful data processing practices in today's digital world.

BIBLIOGRAPHY

Books

- Ashby, William Ross (1956). *An introduction to cybernetics*. London: Chapman & Hall.
- Assimakopoulos Stavros, Baider Fabienne & Millar Sharon (2017). *Online Hate Speech in the European Union: A Discourse-Analytic Perspective*. Springer.
- Ausloos, Jef, Mahieu, René & Veale, Michael (2019) Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10(3):283-309.
- Balboni, Paolo (2019). *Personal data protection as the new competitive edge: Generating socially responsible corporate behaviour*. Maastricht University.
- Barrington Moore, Junior (2018). *Privacy: Studies in Social and Cultural History*. Routledge.
- Bellinger, Andrea and Krieger, David (2018). *Network Publicity Governance. On Privacy and the Informational Self*. Bielefeld: Transcript Verlag.
- Benyekhlef, Karim (1993). *La protection de la vie privée dans les échanges internationaux d'informations*. Montréal : Thémis.
- Bensoussan, Alain, Henrotte, Jean-François, Gallardo, Marc, Fanti, Sébastien & Falque-Pierrotin, Isabelle (2018). *General Data Protection Regulation: Texts, Commentaries and Practical Guidelines*. Mechelen: Wolters Kluwer Belgium.
- Bergt, Matthias (2020). Artikel 79 DSGVO, margin number 24. Kühling & Buchner (eds). *DS-GVO BDSG*. C.H. Beck.
- Besemer, Leo (2020). *Privacy and Data Protection Based on the GDPR: Understanding the General Data Protection Regulation*. Van Haren Publishing.
- Boehm, Franziska (2012). *Information sharing and data protection in the area of freedom, security and justice: towards harmonised data protection principles for information exchange at EU-level*. Berlin: Springer.

- Boehm, Franziska (2019). Article 79 GDPR, margin number 10. Simitis, Hornung, Spiecker & Döhmman (eds). *Datenschutzrecht*. C.H. Beck.
- Cauer, Wilhem (1941). *Theorie der linearen Wechselstromschaltungen*. Akademische Verlags-Gesellschaft Becker & Erler. Leipzig.
- Campbell-Kelly, Martin (2018). *Computer: A history of the information machine, economy edition*. Routledge (3 ed.).
- Chemillier-Gendreau, Monique (1995). *Humanité et souverainetés: Essai sur la fonction du droit international*. Paris: La Découverte.
- Cote, Amanda (2020). *Gaming Sexism: Gender and Identity in the Era of Casual Video Games*. NY University Press.
- Custers, Bart, Calders, Toon, Schermer, Bart & Zarsky, Tal (2013). *Discrimination and Privacy in the Information Society*. SAPERE. Springer.
- Datta, Anumpam, Sharma Divya & Sinha Arunesh (2012). Provable de-anonymization of large datasets with sparse dimensions. Degano P. & Guttman J. D. (eds.). *International Conference on Principles of Security and Trust*. Springer.
- Demers, Valérie (1996). *Le contrôle des fumeurs. Une étude d'effectivité du droit*. Montréal : Thémis.
- De Hert, Paul & Gutwirth, Serge (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.). *Privacy and the criminal law*. Intersentia.
- Dumortier, Jos & Robben, Frank (1995). *Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer*. Brugge: Die Keure.
- Dutton, William & Graham, Mark (2014). *Society and the Internet: How Networks of Information and Communication are Changing our Lives*. M. Graham and W. H. Dutton (eds). Oxford: Oxford University Press.
- Edelstein, Ludwig (1943). *The Hippocratic Oath: Text, Translation and Interpretation*. Baltimore: The Johns Hopkins Press.
- Edo, Anthony & Jacquemet, Nicolas (2013). *La Discrimination à l'embauche sur le Marché du Travail Français*. Paris: Édition Rue D'Ulm.
- Ferguson, Andrew Guthrie (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York University Press.
- Foucault, Michel (1989). *Surveiller et punir : Naissance de la prison*. Paris: Gallimard.

Friedland, Martin (1989). *Sanctions and Rewards in the Legal System: A Multidisciplinary Approach*. University of Toronto Press.

Fuller, Lon (1969). *The Morality of Law*. Yale University Press.

Georgieva, Ludmila & Kuner, Christopher (2020). Article 9: Processing of special categories of personal data. Christopher Kuner (ed.) et al. *The EU General Data Protection Regulation (GDPR): A Commentary*. New York. Oxford Academic, p. 369.

Gillespie, Tarleton (2018) *Custodians of the Internet: Platforms, Content Moderation and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press.

Gong, Shaogang, Cristani, Marco, Shuicheng, Yan & Loy, Chen Change (2014). *Person Re-Identification. Advances in Computer Vision and Pattern Recognition*. Springer.

González Fuster, Gloria (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer International Publishing.

González Fuster, Gloria (2018). Transparency As Translation in Data Protection. Emre Bayamlioglu, Irina Baraliuc, Liisa Albertha Wilhelmina Janssens and Mireille Hildebrandt (eds). *Being Profiled: Cogitas Ergo Sum*. Amsterdam: Amsterdam University Press.

Goodman, Bryce & Flaxman, Seth (2017). EU Regulations on Algorithmic Decision-Making and a 'right to Explanation'. *AI Magazine*, 38(3):50-57.

Gutwirth, Serge (2009). *Reinventing data protection?* Berlin: Springer.

Gutwirth, Serge, Leenes, Ronald, De Hert, Paul de & Poullet, Yves (2012). *European data protection: In good health?* Dordrecht: Springer.

Habermas, Jürgen (1996). *Between facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Translated by William Rehg. Oxford: Polity.

Hess, Burkhard & Mariottini, Cristina (2015). *Protecting privacy in private international and procedural law: European and American Developments*. Baden-Baden: Nomos.

Hildebrandt, Mireille & Gutwirth, Serge (2008). *Profiling the European Citizen. Cross-Disciplinary Perspectives*. SpringerLink

Holm, Anna B. (2012). E-recruitment: the move towards a virtually organized recruitment process. De Juana-Espinosa, S., Fernandez-Sanchez, J.A., Manresa-Marhuenda, E. & Valdes-Conca, J. (eds). *Human Resource Management in the Digital Economy: Creating Synergy Between Competency Models and Information*. IGI Global, Hershey PA.

Hondius, Frits W. (1975). *Emerging data protection in Europe*. Amsterdam : North Holland Publishing Company.

Hijmans, Hielke (2016). *The European Union as Guardian of Internet Privacy*. Springer.

Hijmans, Hielke (2000). Article 1 Subject-matter and objectives. Kuner, C. (ed.) & al. *The General Data protection Regulation (GDPR): A Commentary*. Oxford University Press.

Jahnel, Dietmar (2021). Article 79 GDPR, margin number 29. Jahnel, D. (ed.). *DSGVO*. Jan Sramek.

Jeammaud, Antoine (2006). Le concept d'effectivité du droit. Ph. Auvergnin (ed.). *L'effectivité du droit du travail : à quelles conditions ?* COMPTRASEC.

Kelsen, Hans (1962). *Théorie pure du droit*. Paris : Dalloz.

Kosta, Eleni, Leenes, Ronald & Kamara, Irene (2022). *Research handbook on EU data protection law*. (1st ed.) (Research Handbooks in European Law). Edward Elgar Publishing.

Kosta, Eleni (2020). Article 35 Data protection impact assessment. In C. Kuner, L. Bygrave, C. D., & L. Drechsler (Eds.). *The EU General Data Protection Regulation: A commentary*. Oxford University Press, pp. 665-679.

Kosta, Eleni (2018). The retention of communications data in Europe and the UK. In L. Edwards (Ed.). *Law, policy and the internet*. Hart Publishing, pp. 193-212.

Kotschy, Waltraut (2020). Article 6. Lawfulness of processing. Kuner, C., Bygrave, L. & Docksey, C. (eds). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.

Kreße, Bernhard (2018). Article 79 GDPR, margin number 4. Sydow (ed.). *Europäische Datenschutzverordnung*. Nomos.

Kuner, Christopher, Bygrave, Lee A. & Docksey, Chris (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.

Lajoie, Andrée, Rocher, Guy, MacDonald, Roderick & Janda, Richard (1998). *Théories et émergence du droit : pluralisme, surdétermination et effectivité*. Montréal : Thémis.

Lochak, Danièle, Memmi, Dominique, Spanou, Calliope & Lehinge, Patrick. *Les usages sociaux du droit*. Paris: P.U.F.

Lonza, Andrea (2019). *Reinforcement Learning Algorithms with Python: learn, understand and develop smart algorithms for addressing AI challenges*. Packt Publishing.

Lynskey, Orla (2015). *The Foundations of EU Data Protection Law*. Oxford Studies in European Law. Oxford: Oxford University Press.

Manners, Ian (2000). *Normative Power Europe: A Contradiction in Terms?* Copenhagen Peace Research Institute.

Martini, Mario (2021). Article 79 GDPR, margin number 12. Paal, B. & al. (eds). *Datenschutz Grundverordnung Bundesdatenschutzgesetz*. C.H. Beck.

Mortensen, Torill Elvira & Sihvonen, Tanja (2020). Negative Emotions Set in Motion: The Continued Relevance of #GamerGate. Holt, T. J., Bossler, A. M. (eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Springer International Publishing, pp. 1353–1374.

Mundil, Daniel (2020). Article 79 GDPR. Wolff & Brink (eds). *BeckOK Datenschutzrecht*. C.H. Beck.

Nardell, Gordon (2010). Levelling up: Data Privacy and the European Court of Human Rights. Serge Gutwirth, Yves Poullet and Paul de Hert (eds). *Data Protection in a Profiled World*. Dordrecht: Springer.

Negroponte, Nicholas (1995). *Being digital*. New York: Alfred A. Knopf.

O’Neil, Cathy (2016). *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*. Crown Books.

Ost, François (2010). De la pyramide au réseau? Pour une théorie dialectique du droit. *Presses de l’Université Saint-Louis*.

Pariser, Eli (2012). *The Filter Bubble. How the new personalized web is changing what we read and how we think*. Penguin Random House.

Phillips, Amanda (2020). *Gamer Trouble: Feminist Confrontations in Digital Culture*. Feuilleter.

Quintel, Teresa & Ullrich, Carsten (2020). *Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond*. Petkova/Ojanen (eds.) *Fundamental Rights Protection Online: The Future Regulation of Intermediaries*. Elgar.

Raz, Joseph (1979). *The Authority of Law: Essays on Law and Morality*. Oxford: Oxford University Press.

Roberts, Sarah (2019). *Behind the screen. Content moderation in the shadows of social media*. Yale University Press.

Schmahl, Stefanie & Breuer, Martin (2017). *The Council of Europe: Its Laws and Policies*. Oxford: Oxford University Press.

Schrems, Maximilian (2018). Article 79 GDPR, margin numbers 25 to 28. Knyrim (ed.). *Der DatKomm online. Praxiskommentar zum Datenschutzrecht – DSGVO und DSG*. MANZ Verlag.

Shaw, Malcom (2017). *International law* (8th ed.). Cambridge: Cambridge University Press.

Snowden, Edward (2019). *Permanent Record*. Metropolitan Books.

Suzor, Nicolas (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press.

Svanberg, Konrad (2014). *Decreased Commuting Time and Its Effects on Accessibility and Productivity*. Master's Thesis in Economics. Upsala University Library.

Theodorakis, Nikolaos & Dhont, Jan (2019). *General Data Protection Regulation: For Practitioners*. Cambridge: Intersentia.

Tizzano, Antonio (2008). The Role of the European Court of Justice in the Protection of Fundamental Rights. Arnulf, A., Eckhout, P. and Tridimas T. (eds.). *Continuity and Change in EU Law: Essays in Honour of Francis Jacobs*. Oxford Academic.

Tosoni, Luca & Bygrave, Lee Andrew (2020). Article 4(2). Processing. Kuner, C. (ed.) & al. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, p. 119.

Tridimas, Takis (2000). *The general principles of EC Law*. Oxford EC Law Library.

Troper, Michel (2003). *La philosophie du droit*. Paris : PUF.

Turow, Joseph (2006). *Niche Envy. Marketing Discrimination in the Digital Age*. MIT Press Books.

Tzanou, Maria (2017). *The fundamental right to data protection: normative value in the context of counter-terrorism surveillance*. Oxford: Hart Publishing.

Van Gerven, Walter & Zuleeg, Manfred (1996). *Sanktionen Als Mittel Zur Durchsetzung Des Gemeinschaftsrechts*. Köln: Bundesanzeiger.

Voigt, Paul & Von Dem Bussche, Axel (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

Waldron, Jeremy (2012). *The Harm in Hate Speech*. Cambridge: Harvard UP.

Westin, Alan (1967). *Privacy and Freedom*. New York: Atheneum.

Wolter, Andrä (2015). Massification and diversity: Has the expansion of higher education led to a changing composition of the student body? European and German experiences. In P. Zgaga, U. Teichler, & H. G. Schuetze (Eds.). *Higher education research and policy. Higher education reform. Looking back – looking forward*. Frankfurt: Peter Lang GmbH.

Yeung, Karen, Howes Andrew & Pogrebna, Ganna (2019). Why Industry Self-regulation Will Not Deliver 'Ethical AI': A Call for Legally Mandated Techniques of 'Human Rights by Design'. Dubber and Pasquale (eds.). *The Oxford Handbook of AI Ethics*. Oxford University Press.

Zimbardo, Philip (1969). The human choice: Individuation, reason, and order vs. deindividuation, impulse, and chaos. W. J. Arnold & D. Levine (Eds.). *Nebraska Symposium on Motivation*. Lincoln: University of Nebraska Press.

Zuiderveen Borgesius, Frederik J. (2015). *Improving Privacy Protection in the Area of Behavioural Targeting*. Kluwer Law International.

Journals

Allott, Philip (1998). *The True Function of Law in the International Community*. *Indiana Journal of Global Legal Studies*, 5:391-395.

Albrecht, Jan Philipp (2016). How the GDPR will change the world. *European Data Protection Law Review*, 3:286.

Afzali, Golnar Assadat & Mohammadi, Shahriar (2018). Privacy preserving big data mining: Association rule hiding using fuzzy logic approach. *IET Information Security*, 12(1):15-24.

Aro, Jessikka (2016). The Cyberspace War: Propaganda and Trolling as Warfare Tools. *European View* 15(1):121-32.

Bailey, Ronald (2019). Can Algorithms Run Things Better Than Humans? Welcome to the Rise of the Algocracy. *Reason Magazine*, 50(8):20-26

Baker, Stephanie, Wade, Matthew & Walsh, Michael James (2020). The Challenges of Responding to Misinformation during a Pandemic: Content Moderation and the Limitations of the Concept of Harm. *Media International Australia*, 177(1): 103-07.

Balboni, Paolo, Taborda Barata, Martin, Botsi, Anastasia & Francis, Kate (2019). Accountability and Enforcement Aspects of the EU General Data Protection Regulation: Methodology for the Creation of an Effective Compliance Framework and a Review of Recent Case Law. *The Indian Journal of Law and Technology*, Volume 15(1), 103-254.

Baldwin, Robert, Cave, Martin & Lodge, Martin (2011). *Understanding Regulation: Theory, Strategy, and Practice*. Oxford Academic.

Balkin, Jack (2018). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *UC Davis Law Review*, 51:1149.

Balz, Suzanne Dionne & Hance, Olivier (1996). Privacy and the internet: Intrusion, surveillance and personal data. *International Review of Law, Computers & Technology*, 10(2):219-234.

Barocas, Solon (2014). Data Mining and the Discourse on Discrimination. Proc. Data Ethics Workshop (web version).

Barocas, Solon & Selbst, Andrew D. (2016). Big Data's Disparate Impact. *California Law Review*, 104:671.

Bauman, Sheri, Toomey, Russell B., & Walker, Jenny L. (2013). Associations among Bullying, Cyberbullying, and Suicide in High School Students. *Journal of Adolescence*, 36(2):341-50.

Bernabe, Alberto (2012). Giving credit where credit is due: A comment on the historical origin of the tort remedy for invasion of privacy. *The John Marshall Journal of Computer & Information Law*, 29(3):493-512.

Berger Levinson, Rosalie (2013). Targeted hate speech and the first amendment: How the supreme court should have decided Snyder. *Suffolk University Law Review*, 46(1):45.

Bertrand, Marianne & Mullainathan, Sendhil (2004). Are Emily and Greg more employable than Lakisha and Jamal? A field experiment on labor market discrimination. *Am. Econ. Rev.*, 94:991–1013.

Bloustein, Edward J. (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review*, 39:962.

Bonnici, Jeanne Pia (2014). Exploring the non-absolute nature of the right to data protection. *International Review of Law, Computers & Technology*, 28(2).

Boulanger, Marie-Hélène, Moreau, Damien, Léonard, Thierry, Louveaux, Sophie, Pouillet, Yves, & de Terwangne, Cécile (1997). La protection des données à caractère personnel en droit communautaire: troisième partie. *Journal des Tribunaux - Droit Européen*, 42:173-179.

Bösch, Christoph, Erb, Benjamin, Kargl, Frank, Kopp, Henning & Pfattheicher, Stefan (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies* 2016(4):237-254

Burchardt, Dana (2019). The Functions of Law and their Challenges: The Differentiated Functionality of International Law. *German Law Journal*, 20:409-429.

Burrell, Jenna (2016). How the Machine “thinks”: Understanding Opacity in Machine Learning Algorithms. *Big Data & Society*, 3(1):12.

Burt, Andrew (2017). Is there a ‘right to explanation’ for Machine Learning in the GDPR? iapp: Privacy Tech.

Bradford, Ben, Frisel, Florian, Meares, Tracey L., Owens, Emily, Pineda, Baron L., Shapiro, Jacob. N., Tyler, Tom R. & Peterman, Danieli Evans. (2019). Report of the Facebook Data Transparency Advisory Group. *Yale Law School*.

Brkan, Maja (2019). Do Algorithms Rule the World? Algorithmic Decision-making and Data Protection in the Framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 27(2).

Brkan, Maja (2019b). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning. *German Law Journal*, 20(6):864-883.

Brooks, Rachel (2018). Understanding the higher education student in Europe: a comparative analysis. *Compare: A Journal of Comparative and International Education*, 48:4:500-517.

Cáceres, Sigfrido Burgos (2012). NGOs, IGOs and International Law: Gaining Credibility and Legitimacy through Lobbying and Results. *Georgetown Journal of International Affairs*, 13(1): 79-87.

Caers, Ralf & Castelyns, Vanessa (2011). LinkedIn and Facebook in Belgium: The Influences and Biases of Social Network Sites in Recruitment and Selection Procedures. *Social Science Computer Review*, 29:437-448.

Calvi, Alessandra (2022). Gender, data protection & the smart city: Exploring the role of DPIA in achieving equality goals. *European Journal of Spatial Development (EJSD)*, 19(3):24–47.

Carlson, Caitlin & Rousselle, Hayley (2020). Report and repeat: Investigating Facebook’s hate speech removal process. *First Monday*, 25(2).

- Carlton, Alessandra (2020). Sextortion: The Hybrid 'Cyber-Sex' Crime. *North Carolina Journal of Law & Technology*, 21(3):215.
- Carson, Bryan (2013). Legally Speaking - Warren, Brandeis, and the Creation of the Legal Concept of Privacy. *Against the Grain*, 20(2).
- Casey, Bryan, Farhangi, Ashkon & Vogl, Roland (2019). Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise. *Berkeley Technology Law Journal*, 34(1):179.
- Citron, Danielle & Norton, Helen (2011). Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age. *Boston University Law Review*, 91(4):1435-1484.
- Citron, Danielle (2014). Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace. *Journal of Law, Technology and the Internet*, 6:1-12, p. 5
- Citron, Danielle (2020). Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (and as It Should Be). *Michigan Law Review*, 118(6):1073–1093.
- Cohen, Rosalyn (1961). The Concept of Statehood in United Nations Practice. *University of Pennsylvania Law Review*, 109(8), pp. 1127-1171.
- Cole, Mark, Etteldorf, Christina & Ullrich, Carsten (2021). Updating the Rules for Online Content Dissemination - Legislative Options of the European Union and the Digital Services Act Proposal. *Schriftenreihe Medienforschung der Landesanstalt für Medien NRW*, 83.
- Common, MacKenzie (2020). Fear the Reaper: How Content Moderation Rules Are Enforced on Social Media. *International Review of Law, Computers & Technology*, 34(2): 126-52.
- Corcoran, Lucie, Mc Guckin, Connor & Prentice, Garry (2015). Cyberbullying or Cyber Aggression? A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression. *Societies* 5(2):245-255.
- Cox, Cassie (2014). Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosecutions and Effective Laws. *Jurimetrics Journal of Law, Science and Technology*, 54(3):277–302.
- Crépeau, Paul-A. (1998). La fonction du droit des obligations. *McGill Law Journal*, 43(4):729.
- Danziger, Shai, Levav, Jonathan & Avnaim-Pesso, Liora (2011). Extraneous Factors in Judicial Decisions. Daniel Kahneman (ed.). *Proceedings of the National Academy of Sciences of the United States*, 108(17):6889–6892.
- D'Ath, Florence (2022). Luxembourg DPA Raises the Bar for Data Protection Officers. *European Data Protection Law Review*. 8(1):121-127

- Datta, Amit, Tschantz, Michael & Datta, Anumpam (2015). Automated Experiments on Ad Privacy Settings. *Proceedings on Privacy Enhancing Technologies*, 1(10):1515.
- de Búrca, Gráinne (2010). The Road Not Taken: The EU as a Global Human Rights Actor. *American Journal of International Law*, 105(4):649-693.
- De Hert, Paul & Gutwirth, Serge (2009). Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. *Reinventing data protection?* eds. Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne and Sjaak Nouwt eds. Berlin: Springer.
- de Montjoye Yves-Alexandre, Hidalgo César A., Verleysen Michel & Blondel Vincent D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports*, 3 :1376.
- de Montjoye Yves-Alexandre, Radaelli Laura, Singh, Vivek & Pentland, Alex (2015) Unique in the shopping mall: on the reidentifiability of credit card metadata. *Science*. 347(6221):536–539.
- Diaz, Fernando L. (2016). Trolling & the First Amendment: Protecting Internet Speech in the Era of Cyberbullies & Internet Defamation. *University of Illinois Journal of Law, Technology & Policy*, 1:159.
- Diggelmann, Oliver & Cleis, Maria (2014). How the Right to Privacy Became a Human Right. *Human Rights Law Review*, 14(3):442.
- Docksey, Christopher (2016). *Four fundamental rights: finding the balance*. *International Data Privacy Law*, 6(3):195–209.
- Douglas, David (2016). Doxing: A Conceptual Analysis. *Ethics and Information Technology* 18(3):199-210
- Easpaing, Bróna N. (2018). An exploratory study of sexism in online gaming communities: Mapping contested digital terrain. *Community Psychology in Global Perspective*, 4(2):119-135.
- Edelman, Benjamin & Luca, Michael (2014). Digital discrimination: the case of Airbnb.com. *Harvard Business School*. NOM Unit Working Paper 14-054.
- Edwards, Lilian & Veale, Michael (2017). Slave to the Algorithm? Why a ‘right to an explanation’ is Probably not the Remedy you are Looking For. *Duke Law & Technology Review*, 16(1).
- El Zeidy, Mohamed (2002). The Principle of Complementarity: A New Machinery to Implement International Criminal Law. *Michigan Journal of International Law*, 23(4).

Farzanehfar, Ali, Houssiau, Florimond & De Montjoye, Yves-Alexandre (2021). The risk of re-identification remains high even in country-scale location datasets. *Patterns*, 2(3).

Fenger, Niels & Broberg, Morten (2011). Finding Light in the Darkness: On the Actual Application of the *acte clair* Doctrine', *Yearbook of European Law*, 30(1):180–212.

Finck, Michèle & Pallas, Frank (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1):11-36.

Flaxman, Seth, Goel, Sharad, & Rao, Justin (2016). Filter Bubbles, Echo Chambers, and Online News Consumption. *Public Opinion Quarterly*. 80:298–320.

Flew, Terry, Martin, Fiona & Suzor, Nicolas (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, 101:33–50.

Flores, Anthony, Bechtel, Kristin & Lowekamp, Christopher (2016). False Positives, False Negatives, and False Analyses: A Rejoinder to 'Machine Bias. *Federal Probation Journal*, 80(2).

Franks, Marry Anne (2015). Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators. University of Miami School of Law (web version).

Galinsky, Adam D. & Wang, Cynthia (2013). The Reappropriation of Stigmatizing Labels: The Reciprocal Relationship Between Power and Self-Labeling. *Psychological Science*, 24(10):2020–2029.

Gentile, Giulia & Lynskey, Orla (2022). Deficient by design. The transnational enforcement of the GDPR. *International and Comparative Law Quarterly*, 71(4):799-830.

Gerkrath, Jörg (2007). Les principes généraux du droit ont-ils un avenir en tant qu'instrument de protection des droits fondamentaux dans l'Union européenne ? *Revue des Affaires Européennes*, 2007(1):31-34.

Gerkrath, Jörg (2009). Signification et fonctions d'une constitution. *Forum, Zeitschrift für Politik, Gesellschaft und Kultur in Luxemburg*, 286:23-26

Gillespie, Tarleton (2020). Content Moderation, AI, and the Question of Scale. *Big Data & Society*, 7(1).

Giraed, Aurélie & Fallery, Bernard (2009). E-recruitment: new practices, new issues, an exploratory study. *Proceedings of HRIS'2009 11th International Conference ICEIS in Human Resource Information System*, 39-48.

- Giurgiu, Andra, & Larsen, Tine A. (2016). Roles and powers of national data protection authorities. *European Data Protection Law Review*, 2(3):342-352.
- Goddard, Kate, Roudsari, Abdul & Wyatt, Jeremy (2014). Automation bias: empirical results assessing influencing factors. *Int J Med Inform*, 83(5):368-375.
- González Fuster, Gloria & Gellert, Raphaël (2012). The fundamental right of data protection in the European Union: In search of an uncharted right. *International Review of Law, Computers & Technology*, 26(1):74.
- González Fuster, Gloria & Gutwirth, Serge (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 29(5).
- Gorwa, Robert, Binns, Reuben & Katzenbach, Christian (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big data & society*, 7(1).
- Gray, Kishona L., Buyukozturk, Bertran & Hill, Zachary (2017). Blurring the boundaries: Using Gamergate to examine “real” and symbolic violence against women in contemporary gaming culture. *Sociology Compass*, 11(3).
- Grigg, Dorothy Wunmi (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. *Australian Journal of Guidance & Counselling*, 20(2):143-156.
- Gutierrez, Carlos Ignacio, Marchant, Gary & Tournaso, Lucille (2020). Lessons for artificial intelligence from historical uses of soft law governance. *Jurimetrics Journal of Law, Science and Technology* 61(1):133.
- Henman, Paul & Martson, Greg (2008). The Social Division of Welfare Surveillance. *Journal of Social Policy*, 37(2):187-205.
- Henriksen-Bulmer, Jane & Jeary, Sheridan (2016). Re-identification attacks—A systematic literature review. *International journal of information management*, 36(6):1184–1192.
- Hensler, Jack (2019). Algorithms as Allies: Regulating New Technologies in the Fight for Workplace Equality. *Temple International & Comparative Law Journal*, 34(1):31-60.
- Hijmans, Hielke (2018). How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? *European Data Protection Law Review*, 4(1):80-84.
- Hildebrandt, Mireille (2013). Balance or Trade-off? Online Security Technologies and Fundamental Rights. *Philosophy & Technology*, 26(4):357–379.
- Hildebrandt, Mireille (2021, March 15). Practical and Effective Protection’ of Human Rights in the Era of Data-Driven Tech: Understanding European Constitutional Law. *JOTWELL*.

Hoofnagle, Chris Jay, van der Sloot, Bart & Zuiderveen Borgesius, Frederik (2019) The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1): 65-98.

Hondius, Frits W. (1980). Data Law in Europe. *Stanford Journal of International Law*, 16:87-112.

Hosanagar, Kartik, Fleder, Daniel, Lee, Dokyun & Buja, Andreas (2013). Will the Global Village Fracture into Tribes? Recommender Systems and their Effects on Consumers. *Management Science*, 60(4).

Jacobsson, Markus & Menczer, Filippo (2003, December). Untraceable Email Cluster Bombs. *login*, 28(6). <https://www.usenix.org/system/files/login/articles/1154-jacobsson.pdf>.

Jhaver, Shagun, Ghoshal, Sucheta, Bruckman, Amy & Gilbert, Eric (2018). Online Harassment and Content Moderation. *ACM Transactions on Computer-human Interaction*, 25(2):1-33.

Jhaver, Shagun (2019). Human-machine collaboration for content regulation: The case of Reddit Automoderator. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26(5): 1-35.

Jobin, Anaa, Ienca, Marcello & Vayena, Effi (2019, September 2). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9):389–399.

John, Ann, Glendenning, Alexander Charles, Marchant, Amanda, Montgomery, Paul, Stewart, Anne, Wood, Sophie & Hawton, Keith (2018). Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review. *Journal of medical Internet research*, 20(4).

Johnson, Neil F. & al. (2019). Hidden resilience and adaptive dynamics of the global online hate ecology. *Nature*, 573:261–265.

Jones, Harry W. (1963). *The Creative Power and Function of Law in Historical Perspective*. *Vanderbilt Law Review*, 17:135-139.

Kaminski, Margot & Malgieri, Gianclaudio (2021, April). Algorithmic impact assessments under the GDPR: producing multi-layered explanations. *International Data Privacy Law*, 11(2): 125–144.

Kaplan, Andreas & Haenlein, Michael (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1): 15–25.

Karras, Tero, Laine, Samuli & Aila, Timo (2019). A Style-Based Generator Architecture for Generative Adversarial Network. *ArXiv*. [arXiv:1812.04948v3](https://arxiv.org/abs/1812.04948v3).

Katzenbach, Christian & Ulbricht, Lena (2019). Algorithmic governance. *Internet Policy Review*, 8(4):118.

Keerie, Catriona, Tuck, Christophe, Milne, Garry, Eldridge, Sandra, Wright, Neil & Lewis, Steff C. (2018). Data sharing in clinical trials - practical guidance on anonymising trial datasets. *Trials*, 19(1):25.

Kilbertus, Niki, Rojas-Carulla, Mateo, Parascandolo, Giambattista, Hardt, Moritz, Janzing, Dominik & Schölkopf, Bernhard (2017). Avoiding Discrimination through Causal Reasoning. *Advances in Neural Information Processing Systems*, 30:656-666.

Kim, Pauline T. (2020). Manipulating opportunity. *Virginia Law Review*, 106(4):867-875.

Kirby, Michael D. (2011). The history, achievement and future of the 1980 OECD guidelines on privacy. *International Data Privacy Law*, 1(1): 6-14.

Köchling, Alina & Wehner, Marius Claus (2020). Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, 13:795-848.

Kokott, Julian, & Sobotta, Christoph (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4).

Koops, Bert-Jaap (2014). *The trouble with European Data Protection Law*. *International Data Privacy Law*. doi: 10.1093/idpl/ipu023.

Kosta, Eleni (2014). The future of data protection: Collapse or revival? *International Review of Law, Computers & Technology*, 28(2):115.

Kornezov, Alexander (2016). The new format of the Acte Clair doctrine and its consequences. *Common Market Law Review*, 53(5):1317–1342.

Kramer, Irwin R. (1990). The birth of privacy law: A century since Warren and Brandeis. *Catholic University Law Review*, 39(3):703-724.

Kramer, Adam, Guillory, Jamie & Hancock, Jeffrey (2014). Experimental Evidence of Massive-scale Emotional Contagion Through Social Networks. *Proceedings of the National Academy of Sciences of the USA*, 111:8788.

Kuncel, Nathan R., Ones, Denis S. & Klieger, David M. (2014, May). In Hiring, Algorithms Beat Instinct. *Harvard Business Review*, 92(5):32.

Lacroux, Alain & Martin-Lacroux, Christelle (2022, July 6). Should I Trust the Artificial Intelligence to Recruit? Recruiters' Perceptions and Behavior When Faced With Algorithm-Based Recommendation Systems During Resume Screening. *Front Psychol.*, 6(13):895-997.

Langlois, Ganaele & Slane, Andrea (2017). Economies of reputation: the case of revenge porn. *Communication and critical/cultural studies*, 14(2):120–138.

Laulom, Sylvaine (2018). Better regulation and the social acquis: Is the REFIT fit for purpose? *European Labour Law Journal*, 9(1), pp.7–23.

Laurer, Moritz & Seidl, Timo (2021). Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation. *Policy and Internet*, 13(2): 257-77.

Le Fur, Louis (1935). Les caractères essentiels du droit en comparaison avec les autres règles de la vie sociale. *Archives de philosophie du droit*.

Leroy, Yann (2011). La notion d'effectivité du droit. *Droit Et Société*, 79(3).

Litwiller, Brett & Brausch, Amy (2013). Cyber Bullying and Physical Bullying in Adolescent Suicide: The Role of Violent Behavior and Substance Use. *Journal of Youth and Adolescence*, 42(5): 675-84.

Lock, Tobias & Layden, Patrick (2011). Protection of Fundamental Rights Post-Lisbon: The Interaction between the EU Charter of Fundamental Rights, the European Convention on Human Rights (ECHR) and National Constitutions. *FIDE National Report for the United Kingdom*. Web version.

Loi, Michele & Christen, Markus (2019). Two Concepts of Group Privacy. *Philosophy & Technology*, 1:18.

Lokke, Moerel (2011). The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, *International Data Privacy Law*, 1(1):28-46

Longhofer, Wesley, Schofer, Evan, Miric, Nick & Frank, David J. (2016). NGOs, INGOs, and Environmental Policy Reform: 1970–2010. *Social Forces* 94.4: 1743-768.

Lowry, Stella I. & McPherson, Gordon (1988, March 5). A blot on the profession. *British Medical Journal*, 296(6623):657-658.

Lynskey, Orla (2014). Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly*, 63(3):569-597.

Madden, Raul (2019). *Equity, 'Revenge Porn', and Cambridge Analytica: The Doctrine of Confidence as a Protection for Human Dignity in the Technological Age*. *Griffith Journal of Law & Human Dignity*, pp. 1-30.

Margalit, Avishai (2001). Privacy in the Decent Society. *Social Research*, 68(1).

- McDermott, Irene E. (2012). Trolls, Cyberbullies and Other Offenders: Dealing with Antisocial Behaviour on the Internet. *Searcher*, 20(10):7-11.
- McDermott, Yvonne (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1):2-7.
- Mehrabi, Ninareh, Morstatter, Fred, Saxena, Nripsuta, Lerman, Kristina & Galstyan, Aram (2021). A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys*, 54(6):1-35.
- Meyer, Robert & Cukier, Michel (2006). Assessing the Attack Threat due to IRC Channels. *International Conference on Dependable Systems and Networks (DSN'06)*:467-472.
- Miller, John (2010). Locking Down Privacy. *Managed Healthcare Executive*, 20(3):2-16.
- Miscenic, Emilia & Hoffmann, Anna-Lena (2020). The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation. *EU and comparative law issues and challenges series*, 2020:44-61.
- Mittelstadt, Brent (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology*, 30(4):475-494.
- Moerel, Lokke (2011). The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? *International Data Privacy Law*, 1(1):23-41.
- Moore, Gordon E. (1965, April 19). Cramming more components onto integrated circuits. *Electronics*, 38:8.
- Muir, Elise (2014). Fundamental Rights: An Unsettling EU Competence. *Human Rights Review*, 15(1):25-37.
- Murazzani, Maria (2009). NGOs, Global Governance and the UN: NGOs as "Guardians of the Reform of the International System". *Transition Studies Review* 16(2):501-09.
- Narayanan, Arvind & Shmatikov, Vitaly (2008). Robust De-anonymization of Large Sparse Datasets. *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 111:25.
- Narayanan, Arvind & Shmatikov, Vitaly (2019) Robust de-anonymization of large sparse datasets: a decade later. *Computer Science*. Princeton University (Web version).
- Nicolaidis, Kalypso & Howse, Robert (2002). 'This is my EUtopia ...': Narrative as power. *Journal of Common Market Studies*. 40(4): 767-792.

Nieves Saldaña, Maria (2012). The right to privacy: La génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis. *Revista De Derecho Político*, 0(85):195-239.

Noorbakhsh-Sabet, Nariman, Zand, Ramin, Zhang, Yanfei & Abedi, Vida (2019). Artificial Intelligence Transforms the Future of Health Care. *The American Journal of Medicine*, 132(7):795-801.

Nurse, Angus (2013). Privatising the Green Police: The Role of NGOs in Wildlife Law Enforcement. *Crime, Law and Social Change* 59.3: 305-18.

O'Neill, Brian & Dinh, Thuy (2015). Mobile Technologies and the incidence of cyberbullying in seven European countries: findings from the Net Children Go Mobile. *Societies*, 5:384-398.

Ohm, Paul (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57:1701.

Parasuraman, Raja, Molloy, Robert & Singh, Indramini L. (1993). Performance consequences of automation-induced "complacency." *Int J Aviat Psychol*, 3(1):1-23.

Parry, Emma & Tyson, Shaun (2008). An analysis of the use and success of online recruitment methods in the UK. *Human Resource Management Journal*, 18(3):257-274.

Pasquale, Frank (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Pech, Laurent & Groussot, Xavier (2010). Fundamental Rights Protection in the European Union post Lisbon Treaty. *European Issues* 173.

Post, Dana (2014). The long arm of the EU Data Protection directive. *Computing*, 24.

Powell, Connie Davis (2011). 'You already have zero privacy. Get over it!' Would Warren and Brandeis argue for privacy for social networking? *Harvard Law Review*, 4:193.

Purtova, Nadezhda (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1):40-81.

Rahman, Adzlia, Yusoff, Zaharah, Aziz & Omar, Dasimah (2014). Reducing Employee Travelling Time through Smart Commuting. *Earth and Environmental Science*, 18(2014)012074.

Rai, Arun (2020). Explainable AI: from black box to glass box. *Journal of the Academy of Marketing Science volume*, 48:137-141.

Ramirez, Rodolfo (2012). Online Impersonation: A New Forum for Crime on the Internet. *Criminal Justice*, 27(2):4–9.

Roberts, Lynne Diane (2008). Jurisdictional and Definitional Concerns with Computer-mediated Interpersonal Crimes: An Analysis on Cyber Stalking. *International Journal of Cyber Criminology*, 2(1).

Rutkin, Aviva (2016). Digital discrimination. *The New Scientist*, 231(3084):18-19, p. 18-19.

Salter, Michael (2018). From Geek Masculinity to Gamergate: The Technological Rationality of Online Abuse. *Crime, Media, Culture* 14(2):247-64.

Samuel, Arthur L. (1959). Some Studies in Machine Learning Using the Game of Checkers. *IBM Journal of Research and Development*, 44: 206–226.

Sandvig, Christian, Hamilton, Kevin, Karahalios, Karrie & Langbort, Cédric (2016). When the Algorithm Itself Is a Racist: Diagnosing Ethical Harm in the Basic Components of Software. *International Journal of Communication*, 10(19).

Sanfilippo, Madelyn R., Fichman, Pnina & Yang, Shengnan (2018). Multidimensionality of online trolling behaviors. *The Information Society*, 34(1):27-39.

Seering, Joseph, Kraut, Robert & Dabbish, Laura (2017). Shaping pro and anti-social behaviour on twitch through moderation and example-setting. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*, 111–125.

Selbst, Andrew D. & Powles, Julia (2017). Meaningful information and the right to explanation. *International Data Privacy Law*, 7(4):237.

Shah, Dhavan V., Cho, Jaeho & Kwak, Nojin (2005). Information and Expression in a Digital Age: Modeling Internet Effects on Civic Participation. *Communication Research*, 35:531.

Silver, David, Schrittwieser, Julian, Simonyan, Karen, Antonoglou, Ioannis, Huang, Aja, Guez, Arthur, Hubert, Thomas, Baker, Lucas, Lai, Matthew, Bolton, Adrian, Chen, Yutian, Lillicrap, Timothy, Hui, Fan, Sifre, Laurent, van de Driessche, George, Graepel, Thore & Hassabis, Demis (2017). Mastering the game of Go without human knowledge. *Nature*, 550:354-359.

Simitis, Spiros (2010). Privacy—An Endless Debate? *California Law Review*, 98(6):1995.

Sirakova, Iliyana (2016). EU-Food Law after REFIT: Better Regulations or More of the Same. *European Food and Feed Law Review*, 11(6): 531-33.

Školka, Andrej (2016). Can a 'Lone wolf' quasi-investigative journalist substitute the low functionality of the law enforcement system? *Central European Journal of Communication*, 9:197-212.

Spindler, Gerald & Schmechel, Philipp (2016). Personal Data and Encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 7: 163-177.

Stalla-Bourdillon, Sophie & Knight, Allison (2017). Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data. *Wisconsin International Law Journal*, 34(284), p. 301.

Stade-Müller, Frithjof, Hansen, Britta & Voss, Mélanie (2012). How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology*, 9:260-274.

Suler, John (2004). The Online Disinhibition Effect. *Cyber Psychology & Behaviour*, 7(3):321.

Sunstein, Cass R. (1995). Problems with Rules. *California Law Review*, 83(953).

Sunstein, Cass R. (2019). *On the Expressive Function of Law*. *University of Pennsylvania Law Review*, 144:2021.

Suominen, Annika (2014). Effectiveness and Functionality of Substantive EU Criminal Law. *New Journal of European Criminal Law*, 5(3): 388-415.

Svoboda, Elizabeth (2020). Deep learning delivers early detection. *Nature*, 587:20-22.

Szydło, Marek (2013). Principles Underlying Independence of National Data Protection Authorities: Commission v. Austria. *Common Market Law Review*, 50(6): 1809-826.

Thouvenin, Florent, Früh, Alfred & Henseler, Simon (2022). Individual Decision-Making: Prohibition or Data Subject Right? *EDPL* 2/2022, 8:183-198.

Tucker, Katherine & al. (2016). Protecting patient privacy when sharing patient-level data from clinical trials. *BMC Medical Research Methodology*, Suppl 1(S1):77.

Tulkens, Françoise (2013). The Hate Factor in Political Speech. Where Do Responsibilities Lie? *Council of Europe*. <https://rm.coe.int/16800c170e>.

Turing, Alan Mathison (1937). On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*. 2(42): 230-265.

van Dalen, Steven, Gilder, Alexander, Hooydonk, Eric & Ponsen, Marc (2016, March 31). System Risk Indication: An Assessment of the Dutch Anti-Fraud System in the Context of Data Protection and Profiling. *PILP*.

van der Sloot, Bart (2014). Do data protection rule protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International privacy Law* 4(4):307-325.

van der Sloot, Bart (2015). Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System'. *Computer Law and Security Review*, 31.

Wachter, Sandra, Mittelstadt, Brent & Floridi, Luciano (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2):76–99.

Warren, Samuel D. & Brandeis, Louis D. (1890). The right to privacy. *Harvard Law Review*, 4(5):193-220.

Weatherford, Margaret (1996). A quarter century of microprocessors. *Computer*, 29(3):99.

Weichert, Thilo (2012). Anmerkungen zu Warren/Brandeis — Das Recht auf Privatheit. *Datenschutz Und Datensicherheit - DuD*, 36(10):753-754.

Wetzel, Joseph R. (2003). Improving fundamental rights protection in the European union: Resolving the conflict and confusion between the Luxembourg and Strasbourg courts. *Fordham Law Review*, 71(6):2823-2862.

White, Rob & van der Velden, John (1995). Class and Criminality. *Social Justice*, 22(1):51-74.

White, Rob (2002). Environmental Harm and the Political Economy of Consumption. *Social Justice*, 29:82-102.

Wittes, Benjamin (2017). Cyber Sextortion and International Justice. *Georgetown Journal of International Law*, 48(3):941.

Wolak, Janis, Finkelhor, David, Walsh, Wendy & Treitman, Lah (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health* 62(1):72-79.

Wu, Jianjun, Thorne-Large, James & Zhang, Pengfei (2021). Safety first: The risk of over-reliance on technology in navigation. *Journal of Transportation Safety & Security*, 1(28); Hansen, L. (2015, January 9). Eight drivers who blindly followed their GPS into disaster. The Week. <https://theweek.com/articles/464674/8-drivers-who-blindly-followed-gps-into-disaster>.

Zimmerman, Adam G. (2012) Online Aggression: The Influences of Anonymity and Social Modelling. *University of North Florida Graduate Theses and Dissertations*, 403. <https://digitalcommons.unf.edu/cgi/viewcontent.cgi? article=1472&context=etd>.

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, 28(1), 10–29.

Zuiderveen Borgesius, Frederik J., Trilling, Damian, Möller, Judith, Bodó, Balazs, de Vreese, Claes H. & Helberger, Natali (2016). Should we worry about filter bubbles? *Internet Policy Review*, 5(1).

Zuiderveen Borgesius, Frederik J. & Poort, Joos (2017). Online Price Discrimination and EU Data Privacy Law. *Journal of Consumer Policy*, 40(3):347-366.

Zuiderveen Borgesius, Frederik J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, 4(10):1572-1593.

Reports, studies & general documentation

AlgorithmWatch (2019, January). Automating Society: Taking stock of Automated Decision Making in the EU. https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf.

Boucher, Philipp (2019). How artificial intelligence works. European Parliamentary Research Service Briefing Note, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI\(2019\)_634420_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI(2019)_634420_EN.pdf).

Bryter (2020, November 12). Female Gamer Survey 2020. <https://www.womeningames.org/wp-content/uploads/2021/03/Bryter-Female-Gamers-Survey-2020-12.11.20-SHORT-no-quotes.pdf>.

Brown, Alexander (2020, May). Models of Governance of Online Hate Speech. Council of Europe. <https://rm.coe.int/models-of-governance-of-online-hate-speech/16809e671d>.

Bychawska-Siniarska, Dominika (2017). Protecting the Right to Freedom of Expression under the European Convention on Human Rights, A handbook for Legal Practitioners. Council of Europe. <https://edoc.coe.int/en/fundamental-freedoms/7425-protecting-the-right-to-freedom-of-expression-under-the-european-convention-on-human-rights-a-handbook-for-legal-practitioners.html>.

Cambridge Consultants (2019). Use of AI in content moderation. *Ofcom*. https://www.ofcom.org.uk/data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf.

Caplan, Robyn (2018, November 14). Report. Content or Context Moderation? *Data & Society*. https://datasociety.net/wp-content/uploads/2018/11/DS_Content_or_Context_Moderation.pdf.

CNIL (2017, December). Comment Permettre à l'Homme de Garder la Main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.

Council of Europe (2014, April 16). Guide to human rights for Internet users. Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31>.

Council of Europe (2016). Background note on sexist hate speech. *Gender Equality Unit*. <https://bit.ly/2LDTcVt>;

Council of Europe (2017). Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. Council of Europe Study DGI(2017)12. <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

Council of Europe (2019, February). Conference report on impacts of artificial intelligence development on human rights, democracy and the rule of law. <https://rm.coe.int/conference-report-28march-final-1-/168093bc52>.

Cowls, Josh & al. (2020). Freedom of Expression in the Digital Public Sphere. Policy brief. *Graphite* <https://graphite.page/policy-brief-values/>.

Duggan, Maeve (2017, July 11). Online Harassment 2017. Pew Research Center. http://assets.pewresearch.org/wpcontent/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf

European Agency for Fundamental Rights (2014, March 5). Violence against women: an EU-wide survey. Main results report. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf

ECtHR (2022, April 31). Guide on Article 8 of the European Convention on Human Rights (as last updated). https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

ERGA (2020). Notions of Disinformation and Related Concepts Report. <https://erga-online.eu/wp-content/uploads/2021/01/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts.pdf>.

European Commission (2018, April 26). Communication Tackling online disinformation: a European Approach. COM(2018) 236 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>.

European Commission's High Level Expert Group on Artificial Intelligence (2019, 8 April). Ethics Guidelines on Trustworthy AI. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

European Parliament (2016, August 30). Study on cyberbullying among young people. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU\(2016\)571367_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf)

European Parliament (2018, September). Study on cyber violence and hate speech online against women. [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU\(2018\)604979_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf)

European Parliament (2020, July). Study on hate speech and hate crime in the EU and the evaluation of online content regulation approaches. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/655135/IPOL_STU\(2020\)655135_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/655135/IPOL_STU(2020)655135_EN.pdf)

European Political Strategy Centre. (2018, March). The Age of Artificial Intelligence. https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf.

European Union Agency for Fundamental Rights (2011). *Report: Access to Justice in Europe: an overview of challenge and opportunities*. https://fra.europa.eu/sites/default/files/fra_uploads/1520-report-access-to-justice_EN.pdf.

European Union Agency for Fundamental Rights (2014). *An EU internal strategic framework for fundamental rights: Joining forces to achieve better results*. Luxembourg: Publications Office.

European Union Agency for Human Rights (2019, June). Paper on Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf.

Fletcher, Richard & Jenkins, Joy (2019, March). Study on polarisation and the news media in Europe. EPRS. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU\(2019\)634413_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634413/EPRS_STU(2019)634413_EN.pdf).

Ferrier, Michelle (2018). Attacks and Harassment: The Impact on Female Journalists and Their Reporting. *International Women's Media Foundation*. <https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf>.

Martens, Bertin, Aguiar, Luis, Gomez-Herrera, Estrella & Mueller-Langer, Frank (2018, April). The digital transformation of news media and the rise of disinformation and fake news. European Commission. JRC Technical Report 2018-02. https://ec.europa.eu/jrc/communities/sites/jrccties/files/dewp_201802_digital_transformation_of_news_media_and_the_rise_of_fake_news_final_180418.pdf.

McCully, Jonathan (2019, March 3). Legal Responses to Online Harassment and Abuse of Journalists: Perspectives from Finland, France and Ireland. *Organization for Security and Co-operation in Europe (OSCE) & International Press Institute (IPI)*. <https://www.osce.org/files/f/documents/1/6/413552.pdf>.

North Yorkshire Police & Crime Commissioner (2018). *Suffering in Silence, Why revenge porn victims are afraid and unwilling to come forward because of a fear they'll be named and shamed – and why that needs to change. Image-based Sexual Abuse Report* 2018. <https://www.northyorkshire-pfcc.gov.uk/content/uploads/2018/11/Suffering-in-Silence-Report.pdf>.

Porcedda, Maria Grazia (2017). *Use of the Charter of Fundamental Rights by Data Protection Authorities and the EDPS. Research Project Report. EUI*. [https://op.europa.eu/o/opportal-service/download-handler?identifier=c17ffac6-5ae5-11e7-954d-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=.](https://op.europa.eu/o/opportal-service/download-handler?identifier=c17ffac6-5ae5-11e7-954d-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=)

Rokša Zubčević, Asja, Bender, Stanislav & Vojvodić, Jadranka (2017). *Media Regulatory Authorities and Hate Speech. Council of Europe*. <https://edoc.coe.int/fr/medias/7431-media-regulatory-authorities-and-hate-speech.html>.

Sartor, Giovanni & Loreggia, Andrea (2020, September). *The impact of algorithms for online content filtering or moderation. Policy Department for Citizens' Rights and Constitutional Affairs. European Parliament*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU\(2020\)657101_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf).

UK Council for Internet Safety (2019, June 26). *Adult Online Hate, Harassment and Abuse: A rapid evidence assessment*. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult Online Harms Report 2019.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf)

Vogels, Emily A. (2021, January 13). *The State of Online Harassment. Pew Research Center*. file:///Users/Flo/Downloads/PI_2021.01.13_Online-Harassment_FINAL-1.pdf.

Zuiderveen Borgesius, Frederik (2018). *Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe*. <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>.