The impact of the principles of GDPR

Charis Tsiamoulis

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

Master of Laws (LL.M.) In Transnational and European Commercial Law, Banking Law, Arbitration/ Mediation

January 2020

Thessaloniki – Greece

Student Name: Charalampos Tsiamoulis

SID: 1104170034
Supervisor: Prof. Komninos Komnios

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

January 2020
Thessaloniki - Greece

Abstract

This dissertation was written as part of the LL.M. program in Transnational and European Commercial Law, Banking Law, Arbitration/ Mediation at the International Hellenic University.
It examines the principles of processing of personal data according to the GDPR, aiming to point out their impact. Processing is every operation performed on personal data. Personal data is now every information relating to a natural person. We live in the 'age of information', thus the European legislation on the protection of the personal data 'touches' every occupation and every social activity. Such immensity of the scope makes it impossible for the legislator to foresee every possible issue. Therefore, the GDPR may contain numerous and detailed provisions, but the core of it are the abstract principles, which have evolved the past 40-50 years and reflect the rationale of the legislation.
In order to analyze and assess the principles of the GDPR, one has to have a historical and cultural overview of their 'source', the concept of privacy, which is already elevated to the status of a fundamental right in Europe. Hence, this paper will first try to present a brief history of privacy and personal data protection, how they are conceived in Europe and other parts of the world, then an analysis of the principles and finally the difficulties that their implementation faces as well as poses to other professional and social activities.

Keywords: GDPR, privacy, principles, personal data

Charis Tsiamoulis
31-1-2020

Preface

I want to thank Prof. Dr. Komninos Komnios for the introduction to the personal data protection law, for his valuable advices and particularly for urging me to attend a second LL.M., nearly twenty years after a previous one in Germany. Despite my professional and family commitments, I really enjoyed it.

I dedicate the dissertation to my beloved wife Frida, my friend.

Contents

Introduction

Beginning from a personal perspective, during 20 years of practice as a lawyer in the fields of commercial and civil law, I was regarding personal data protection law as an obstacle. When I was trying to collect evidence or other information, public servants were often refusing, barricading themselves behind the words ‘‘personal data’’, without ever explaining what that meant and what the violation consisted in; and usually without giving the impression, that as ‘‘protectors of the personal data’’ knew and understood the provisions of the relevant legislation. Hence, what ‘‘personal data protection’’ usually meant for a lawyer in Greece, was ‘‘keep your calm with the public servant’’ and ‘‘go to the district attorney’s office to get a disclosure order’’.

Nevertheless, I have to admit that I hadn’t followed the six years discussion around the GDPR up until the coming to force. It gives me no credit to confess, that when a client running a small commercial enterprise asked me in April 2018, what to do to comply with the new Regulation, I reassured him that there were no particular measures to be taken for the time being and that I would get back to him.[1] What I didn’t explicitly replied, was that at the time I didn’t have a clue (a lawyer rather seldom admits ignorance).

I began studying the GDPR, trying to locate specific new obligations for SMEs and I was struck with its structure, complexity and volume of provisions. Compared to the 34 articles of the Data Protection Directive 95/46/EC (DPD95) there were now 99 articles, appearing to construct a new and much more detailed legal regime. What also struck me was the coexistence of abstract provisions and detailed technicalities. At the time I was rather busy with a couple of litigation cases, and I couldn’t spend more than a few hours, which I thought would be enough not to become an expert, but to spot the obligations and technicalities and to compose a concise checklist of alerts and steps, to provide to my client. But I quickly realized, that a few hours or even a couple of days wouldn’t be enough for me to feel confident that I understood the regime and that I wouldn’t miss an important detail.

[1] The date of entry into force and application was 25 May 2018, article 99 GDPR

So, I started wondering, why this Regulation had to be so extensive and so complex. What was clear from the beginning, was that the scope of the GDPR is very broad as it is addressing every business, *public authority, agency or other body,*[2] irrespective of its size and occupation; it is including in its scope every piece of information '*relating to an identified or identifiable natural person*'[3]; and it is regulating '*any operation or set of operations which is performed on personal data*'[4]. Moreover, the complexity of the provisions and the sophistication of the technical obligations for the controllers and processors gave me the impression that this Regulation had to be having its sights primarily on Google, Facebook and the rest of the tech giants, or on large corporations handling personal data, such as banks and insurance companies, not each and every business which keeps simple records of its clientele.

At the same time, I noticed at the internet the confusion and the same anxiety, that my client had had and I also noticed the appearance of an army of self-declared experts, who were promising to adapt businesses to the new data protection regime, to ensure compliance and avoidance of the severe new penalties and even train others to become certified experts themselves. Finally, I noticed around the end of the spring of 2018 a steep increase of difficulties to obtain information and to carry out my every-day occupational tasks, such as access to the courts' archives, published wills, public documents and even documents of incorporation of companies.

All these considered, the new provisions, which the GDPR introduced, may be complex, demanding and hard to approach, generating the recent agitation, nevertheless it is the set of the principles of processing[5], what constitutes the framework of the personal data protection. They are quite abstract,[6] they reflect the spirit of the regulation and lie in its core. They are almost the same as in the DPD95, but they are now regarded as more ''serious'' than before, because of the volume and the complexity of the adjacent new provisions.

This paper will try to focus on these most important provisions of GDPR, the principles of personal data processing, their basis, evolution, interpretation and impact.

---

[2] article 4 (7)
[3] article 4 (1)
[4] article 4 (2)
[5] Articles 5, 6 and 7
[6] as it is always with legal principles

It will first try to explain why personal data enjoy such an elevated state of protection, especially in Europe, by approaching the concept, or rather the fundamental right in privacy, the history of its regulation and the dominant views about it in some parts of the world. The scope is quite wide, as it encompasses elements from philosophy, history and national mores. An in-depth coverage is impossible, therefore an effort will be made, to point out some characteristic points and to extract some deductions.
Finally, some worries will be presented about the impact of the principles of the GDPR.

1. THE CONCEPT OF PRIVACY

"*If this is the age of information, then privacy is the issue of our times*".[7] Today's onslaught of digital information technology is widely seen as a clandestine threat to privacy, because of the trails of everybody's personal data left knowingly and unknowingly in the internet. [8]

Now that the personal data, according to the GDPR, is every information *relating to an identified or identifiable natural person,* privacy which is acknowledged by the European human rights legislation as a fundamental right[9], is the gnomon to determine, when the personal data should be protected. In order to develop effective data protection principles, the very nature and significance of privacy had to be conceived. To do so, the private from the public has to be distinguished.[10] Despite theories developed by numerous scholars across a wide range of disciplines, the nature of privacy remains a controversial, ambiguous and subjective concept. A general theory stumbles upon the fact that privacy is to be circumscribed by the ephemeral social contexts across different cultures, and the varying, subjective specific views of individuals moving inside such social contexts.[11]

1.1. The beginning of the discussion in the USA

The concept of a ''right to privacy'' as referring to control over personal information was famously introduced by US scholars Warren and Brandeis in an eponymous article. They drew references from the French law of the press and described the right they supported as ''*the right to be let alone*''.[12] The argumentation of the article was so influential, that it is considered as the basis of the discussion on the regulation of privacy.

---

[7] Alessandro Acquisti, Laura Brandimarte, George Loewenstein, 'Privacy and human behavior in the age of information', Science 347 (2015), p. 509.

[8] Sheng Yin Soh, Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour, 5 Eur. Data Prot. L. Rev. (2019), p. 65.

[9] Article 8 ECHR

[10] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, Springer, p.26

[11] Kirsty Hughes, A Behavioural Understanding of Privacy and Its Implications for Privacy Law, 75 Mod. L. Rev. 806 (2012).

[12] Samuel D. Warren, Louis D. Brandeis, 'The right to privacy', Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 195, 214.

1.2. Theories of categorization of privacy

1.2.1. Categories of privacy torts

Hence, in 1960, another US scholar, William Prosser, acknowledged a privacy tort, distinguishing four types of it: the intrusion upon a person's solitude or seclusion; the appropriation, for commercial purposes, of a person's name, likeness, or personality; the public disclosure of embarrassing private facts about a person; and the publicity that places a person in a false light in the public eye.[13]

Nevertheless, privacy protection in the USA eventually found its way not only in tort law, but also in constitutional law, (although not explicitly) as referring to the right for individuals to refuse interferences from the government.[14]

1.2.2. States of privacy

Equally influential was Alan Westin's ''states of privacy'', placing information to the core of the concept of privacy. In his words: ''*privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*''. [15] Westin categorized privacy into four ''states'': solitude, intimacy, anonymity and reserve. Solitude means total physical separation from others. Intimacy involves close, relaxed, and frank relationships inside a small unit. Anonymity is ''*the desire of individuals for times of public privacy*'' and reserve, is the ''erection'' of a psychological barrier to limit communication about himself.[16]

1.2.3. Theory of spheres

Meanwhile, in post-war Germany, the German Federal Constitutional Court had adopted the ''theory of the spheres''[17], according to which, a series of concentric

[13] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, Springer, p.27
[14] Ibid., p.28
[15] Ibid., p.31
[16] Kirsty Hughes, A Behavioural Understanding of Privacy and Its Implications for Privacy Law, 75 Mod. L. Rev. 811 (2012).
[17] Sphärentheorie

circles, delineating different areas, based on distinct degrees of the private, derive from the general right to free development of personality[18]; the ''Individualsphäre'', the ''Privatsphäre'' and the ''Intimsphäre''.[19]

1.2.4. Various other categorizations

Other scholars tried to identify the scope of privacy rights by categorizing them into those that protect private places; those that seek to establish a realm of private decision-making; those that are based upon managing private information; and those that encompass limiting access to self. Others have focused upon "privacy problems", such as surveillance and information processing[20].

Still, although the above concepts of ''states'', ''spheres'', ''places'' etc. aim to define the concept of privacy, they also have to be defined. Does the ''Privatsphäre'' exist inside a concrete place, particularly ''at home'', or anywhere the subject so desires? For example, does the workplace fall into the private or public sphere/state/life of an employee?

In the Niemetz v Germany judgment [21] the ECtHR acknowledged that it is not possible (and even necessary!) to distinguish between private and working life, since inside the workplace people may coexist with employers and other employees, but it can in the same time be a place where people develop intimate human relationships. Therefore, found in 2017 that the concept of private life must be interpreted broadly, including the right to ''*lead a private social life at work*''. [22] So, the description of privacy according to the famous English quote ''a man's home is his castle''[23] appears too narrow for the European Judge. Accordingly, the Article 88 of the GDPR acknowledged the respect for privacy at workplaces as well.

---

[18] allgemeine Persönlichkeitsrecht

[19] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, Springer, p.24-26

[20] Daniel Solove, Conceptualizing Privacy, California Law Review (2002), p.1096-1099

[21] Niemietz v. Germany, ECHR 72/1991/324/396, 16 December 1992, par.29

[22] Antovic and Mirkovic vs Montenegro, ECHR App. Nu. 70838/13 par.41; Elena Kaiser, Monitoring Employees with Hidden Surveillance Cameras Breaches Their Right to Privacy, 4 Eur. Data Prot. L. Rev. 398 (2018).

[23] Sir Edward Coke, The Institutes of the Laws of England, 1628

1.2. Reasonable expectation theory

Such blurred lines about where privacy should be respected and where it doesn't exist, led to the conception of subjective tools such as the ''reasonable expectation privacy'' test, which was first developed in the United States, in the Fourth Amendment case ''Katz''[24] and is used by the ECtHR in its Article 8 ECHR jurisprudence.[25] In short, if the employee wasn't adequately informed about being under surveillance by the employer and had ''a reasonable expectation'' that such surveillance was not taking place, then there was a breach of his privacy rights.[26]

However, the critique in the other side of the Atlantic is that whilst ''*at first glance*'' the test *''seems quite sensible''*, it ''*has failed to live up to its aspirations*'' and that ''*subsequent to the test's development, the US Supreme Court adopted a conception of privacy that countless commentators have found to be overly narrow, incoherent, short-sighted, deleterious to liberty, and totally out of touch with society*''.[27]

Moreover, such subjective tools do not take account of what Spiros Simitis characterizes: ''*a unique experience: an unprecedented readiness to expose even the most private data*.'' He eloquently observes that: ''*The same people who otherwise insist on the inaccessibility of their private sphere, have evidently not the slightest hesitation to publicly revealing all its details. It is no wonder that social networking information, provided, for instance, by widespread flirting on Facebook, is now used in the United Kingdom as a divorce reason in every fifth divorce or separation case. An evaluation of chatting on the Internet has shown that it manifestly contributed to the proliferation of divorces in the last two years*.''[28]

Others name such trends as the ''privacy paradox''. Despite empirical studies showing that internet users are generally aware of the threats to their privacy and are concerned about the potential misuse of their personal information, these concerns do not necessarily translate into adopting privacy protection measures or behaviors

[24] Katz vs United States 389 US 347 (1967)
[25] Kirsty Hughes, A Behavioural Understanding of Privacy and Its Implications for Privacy Law, 75 Mod. L. Rev. 824 (2012).
[26] Barbulescu vs Romania, ECHR App. Nu. 61496/08 par.56; Antovic and Mirkovic vs Montenegro, ECHR App. Nu. 70838/13 par.43
[27] Daniel Solove, Fourth Amendment Pragmatism, 2010 Boston College Low Review (2010) p. 1519
[28] Spiros Simitis, Privacy - An Endless Debate, 98 Calif. L. Rev. 2004 (2010).

online and even freely disclose their data. According to behavioral psychology this privacy paradox is due to the limits and fallacies in individual decision-making [29].

1.2. Conclusions on the privacy theories

The conclusions from these brief remarks are that:

1. Privacy is a fundamental right;[30] legally sacred.
2. It has to be protected against both private entities and the state.
3. We cannot objectively define the borders of privacy.
4. Tools such as ''reasonable expectations'' tests collide to the unexpected irrationalities of human behavior.

Therefore, it appears very difficult to regulate the processing of personal data through concrete rules. The protection has to be based on abstract principles, concretized by a designated public authority and finally, as always with legal principles, by the judge. Such hardships in defining the privacy rights and the adequate personal data protection are reflected in the history of the evolution of privacy protection law.

2. PERSONAL DATA PROTECTION HISTORY

The recognition of a right to privacy or data protection as a legal right is quite recent.[31] Before World War II specific aspects of private life were legally regulated such as the inviolability of the home, or confidentiality of correspondence.[32]

[29] Sheng Yin Soh, Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour, 5 Eur. Data Prot. L. Rev. 69 (2019).
[30] Art 8 ECHR
[31] Franziska Boehm, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Springer [2012] p.3
[32] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, Springer, p.23

2.1. International treaties

2.1.1. UN Universal Human Rights Declaration

In the aftermath of World War II, in 1948 the General Assembly of the United Nations adopted the Universal Declaration of the Human Rights. Article 12 introduced the prohibition against arbitrary interference with privacy. The provision distinguished privacy from the concepts of family, home and correspondence, implying that the former consists of elements that fall outside of the concepts of the three later, which are more definable. This is a direct acknowledgment, that private is not only home, family matters and correspondence, although they are the key elements.

2.1.2. ECHR and Convention (108)

Following, in 1949, ten European states intending to promote the rule of law, democracy, human rights and social development found the Council of Europe (CoE), which adopted the European Convention on Human Rights in 1950. Article 8 of the Convention introduced the protection of privacy, repeating from the Declaration the quartet of privacy, family, home and correspondence.

In order to clarify and specify the framework of privacy protection of Article 8 the Convention 108[33] was adopted in 1981. It offered provisions for the automatic processing of personal data by both private and public entities, was ratified by 55 states,[34] and is the only binding international instrument specifically on data protection, distinguishing the concept from privacy. [35]

[33] Convention for the protection of individuals with regard to automatic processing of personal data

[34] Among them all of the European Union members

[35] European Union Agency for Fundamental Rights and Council of Europe, 'Handbook on European data protection law' (2014) 14 <https://rm.coe.int/16806b294a>.

2.2. EU Regulation

2.2.1. Directive 95/46/EC

From that point on, the EU took over legislation enacting the Directive 95/46/EC (DPD95), which introduced in a European level a concise system of provisions, providing the guidelines for the national laws. Importantly, the continuity to the (non-EU) ECHR was specifically stated in Recital 10 of the DPD95, which refers to Article 8 ECHR.

The DPD95 was followed by European legislation providing rules in specific areas of the law, such as Regulation (EC) No 45/2001 on the processing of personal data by the Community institutions,[36] on privacy and electronic communications[37] and on the electronic communications sector.[38]

As DPD95 was progressively implemented into the national legal order of the Member States, the concepts of personal data, and data protection, spread throughout Europe. However, the from-state-to-state implementation of the Directive resulted in national differences, especially in relation to conflicts between personal data protection and other fundamental rights.[39]

2.2.2. EU's Charter of Fundamental Rights

In 2000 the EU's Charter of Fundamental Rights was signed in Nice by the member states and came into force in 2009. The Charter was the first catalogue of rights ever agreed jointly by the three major EU institutions and designated the rights it recognizes as fundamental. Article 8 of the Charter provided a right not generally to privacy, but specifically for the protection of personal data.[40]

However, according to the Charter, the corresponding rights of ECHR and the Charter deriving from the main sources of fundamental human rights protection, are to be

[36] Regulation (EC) No 45/2001
[37] Directive 2002/58/EC
[38] Directive 2009/136/EC
[39] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, Springer, p.156
[40] Matthew White, Immigration Exemption and the European Convention on Human Rights, 5 Eur. Data Prot. L. Rev. 26 (2019).

interpreted as the same.[41] Thus, the meaning and scope of the right to protection of personal data[42] and the right to private life[43] have been interpreted as effectively the same by the European Courts of Justice. The CJEU found that ''*In those circumstances, it must be considered that the right to respect for private life with regard to the processing of personal data, recognized by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual and the 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 Convention*'', thus merging the two concepts as "*the right to respect for private life with regard to the processing of personal data*".[44]

2.3. National legislation

On national level, several European countries, had adopted laws providing rules on the processing of personal data before the adoption of the DPD95.

2.3.1. State of Hesse

Pioneer had been the Hessisches Datenschutzgesetz[45] in 1970, of the German federal state of Hesse. The provisions of the law, which for the first time adopted the term ''data protection'' and not generally ''privacy'', were primarily designed by Spiros Simitis, who is since honorably called in Germany the 'father of data protection'.[46]
The Law regulated data protection introducing provisions for the lawful processing of records and data such as the collection, storage and transmission and the avoidance of interference by an unauthorized person.[47]

---

[41] EU Charter, art 52(3).
[42] EU Charter, art 8
[43] ECHR, art 8
[44] Cases C-92/09 and C-93/09 Volker und Marcus Schecke GbR and Hartmut Eifert v Land Hessen [2010] EU:C: 2010:662, para 52.; Jessica Bell; Stergios Aidinlis; Hannah Smith; Miranda Mourby; Heather Gowans; Susan E. Wallace; Jane Kaye, Balancing Data Subjects' Rights and Public Interest Research, 5 Eur. Data Prot. L. Rev. 46 (2019),
[45] data protection law
[46] Anne Hardy, 'Spiros Simitis: Es geht um Eure Daten!' Marketing und Kommunikation Goethe-Universität Frankfurt am Main, https://idw-online.de/de/news635029
[47] Section 2 of 1970 Hesse Data Protection Act.

2.3.2. Sweden

In 1973, Sweden, another pioneering state in the theory of the data protection legislation had adopted a law named ‘‘Datalag’’[48], which was the first national law regulating automated data processing. [49]

2.3.3. Germany

Following the Hessisches Datenschutzgesetz, in 1977, Germany had enacted its first Federal Data Protection Law or Law on Protection Against the Misuse of Personal Data in Data Processing,[50] which covered the regulation concerning private processing of personal data as well.[51]

In 1978, France had endorsed a law entitled “informatique et libertes”[52] and Austria was the first state in 1978 to advance a right called ‘‘right to data protection’’ as a constitutionally protected fundamental right. [53]

2.3.4. Rest of Europe

At the same time in the 1970s other European countries, such as Denmark, Norway and Luxembourg passed relevant legislation as well.[54]

2.4. USA

In the other side of the Atlantic, the US adopted the Privacy Act in 1974, with the formal purpose of safeguarding individual privacy from the misuse of federal records and providing individuals access to them.[55]

---

[48] Data Act

[49] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, Springer, p.58

[50] Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung, Bundesdatenschutzgesetz, BDSG

[51] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, Springer, p.60

[52] Computers and freedoms, Ibid., p.21

[53] Ibid, p.71

[54] Ibid, p.65

[55] Ibid., p.35

3. RATIONALE OF THE PERSONAL DATA PROTECTION REGULATION

The evolution of the European regulation of privacy or personal data reflects cultural elements, collective mentalities and idiosyncrasies of the relevant nations.[56]

3.1. Memories of oppressive regimes

Especially in Europe, the State's abuse of surveillance and record keeping during the Second World War and Cold War, left deep scars in the minds of the Europeans, a fact that explains the elevation of the protection of privacy, not only to a positive legal level, but to a fundamental, constitutional right.[57]

Even cases of record keeping by liberal governments sometimes didn't escape abuses. An extreme example is the Dutch population information systems of the 1930s serving the improvement of administrative efficiency. The data collected, contained religious elements as well, as was then common. When the Netherlands were occupied by Nazi Germany, those archives helped the Nazis to efficiently trace the Dutch Jews.[58]

3.1.1. Germany

Therefore, it is understandable that the Germans are not only the pioneers in data protection, but also among the most jealous proponents of data protection.

However, any foreigner who found himself in a German spa without having been warned, may feel the least awkward before the sight of completely nude men and women. Germans don't call like the Americans ''private parts'' what according to them everybody has. The paradox is that they are very private people when it comes to personal data such as names, telephone numbers or addresses, in sharp contrast to the Americans. The reason for this is thought to be memories of the Gestapo and

[56] Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle, 2 Eur. Data Prot. L. Rev. 294 (2016).

[57] David J. Stute, Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, 36 Mich. J. Int'l L. 649 (2015).

[58] David Lazer; Victor Mayer-Schoenberger, Drawing Lessons for the DNA Data Banks from Other Government Data Systems, 34 J.L. MED. & ETHICS 366, 368 (2006), David J. Stute, Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, 36 Mich. J. Int'l L. 652 (2015).

Stasi.[59] The widespread subconscious ‘‘Angst’’ of ordinary Germans that they are under surveillance.

Such feelings often touching the realms of conspiracy theories, were recently reinforced by the revelations about the NSA surveillance scandal.[60] Even the fact that the otherwise progressive Germans still mistrust electronic means of payment and prefer cash, has its roots in their obsession with surveillance and personal data.[61]

Such mistrust of government practices persisted in the subconscious not only of the Germans, but of a significant part of the Europeans and gradually with the advent of digital technology transformed to a contemporary set of ‘‘*crises of trust*’’ in individuals, organizations and social groups.[62]

3.1.2. Greece

Similarly, the Greek post War anti-liberal governments’ and particularly the military junta’s practice of keeping files not just for dissidents, but for a broad part of the population, even today subconsciously corelates the collection of personal data by the state, to oppression.

3.1.3. USA

The United States having not felt the rule of a totalitarian state and firmly believing to be the nation of the free people, approach the regulation differently. For instance, freedom of press outweighs privacy much more often than in Europe.[63]

Nevertheless, the truth is that the American citizens are also worried about their privacy, as shown by a 2000 Washington Post survey which found that 86 per cent of users are either very concerned or somewhat concerned about electronic privacy.[64]

---

[59] Sabine Davis, https://www.handelsblatt.com/today/handelsblatt-explains-why-germans-are-so-private-about-their-data/23572446.html?ticket=ST-855776-drIUHOli4Cr0ITOmTLsf-ap4

[60] Der Spiegel, 28-10-2013 p.21

[61] https://www.dw.com/en/times-change-but-german-obsession-with-cash-endures/a-43718626

[62] Ethics Advisory Group of the European Data Protection Supervisor, 2018 report p. 20

[63] Kurt Wimmer, Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers, 68 SYRACUSE L. REV. 577 (2018).

[64] Theodore Grossman & Aaron M. Grossman, Understanding Internet Privacy: The US Perspective, 29 Int'l Bus. Law. 391 (2001).

3.2. Digital technology

Another big factor behind personal data regulation is the pace of digital technology. Technology has always generated concerns about unpredictable future consequences. The modern digital information technology creates to many people Orwellian anxieties: "*The relentless march of the omnipresent and totalizing mediation of information technologies onto, and into, our daily lives, is like air, everywhere. Without air we die, yet with too much we die as well*".[65] People believe that due to modern digital technology, never before so much information about them was available to others, they are confused about how to access such information and fear that if circumstances or motives change in the future, they are not going to be able to delete it.[66]

Such worries are implicitly confirmed by recital 6 of the GDPR: ''*Rapid technological developments and globalisation*''. Even though, as mentioned in the introduction, one of the supposed aims of the legislation is the facilitation of the free flow of information, and even though technology and globalization are the two key boosters of the flow of information, it seems, as later on will be suggested, that too much facilitation worries the European legislator.

3.3. Ethics

The Europeans supposedly base demands for privacy and personal data protection also from an ethical point of view to human dignity, which, as Kant famously wrote, mandates that people be treated as ends in themselves, not simply as means, tools or instrument of other's aims.[67]

In that spirit James Whitman acknowledges that dignity concerns are weightier in Europe while liberty interests predominate in the United States.[68] However, Spiros Simitis rejects this view of the European approach by Whitman, highlighting the European obligations to protect privacy in both their internal regulations and external

[65] Gary T. Marx, A Less Perfect but Freer Society, 4 Eur. Data Prot. L. Rev. 420 (2018).
[66] Bart van der Sloot, Editorial, 5 Eur. Data Prot. L. Rev. p.3 (2019).
[67] Anita L. Allen, Debating Ethics and Digital Life, 5 Eur. Data Prot. L. Rev. 11 (2019).
[68] James Q. Whitman, The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale L.J. 1151 (2004), David J. Stute, Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, 36 Mich. J. Int'l L. 663 (2015).

agreements, without sacrificing liberty for dignity. [69] According to his view it is not dignity versus liberty, but the duty to secure the best possible privacy protection for persons concerned, while freedom of the press generally prevails over privacy in the United States. [70]

3.4. National mentalities

3.4.1. France

Apart from fears and ethics, other sorts of feelings are also present behind the evolution of the European privacy legislation.

Take for example the less surveillance-phobic French. Behind the debate about personal data protection regulation in France, aside from the concept of privacy and the respect of it, hides the traditional French anti-Americanism and the rejection of the American culture as an expression of the legendary French chauvinism.

In the eyes of the French, modern technology is one of the core elements of the ‘‘American way of life’’. This is not to say that French are backwards or luddites; on the contrary, but technologies coming from the United States enjoy a ‘‘love-hate’’ relationship in France.

President d'Estaing had commissioned the famous “1978 Nora-Minc Report”[71] on the way computers may influence French society, with particular emphasis on telecommunications. The report had an enormous impact in France, constituting the theoretical foundation of the French nascent cyber policy and concluding that American digital hegemony poses an existential threat to the economic, social, and political fabric of the French nation and that France must develop an alternate model of cybergovernance to rival the domineering American computer industry.[72]

The internet, as the most important ‘‘information highway’’ of today is the most characteristic example of a mistrusted technology in France, as it is dominated by the American tech giants.

---

[69] Spiros Simitis, Privacy - An Endless Debate, 98 Calif. L. Rev. 1993 (2010).
[70] Ibid., p.1994
[71] Zarine Kharazian, Yet Another French Exception: The Political Dimensions of France's Support for the Digital Right to Be Forgotten, 3 Eur. Data Prot. L. Rev. 454 (2017).
[72] Ibid., p.456

It is also resented, because the popularization of the internet happened approximately a decade after the launch of Minitel, an online service, accessible through telephone lines and the world's most successful online service prior to the World Wide Web. [73] It was installed in one million French homes by 1985 and at the end of the 1980s, nine million terminals were linked to some 25,000 Minitel services[74], at a time when almost nobody outside the universities knew the internet. And yet, in a few years' time the internet redefined the world, while Minitel fell in oblivion and was officially terminated in 2012. That was a blow for the French pride. Even a much-publicized mock trial of the Internet was held as the main attraction of a national festival in 1998, expressing the willingness of the French to lead the Western resistance against American digital hegemony.[75]

Recently, the Edward Snowden revelations about the acts of surveillance of security agencies, fueled the skepticism of entrusting U.S. technology companies with large quantities of personal data.[76]

Such mistrust and antipathy for the American digital information companies is characteristic in France, but by no means restricted there. It seems to be a dominant trend in Europe and it is reflected in the most famous judgment of the CJEU on personal data against the leading American player in the field of digital information technology, Google. [77]

3.4.2. Netherlands

However dominant, this trend is not universal in Europe. For instance, in contrast to the CJEU, on two similar cases concerning the ''right to be forgotten'' a Dutch court in Amsterdam[78] began by stressing that the right to privacy is not absolute, that the right

---

[73] Wikipedia, Minitel

[74] John Lichfield, How France fell out of love with Minitel, The Independent, 9 June 2012

[75] Zarine Kharazian, Yet Another French Exception: The Political Dimensions of France's Support for the Digital Right to Be Forgotten, 3 Eur. Data Prot. L. Rev. 453 (2017).

[76] David J. Stute, Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, 36 Mich. J. Int'l L. 654 (2015).

[77] Case C-131/12 Google Spain SL and Google Inc. v Agencia Espatiola de Protecci6n de Datos (AEPD) and Mario Costeja Gonzalez [2014] EU:C: 2014:317

[78] Rechtbank Amsterdam, 18 September 2014, ECLl:NL:RBAMS:2014;6118 and Rechtbank Amsterdam, 13 February 2015, ECLI:NL:RBAMS:2015:716.

of freedom of expression is protected by the Dutch Constitution as well as the ECHR[79] and that because of the fact that the internet contains ''an ocean of information'', search engines, such as Google, play an important role in society as they help people to find information online. If search engines were subject to too many restrictions, their cataloguing function would be hampered, resulting in a loss of credibility for those search engines.[80]

Aside of the legal argumentation and the different approach to the balancing of rights between the CJEU and the Dutch Court, no doubt that a big role plays the approach to entrepreneurship. In terms of economic liberty, the Dutch (as well as the British and the Irish), are more liberal, strive more to attract foreign investments and enterprises, than the French and more or less the rest of Europe and are less hostile to American companies.

It is likely that the CJEU when judging on "the right to be forgotten", would consider more the freedom to expression, to information and to conduct business, if the search engine was European, if there was no dominance of Google and if the field was more fragmented and balanced between the continents.

3.4.3. Japan

Outside Europe, the reflection of national culture to the judicial approach to the protection of privacy, is even more characteristic in Japan.

In contrast to the CJEU, the Supreme Court of Japan rejected in January 2017 a deletion claim against Google, putting higher emphasis on society's "right to know".[81] The claimant had submitted that by using the search engine, his acquaintances could easily find out about his criminal record, that during the more than five years after the sentencing he could reflect on his actions and that he had started a new life.[82]

With reference to Google's interest in publishing, the court stated that not only the individual's personal circumstances should be considered, but also the historical and

[79] Article 10 ECHR

[80] Stefan Kulk; Frederik Zuiderveen Borgesius, Freedom of Expression and Right to Be Forgotten Cases in the Netherlands after Google Spain, 1 Eur. Data Prot. L. Rev. p.120 (2015).

[81] Frederike Zufall, Challenging the EU's Right to Be Forgotten: Society's Right to Know in Japan, 5 Eur. Data Prot. L. Rev. 18 (2019).

[82] Ibid., p.20

social significance of the crime, its severity and importance for the parties, the purpose and necessity of mentioning the individual's full name in the publication, the important role of a search engine for freedom of expression and the "right to know" by providing the means to access relevant information to society. Regarding the legal argumentation, the court not only recognized the right of access to information, but also affirmed the search engine provider's own "freedom of expression".[83]

The different judicial approaches reflect the European individualism, placing the fundamental rights to privacy and data protection ahead of the general public interest, while in Japan it was more important whether the facts as such were in the public interest. Japanese law and judiciary thus take the viewpoint of society, placing the emphasis on social values, as the concept of social harmony is one of the key characteristics of Japanese culture.[84]

4. THE PRINCIPLES OF THE GDPR

Having viewed the history of the regulation and some paradigms of cultural elements, we arrive to the GDPR, which was proposed as a data protection reform package in 2012, adopted in 2016 and came to force in 2018.

In part, the GDPR confirms choices made by the EU legislator and the CJEU in the context of the DPD95. However, many new elements have been introduced.[85] Apart from the extended territorial scope, the most important are a much higher standard required of controllers and processors, greater accountability and transparency, a wide spectrum of reporting requirements,[86] the accord of specific rights to the data subjects, among them particularly ''the right to be forgotten'',[87] the introduction of the

[83] Ibid., p.22
[84] Ibid., p.23
[85] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, p.3
[86] Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle, 2 Eur. Data Prot. L. Rev. 290 (2016).
[87] Article 17

data processing officer,[88] the organization of the independent supervisory authorities and of course the widely known and dreaded administrative fines.[89]

All these provisions are important and the infringements can inflict serious consequences. However, the core of the data protection regulation in the EU are the principles of the processing of the personal data.

It has been claimed that data protection law is ''*a bundle of principles"* and that they "*carry the data protection architecture*",[90] which is true, even if especially the GDPR contains numerous technicalities, procedures and specific provisions as well, which cannot be characterized as principles.

The data protection law is based in the contemporary prevailing European ethics and principles are abstract expression of ethics. Their central role in the GDPR reflects the choice of the European regulators for the data protection rules to be ethics oriented. This is why the European Union Data Protection Supervisor urging for greater attention to ethics and an Ethics Advisory Group,[91] issued a report early in 2018, "Towards a Digital Ethics", highlighting the role of traditional European values of dignity, personhood and democracy in the protection of personal data in the modern digital age.[92]

Such traditional values and ethics may be firmly established in Europe, but their context is constantly evolving. The principles of the European personal data protection serve the cause of the adaptation of the legislation to such evolution of the ethics. The need for such adaptation is greater when it concerns a fundamental right such as privacy, which is a mental construction and less tangible than life or property, for example. The European legislator acknowledges this reality and the inability to be constantly specific and up to date and gives way to the judge. The more principles the provisions of a law contain, the more the judge assumes the role of the legislator. This effects to more flexibility, but also less legal certainty.

---

[88] Articles 37-39

[89] Article 83

[90] Paul De Hert, Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules: Piercing the Veil of Stability Surrounding the Principles of Data Protection, 3 Eur. Data Prot. L. Rev. 160 (2017).

[91] convened by the Supervisor Giovanni Buttarelli and chaired by J Peter Burgess

[92] Anita L. Allen, Debating Ethics and Digital Life, 5 Eur. Data Prot. L. Rev. 10 (2019).

4.1. OECD Guidelines on the Protection of Privacy

The principles of GDPR trace their origins in the Council of Europe and OECD Principles, both proclaimed in September 1980.

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data introduced 8 Basic Principles of National Application: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability.[93]

4.2. Convention 108

Article 5 of the Convention (108) introduced the data quality principle which encompasses the principles of lawfulness[94], legitimate purpose[95], purpose limitation[96] , accuracy[97] and time limitation[98].

4.3. From Directive 95/46/EC to the GDPR

The DPD95 named five almost identical predominant principles: The principle of lawfulness and fairness of the processing,[99] the principle of purpose limitation,[100] the principle of data minimization,[101] the principle of accuracy[102] and the principle of storage limitation.[103] In a way these principles reflect the elements in the analysis of the proportionality,[104] one of the foremost general principles of European law.[105]

In terms of this continuous evolution of the European privacy law, under the GDPR, the principles for the processing are largely the same as those of DPD95 and Article 5

[93] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[94] Art. 5 (a)

[95] Art. 5 (b)

[96] Art. 5 (c)

[97] Art. 5 (d)

[98] Art. 5 (e)

[99] Art. 6 (1) (a)

[100] Art. 6 (1) (b)

[101] "adequate, relevant and not excessive", Art. 6 (1) (c)

[102] Art. 6 (1) (d)

[103] Art. 6 (1) (e)

[104] Raphael Gellert, On Risk, Balancing, and Data Protection: A Response to van der Sloot, 3 Eur. Data Prot. L. Rev. 182 (2017).

[105] Art. 5 TEU

GDPR is an enriched copy of Article 6 of the DPD95, [106] introducing some clarifications and additions: the element of transparency of data processing added to the principle of lawfulness and fairness, the principle of integrity and confidentiality and the principle of accountability. Outside article 5, new and more extensive conditions and elements for lawful processing are introduced in article 6 and special conditions for consent in article 7, which constitutes one of the bases for the lawfulness of the processing.[107]

So, it may be supported that article 5 of the GDPR together with its clarifications and additions in Articles 6 and 7 contains the core of the general provisions on data processing[108] and holds a central place in the Regulation. Infringement of the principles are explicitly subject to the administrative fines of up to 20.000.000 euros or up to 4 % of the total worldwide annual turnover.[109]

Summing it up, the GDPR in article 5 sets out the seven key principles for processing personal information.

4.3.1. First principle: “lawfulness, fairness and transparency” art. 5 (1) (a). Lawfulness

The first and most important principle is labeled “principle of lawfulness, fairness and transparency”. The requirement all processing of personal data to have a lawful, fair and transparent basis. 'Processing' includes all activities that relate to the collection, storage and use of data, including processing to alter data from an identifiable to non-identifiable form.

The importance of this principle is highlighted from the fact that the next article 6 is dedicated to concretize the element or ‘subprinciple’ of lawfulness, which does not necessarily require a legislative act adopted by a parliament. Article 6 provides six bases.[110]

[106] Daniel Rücker, Tobias Kugler, New European general data Regulation, Beck-Hart-Nomos 2018, p.49

[107] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Review: The International Journal of Technology Law and Practice 5 (2017)

[108] in contrast to Article 8 which contains special provisions for a special category of data subjects, namely children and falls out of the scope of this paper

[109] Art. 83 (5) (a)

[110] Recital 41

4.3.1.1. First basis: 'consent' art. 6 (1) (a)

The first basis for the processing to be lawful is the acquisition of consent from the data subject, specifically for the purposes for which the data is processed.[111]

Consent is further elaborated in article 7, which underlines that it has to be given freely via a positive act, as absence of refusal doesn't suffice, be informed according to article 14, specific, unambiguous and has to remain for the entire duration of the processing, as it is withdrawable, according to article 7 (3).[112]

Such high threshold for consent, particularly as elaborated in recital 39, makes it particularly difficult, if not impossible for companies to acquire. To be adequately informed according to the specifications of the law, the data subject has not only to be given a thorough text of the conditions of the processing, but also the same data subject has to herself process these conditions in order to provide a conscious consent. Expectations that an individual will make an informed decision about privacy when faced with competing considerations to be weighed in a single moment of absolute consent, seem optimistic. It is furthermore observed, that the idea of social media users making conscious, rational and autonomous choices about the disclosure of their personal data is highly 'questionable.[113]

Thus, what happens in practice is that lawyers compose long texts, which often nobody, not even the entrepreneurs read and the data subject just ticks, or signs. When such texts are submitted to courts, they are unlikely to be admitted as grounds for a lawful consent. And even when a collector of data undoubtedly obtains consent, he still cannot know for how long, because it depends on the absolute and arbitrary volition of the data subject, who can withdraw it anytime, a fact which creates great uncertainty to the data controller or processor.

[111] Art. 6 (1) (a)

[112] Recital 39

[113] Sheng Yin Soh, Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour, 5 Eur. Data Prot. L. Rev. 67 (2019).

4.3.1.2. Sixth basis: 'legitimate interest' art. 6 (1) (f)

A survey[114] showed that companies are aware of such demanding requirements and that they view "legitimate interest", which is an alternative basis[115] to consent as an easier reliance.[116]

It has to be also noted that, according to Article 29 Working party, when the initial basis of processing is consent, it is forbidden to "swap" this basis to another one for example legitimate interest,[117] if consent is withdrawn. Such requirement seems unjustifiable, since the other alternative five bases of article 6 are of equal strength to the consent. What if the two simultaneous bases are contract and consent and the data subject later withdraws consent? It is absurd to suggest that the personal data would no longer be processible, although a contract will be still binding.

Nevertheless, to justify a legitimate interest in the first place is not easy.[118] What is a legitimate interest, it is not defined in the GDPR. Of course, it has to be in accordance with the law in general, to be legitimate.

The GDPR gives some non-exhaustive examples of the legitimate interests for example in recital 47, such as when the data subject is a client, or for preventing fraud, or for marketing purposes, but there cannot be a clear distinction to a legitimate purpose of the article 5 (1) (b) for example. Somebody cannot help but wonder, why preventing fraud is a legitimate interest of art. 6 (f) and not a legitimate purpose of art. 5 (1) (b). A purpose is literally a target, whereas an interest means a psychological relationship or stake to something. It is obvious that a clear distinction is hard to be made.

Laws are destined to contain abstract terms, because no legislator can foresee all possible circumstances and legal scholars are doomed to scholastically dig under the words. However, when a law contains more than one abstract term with a similar meaning, apart from legal insecurity, the outcome is often confusion.

---

[114] The Centre for Information Policy Leadership & AvePoint, 'Organisational Readiness for The European Union General Data Protection Regulation' (AvePoint 2017), downloadable after registration at <http://www.informationpolicycentre.com/ global-readiness-benchmarks-for-gdpr.htm l>.

[115] Article 6 (f)

[116] Wim Nauwelaerts, GDPR - The Perfect Privacy Storm: You Can Run from the Regulator, but You Cannot Hide from the Consumer, 3 Eur. Data Prot. L. Rev. 253 (2017).

[117] Article 29 Working party, Guidelines on consent under Regulation 2016/679 [2017] p.23

[118] Wim Nauwelaerts, GDPR - The Perfect Privacy Storm: You Can Run from the Regulator, but You Cannot Hide from the Consumer, 3 Eur. Data Prot. L. Rev. 253 (2017)

According to the findings of the second Global GDPR Readiness Report released on March 26, 2018, tracking the GDPR implementation efforts of over 235 multinational organizations, legitimate interest remains the area most in need of clarity under the GDPR, followed by data protection impact assessments and risk, breach notification, notice and consent, and privacy by design.[119]

Nevertheless, defining the concept of the legitimate interest of art. 6 (1) (f), which is the fifth alternate basis for lawful processing, is not the only difficulty, as a bearer of a legitimate interest also has to prove, that such a legitimate interest is not overriding the interests or fundamental rights and freedoms of the data subject. The term "override" refers to a central examination procedure in the data protection law: The "weighing", or "balancing", a judicial task, which we are going to comment on later.

4.3.1.3. Second basis: 'performance of a contract' art. 6 (1) (b)

Coming back, after having jumped to the article 6 (1) (f), the second alternate basis for processing to be lawful is the necessity of the processing for the performance of a contract of article 6 (1) (b), which is not entirely alternate to the previous one (consent), but rather a subcategory of it, as no contract can be formed without the willing exchange of the necessary details.

The raison d'être of this basis is, that if a contract is still binding, even if the data subject withdraws her consent, the processing remains lawful. This basis is one of the most concrete, but is also self-evident. Because if it didn't exist (a paranoid assumption), this would mean that data protection put an end to contracts altogether. The mere existence of this concrete clause may allow the connotation that the legislator by needing to include a basis so self-evident in the law, implies, if not underlines, the lawfulness of the processing of personal data as an exception and not the rule.

4.3.1.4. Third basis: 'legal obligation' art. 6 (1) (c)

The third alternate basis is compliance with a legal obligation of the controller of article 6 (1) (c), which together with the fifth basis of point (e), namely the

[119]CIPL & AvePoint, 2nd GDPR Organisational Readiness Survey Report, accessible at https://www.informationpolicycentre.com/global-readiness-benchmarks-for-gdpr.html

performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, are to be laid down in either European or Member State legislation, to which the controller is subject. These two alternate bases constitute a serious crack in the harmonization of the data protection regulation, in view of the varying national policies of the member states.
Furthermore, according to the CJEU, the processing has to be necessary for the compliance with the legal obligation.[120]

4.3.1.5. Fourth basis: 'vital interests' art. 6 (1) (d)

The fourth alternate basis of lawfulness is the protection of the vital interests of the data controller or another natural person. Recital 46 defines the term "vital interest" as an interest which is essential for the life of the data subject.[121] Risking a brash assumption, I would say that the need of the legislator to clarify again something so self-evident, as that human life is above privacy, seems either another implicit expression of how sacred privacy is, that risks to be considered on par with the human life, or naïveté.

4.3.1.6. Fifth basis: 'performance of a task' art. 6 (1) (e)

The fifth alternate basis of lawfulness, that data processing *"is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" according to Article 6 (1)(e) is most likely to be appropriate for public authorities processing personal data without individual consent.[122]

These are the six alternate bases or conditions of the "subprinciple" of lawfulness of the first principle 'lawfulness, fairness and transparency' of art. 5 (1).
Continuing with the other two terms (or subprinciples) of this clause, "fairly" is equally if not more abstract than the others. Does "fairness" imply equality of guns, or that

[120] Case C-496/17, Deutsche Post AG v Hauptzollamt Köln [2019] ECLI:EU:C:2019:26 para. 58; see also Case C-201/14, Bara and Others [2015] EU:C:2015:638, para. 34
[121] Daniel Rücker, Tobias Kugler, New European general data Regulation, Beck-Hart-Nomos 2018, p80
[122] Jessica Bell; Stergios Aidinlis; Hannah Smith; Miranda Mourby; Heather Gowans; Susan E. Wallace; Jane Kaye, Balancing Data Subjects' Rights and Public Interest Research, 5 Eur. Data Prot. L. Rev. 45 (2019).

ethics must apply? Is it ever possible that a processing is lawful, according to the above five conditions of art. 6 and not fair? Don't expect an answer neither from the recitals. [123]

I would say that the term fair in art 5 (1) (a) is verbalism. Aside of the processing of personal data, is there any activity in general, which any law allows to be conducted in unfair modus? The consequence of verbalism in a law, where every word has to have if not an exact meaning, at least a 'reason d'être', is that it leads to fruitless over-analysis (as maybe is the case with this paper), but also to insecurity and reserve. When a prohibition is general and extensive and somebody cannot figure what is allowed because the exceptions to the prohibition are ambiguous and vague; when he even has to ensure that he processes the data 'fairly' (according to whose standards?), he may choose to abstain from data processing altogether, to avoid the risk of infringement, which will not facilitate the flow of information, a target of the GDPR according to its recitals.

Adding to the confusion, the CJEU commands that the requirement the processing to be fair, according to article 5 (1), means the obligation to inform the data subject of the purposes of the subsequent processing, which is the same with the transparency obligation.[124]

On the contrary, the term "transparent" is one of the most specific of the GDPR. The processing is transparent if all information about it is given to the data subject. Such obligation for transparency is concretized according to the provisions of articles 12-15, which provide specific relevant rights bestowed to the data subject.

The obligation for transparency is also one of the few elements of the principles against which no objection can be supported.[125] The processing should be transparent and the relevant rights of the articles 12-15 are themselves "fair". They serve to reduce mistrust and check arbitrariness of the controller.

The only remark is that the GDPR may rightly promote transparency, regarding the information provided to the data subject, but its unfriendly regime towards disclosure of personal data is functioning the opposite way, reducing transparency of the actions

[123] See recital 60 which gives identical interpretation to 'fairness' and 'transparecy' as the adequate provision of information to the data subject

[124] Case C-496/17, Deutsche Post AG v Hauptzollamt Köln [2019] ECLI:EU:C:2019:26 para. 59

[125] Article 29 Working party, Guidelines on transparency under Regulation 2016/679 [2017] p.6

of politicians or public servants, who fortify themselves behind personal data protection. [126]

4.3.2. Second principle: 'purpose limitation' art. 5 (1) (b)

The second principle is labeled "purpose limitation", according to which data must be collected for '*specified, explicit and legitimate purposes'* and not further processed in a manner that is incompatible with those purposes. We mentioned above the difficulty to legally distinguish between a purpose and an interest.

Examples of cases where law enforcement authorities request access to personal data initially collected by third parties for a different purpose are numerous. Many of them relate to the legal obligation of private parties to retain and disclose personal data to law enforcement authorities, such as in the fields of air transport, where according to directive EU 2016/681 airlines have to retain passenger data, or of banking for anti-laundering uncovering purposes, or of telecommunications, according to Directive 2006/24/EC.[127] Due to the availability of data and technological means to process them, the repurposing of data in the sense of re-use for a different purpose, is a growing phenomenon. When personal data are repurposed to be used in a different context, that repurposing might challenge the principle of purpose limitation. Following that principle, personal data collected for a specific purpose should be used for compatible purposes or further processed under a different legal basis. The situation becomes complicated when personal data have been collected in a particular context (such as commercial) and are further processed in a different one (such as law enforcement). But when rules on data protection are split between two instruments, like in the new EU data protection framework, the situation becomes even more complicated. The new framework is composed of a general legal text, the GDPR, and of

[126] See 5.9.

[127] Which was however invalidated by the EUCJ; see Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others [2014] ECLI:EU:C:2014:238; Catherine Jasserand, Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation, 4 Eur. Data Prot. L. Rev. 153 (2018).

a specific legal text applicable to data processing in the field of law enforcement, Directive 2016/680[128].

4.3.3. Third principle: 'data minimization' art. 5 (1) (c)

The third principle is labeled 'data minimization' according to which personal data have to be adequate, relevant and limited to what is necessary to achieve those purposes. It is self-evident that adequacy and necessity are abstract and subjective terms.

Moreover, at the time of collection of the data more often than not it is not possible to know the needs for data, that will emerge later. At the time of the signing of a contract for example, it is not known whether the parties will end up adversaries in a litigation. The latter often requires additional data, which may be 'not necessary' for the performance of the contract. 'Necessity' is an element of one of the cornerstones of European Law, the general principle of proportionality[129] but it has been analyzed (primarily by the European Judiciary) in retrospect, not as a prediction.

4.3.4. Fourth principle: 'accuracy' art. 5 (1) (d)

The fourth principle is labeled "accuracy", requiring data to be accurate and, where necessary, up to date, terms which are more concrete. Nevertheless, their necessity is questionable, since when the inaccuracy derogates the data subject, there are in every legal order civil as well as penal provisions protecting against defamation. Moreover, the requirement of the data to be always kept up to date may appear somewhat utopic, especially in the age of big data.[130]

4.3.5. Fifth principle: 'storage limitation' art. 5 (1) (e)

The fifth principle is labeled "storage limitation", which requires data to be kept in an identifiable form for no longer than necessary**.** This principle is encompassed in article 17 which formally introduces the so much debated "right to be forgotten".

The CJEU in Google Spain had firmly established the significance of timeliness of personal data, stating that Article 6(c) to (e) of the DPD required that data be

[128] Police and Criminal Justice Directive; Catherine Jasserand, Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation, 4 Eur. Data Prot. L. Rev. 153 (2018).
[129] TEU art 5
[130] See later, ch.5.6.

"adequate, relevant, and not excessive in relation to the purposes" of the data processing. [131] The meaning of this is that data might 'age' to become inadequate, irrelevant, or excessive. When this point is reached, the Court concluded that the information must be removed. But the Court didn't specify, when data goes beyond the "coming of age". [132]

The principle of 'storage limitation' is the framework of the articles 17 and 18[133], which provide some conditions[134] for this relevance of necessity to time, but even though they are analytical, they still are abstract and sometimes overlapping to other provisions of the GDPR. Moreover, articles 17 and 18 introduce rights, which means that the application of the provisions is subject to the exercise of the rights by the data subject. This leads to the conclusion that the principle of storage limitation is applicable only when the data subject is exercising its relevant rights. Otherwise, if we considered the principle of storage limitation as a general obligation, which means that there could be an infringement, even if no data subject exercised its rights, then the nature of the provisions of articles 17 and 18 as rights and not just specifications of the principle, would be contradictory. But this is the interpretation of this paper, whereas in the context of approach of the European legislator, who includes general principles together with detailed provisions, the intention may be the coexistence of a general obligation which includes the right and the same right again, under specific conditions.

4.3.5. Sixth principle: 'storage limitation' art. 5 (1) (f)

The sixth principle is labeled "integrity and confidentiality" according to which the processing has to be conducted in a manner that ensures appropriate security of the data.[135] This principle refers mainly to the articles 33-34 and the rest of the security technical obligations. This is one of the two new principles, that didn't exist in the DPD95 and highlights the advent of technology and especially the hazards of digital information technology, such as hacking, which were not so severe in the time of the adoption of the Directive.

[131] Google Spain SL v. AEPD, para. 92.
[132] David J. Stute, Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, 36 Mich. J. Int'l L. 665 (2015).
[133] Article 17 'right to erasure', article 18 'right to restriction'
[134] Out of the scope of this paper
[135] See also recital 49

4.3.5. Seventh principle: 'accountability' art. 5 (2)

Finally, the seventh new principle is labeled "accountability"[136] for compliance with each of these principles to be demonstrable by the accountable data controller, which is also self-evident.

Importantly, the GDPR provides for research exemptions from both the "purpose limitation" principle in Article 5 (1)(b) and the "storage limitation" principle in Article 5(1)(e), subject to considerable safeguards set out in Article 89 (1) being met.[137]

5. CRITISISM

The European Data protection regulation expressed in its latest version by the GDPR poses an array of difficulties.

5.1. Subjective approaces of privacy

First of all, the subject of protection, namely privacy, may hardly be considered a "tangible" right; on the contrary, as already seen, it depends on the subjective view of what everybody considers private. Equally difficult is the appreciation of the harm inflicted[138], as it depends on the psychological effect of the violation to the individual. We saw for example, that Germans are surprisingly relaxed with nudity, a condition which usually ranks very high in what people consider private.

Another example are again the Dutch. Whereas activities such as video surveillance of workplaces[139] in Europe and even of public places such as streets in Greece are sometimes considered a violation of privacy[140], the Dutch are notorious for having big windows on their houses without curtains and shades. The reason may be a Calvinist remnant in the predominantly atheistic Dutch society, but the striking consequence is, that a passer-by can often peek inside the most private of places, the residence.[141]

---

[136] Art 5 par.2

[137] Jessica Bell; Stergios Aidinlis; Hannah Smith; Miranda Mourby; Heather Gowans; Susan E. Wallace; Jane Kaye, Balancing Data Subjects' Rights and Public Interest Research, 5 Eur. Data Prot. L. Rev. 45 (2019).

[138] Tal Z. Zarsky, The Privacy-Innovation Conundrum, 19 LEWIS & CLARK L. REV. 151 (2015)

[139] See Köpke v Germany, App no 420/07 (ECHR, 5 October 2010), Antovit and Mirkovit v Montenegro App no 70838/13 (ECHR, 28 November 2017)

[140] See Directive 1/2011, Decisions 53/2011 and 136/2011 of the Greek Data Protection Authority

[141] See https://dutchreview.com/culture/why-dont-the-dutch-like-to-use-curtains/, https://www.expatica.com/nl/living/household/xenophobes-guides-open-curtains-107782/

Such variability of approaches makes it very difficult for the jurisprudence to harmonically interpret the abstract principles throughout the EU.

5.2. Pace of technological progress

The GDPR introduced some important innovations of the regulation, but it is questionable whether it broke new ground addressing the issues posed to privacy protection by the ever-evolving cultural mentalities and by the rapid advent of digital technology.[142] However, to be fair, maybe it is utopic to expect the simultaneous accomplishment of the two main objects of the European data protection regulation: The protection of privacy from digital technology and the harmonization of the regulation in the EU, because of the fragmentation of national views on the subject, the pace of the evolution of digital technology and the unfair race with the notoriously slow European regulators.

Digital information technology penetrates so extensively every moment of everyday life and it evolves so rapidly, that today's specific regulation will most likely become obsolete tomorrow. [143]

The GDPR, may contain many detailed provisions aiming primarily to address modern technology, but in a silent acceptance of this reality, the core of regulation is general concepts, namely the principles, which allow the judge to step into the shoes of the slow legislator.

5.3. Complexity

The length of the GDPR compared to the DPD and even more so when compared to the 1980 CoE Convention 108, has also been a subject for critic and even regarded as a sign of weakness and lack of capacity to trust the sacred principles.[144]

A major challenge is the companies' lack of awareness and understanding of the requirements that the GDPR imposes through its new detailed rules. A recent Decision

[142] Daniel Rücker, Tobias Kugler, New European general data Regulation, Beck-Hart-Nomos 2018, p.49; Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle, 2 Eur. Data Prot. L. Rev. 290 (2016).

[143] Tal Z. Zarsky, The Privacy-Innovation Conundrum, 19 LEWIS & CLARK L. REV. 125 (2015).

[144] Paul De Hert, Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules: Piercing the Veil of Stability Surrounding the Principles of Data Protection, 3 Eur. Data Prot. L. Rev. 173 (2017).

by the Greek DPA imposed a fine of 150.000 euros to a company because of violations apart from the principles of processing also of technical requirements by articles 24 and 34.[145] Such demands bring out the need to review and revise current data privacy practices, organizational systems, personnel training and technological data protection measures, as well as possibly plan new ones to ensure compliance with the GDPR. [146]

5.4. Balancing

The new technical requirements introduced by the GDPR raise more questions than answers in relation to how DPAs, controllers and processors, all accountable by the law, are going to achieve compliance in practice, and how they are going to enforce the rules.[147]

Nevertheless, more than the technical requirements, criticism attracts the fact that the balancing act needed to implement the principles of the European data protection law falls primarily on the shoulders of such DPOs, controllers and processors, who have to concretize such abstract terms as 'necessity'. In the case of Google Spain for example, not only the lack of regard or weight the Court gives to the freedom of expression has been critisized, but also that the Court leaves it up to the provider of the search engine, in this case Google, to perform the balancing exercise.[148] Having in mind the vast amounts of data processed, how can a search engine comply with obligations imposed on controllers by the principles under Articles 6 and 7, such as judging when it is "longer than is necessary for the purposes for which the data were collected,"? And how realistic is for a search engine to verify consent for the personal data it processes, as such data have been collected by infinite other controllers? As it is astutely observed, the absurd consequence would be that search engines themselves would be illegal under EU law.[149]

---

[145] Greek DPA Decision 44/2019, par. 31

[146] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Review: The International Journal of Technology Law and Practice p. 2 (2017)

[147] Christopher Hodges, Delivering Data Protection: Trust and Ethical Culture, 4 Eur. Data Prot. L. Rev. 75 (2018).

[148] Herke Kranenborg, Google and the Right to Be Forgotten, EDPL 74 (2015)

[149] David J. Stute, Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, 36 Mich. J. Int'l L. 660 (2015).

According to 'The Leff Dictionary of Law': '*Balancing: The metaphoric term generally used in the law to describe an exceedingly important conceptual operation. In almost all conflicts, especially those that make their way into a legal system, there is something to be said in favor of two or more outcomes. Whatever result is chosen, someone will be advantaged and someone will be disadvantaged; some policy will be promoted at the expense of some other. Hence it is often said that a "balancing operation" must be undertaken, with the "correct" decision seen as the one yielding the greatest net benefit*.'[150]

Balancing is the main tool for judges to determine the outcome of a case when there is a conflict of rights or interests. What is 'balanced' is not the pleasure an act brings about against the pain it causes. Instead, rights are balanced against each other, or against a general interest, such as national security, public health, or even against public morals.[151]

For example, the ECHR found in Barbulescu vs Romania[152] that even though Article 8 ECHR protects individuals against arbitrary interference by the public authorities, it may also generate positive obligations for the legislator, such as adopting measures designed to secure respect for private life. To fulfill their positive obligations under the ECHR, the states had to find a balance between the competing interests which may include competing private and public interests or Convention rights.[153]

Similarly, after the judgment in Barbulescu vs Romania, concerning the monitoring of employees' email communications by private employers, the ECHR heard a case this time concerning video surveillance in the workplace.[154] After having established that the applicants' private life was concerned by the video surveillance cameras, the ECtHR examined whether the State, by virtue of its positive obligations to adopt measures ensuring the respect for individuals' right to privacy, has correctly balanced the employees' right to privacy, the interest of employers in their property rights and, finally, the public interest in the proper administration of justice. It found that the employer did not comply with the legal obligation to notify the employees of the

[150] Arthur Allen Leff, The Leff Dictionary of Law: A Fragment, 94 Yale L. J. p. 2123 (1985)
[151] Bart Van der Sloot, Editorial 3 Eur. Data Prot. L. Rev. 2 (2017).
[152] Bărbulescu v. Romania [GC] - 61496/08 Judgment 5.9.2017 [GC]
[153] Ibid., par 52; Johannes Eichenhofer, Internet Privacy at Work - the ECHR Barbulescu Judgment, 2 Eur. Data Prot. L. Rev. 267 (2016).
[154] Lopez Ribalda And Others v Spain App nos 1874/13 and 8567/13 (ECtHR, 9 January 2018).

existence of hidden cameras installed in the workplace. And held that such surveillance measures were not justified and appropriate to the legitimate interest pursued namely the employer's right to property and not necessary and proportionate to restricting the privacy of the employees.[155]

This judgment contrasts with a previous similar case decided by the ECtHR in 2008, Koepke v Germany[156], regarding the dismissal of a supermarket cashier after having been caught by covert video surveillance cameras while stealing. In that case, the ECHR had not found any violation of Article 8 ECHR and recognized that national courts had correctly struck the balance between the employee's right to protection of private life and the employer's interest in the protection of its property rights and the public interest in the proper administration of justice.[157]

The concept of balancing is explicitly referred only in recitals 4 and 153 of the GDPR: '*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.'*[158] *Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights.*[159]

Although no material provision explicitly refers to balancing, it is understood that because data protection is based on privacy, which is considered a fundamental right, the power of data protection regulation to limit other fundamental rights often has to be the outcome of a balancing procedure.

Notably, article 6 (1) (f) providing for the lawfulness of the processing based on legitimate interest of the controller, mentions the condition that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject. The Article 29 Data Protection Working Party explicitly mentioned, analysed and

[155] Elena Kaiser, Monitoring Employees with Hidden Surveillance Cameras Breaches Their Right to Privacy, 4 Eur. Data Prot. L. Rev. 397 (2018).
[156] 420/07, [2010] ECHR 1725 Koepke vs Germany
[157] Elena Kaiser, Monitoring Employees with Hidden Surveillance Cameras Breaches Their Right to Privacy, 4 Eur. Data Prot. L. Rev. 398 (2018).
[158] Recital 4
[159] Recital 153

provided guidelines for the balancing test required when implementing article 7 (f) of the DPD, which is the same provision to the article 6 (1) (f) of the GDPR. [160]

The question is, are the controllers and processors, who can be anybody, capable of conducting such balancing acts? Imagine for example that a lawyer investigates the feasibility to bring a tort to litigation. He needs several pieces of information, not only if the defendant has property. It may sound trivial, but even the fathers' name may be missing[161]. The mere basis in the principles of articles 5 and 6 able to provide lawfulness to a disclosure of such personal data is the legitimate interest. The controller in possession of such personal data, how likely is it to be capable of ensuring the mere existence of the claim; of finding that it constitutes a legitimate interest and of balancing the overriding interests? Will the average controller, or the appointed DPO, if there is one, study the evidence of a tort case even before the filling of a lawsuit, and decide for the disclosure? Most unlikely. He will probably play it safe and refuse. And just imagine the case of more serious personal data, needed as evidence.

Moreover, serious critique, even before the introduction of the GDPR, earned the expansion of the scope of who is considered controller. According to Advocate General Niilo Jääskinen: "T*he potential scope of application of the Directive in the modern world has become surprisingly wide. Let us think of a European law professor who has downloaded, from the Court's website, the essential case-law of the Court to his laptop computer. In terms of the Directive, the professor could be considered to be a 'controller' of personal data originating from a third party. The professor has files containing personal data that are processed automatically for search and consultation within the context of activities that are not purely personal or household related. In fact, anyone today reading a newspaper on a tablet computer or following social media on a smartphone appears to be engaged in processing of personal data with automatic means, and could potentially fall within the scope of application of the Directive to the extent this takes place outside his purely private capacity. In addition, the wide interpretation given by the Court to the fundamental right to private life in a*

[160] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

[161] Article 118 of the Greek civil procedure law

data protection context seems to expose any human communication by electronic means to the scrutiny by reference to this right" [162]

5.5. Freedom to conduct business (art. 16 of the Charter)

The elevated level of data protection by GDPR, the strict liability of both controllers and processors and the height of the relevant administrative penalties has very much increased concerns among enterprises.[163]

As research and development is based on information, and because data protection legislation raises barriers to the free flow of it, one of the anticipated concerns is that the GDPR may harm entrepreneurial innovation. So, it is remarkable, that the opposite logic is supported by regulators, namely that privacy enhances trust, which leads to more online and virtual engagement, which leads to greater market, social and technical innovation.[164]

According to the Commissioner Viviane Reding '*The new rules also give EU companies an advantage in global competition. Under the reformed regulatory framework, they will be able to assure their customers that valuable personal data will be treated with the necessary care and diligence. Trust in a coherent EU regulatory regime will be a key asset for service providers and an incentive for investors looking for optimal conditions when locating services*.'[165]

However attractive such a reasoning may sound, it clearly reflects the bureaucratic way of thinking, not of the entrepreneur and it is hard to agree to a paradox that putting obstacles to the flow of data through regulation (because that is what the GDPR does) is going to give an advantage against oversees companies, who operate unregulated. The simple counter-argument is that, if regulation was giving a competitive advantage, then companies would apply the rules themselves and no law would be necessary. [166] Whether privacy rights are 'weightier' than profits is debatable, but the assumption that the GDPR instead of harming profits, will push

[162] Opinion of Advocate General Jaaskinen, Google Spain SL v. AEPD, par. 29

[163] Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle, 2 Eur. Data Prot. L. Rev. 291 (2016).

[164] Tal Z. Zarsky, The Privacy-Innovation Conundrum, 19 LEWIS & CLARK L. REV. 129 (2015).

[165] Viviane Reding, The European data protection framework for the twenty-first century, International Data Privacy Law, 2012 vol2, No3, p. 129

[166] Tal Z. Zarsky, The Privacy-Innovation Conundrum, 19 LEWIS & CLARK L. REV. 130 (2015).

them upwards facilitating innovation, cannot be supported. Strict regulation promotes business climate and attracts investors, when it addresses the function of the state, the public sector and the judiciary; when it tackles corruption and exclusion; when it reinforces competition rules. But not when it restricts the private sector from violating personal data rights.

Another argument in favor of the assumed positive impact to innovation is that conditions of diminished privacy also impair innovation because a society that permits the unchecked ascendancy of surveillance infrastructures, leads individuals to engage in constant self-monitoring and conforming behavior-mindsets that are arguably destructive to the processes that promote innovation.[167] In other words, fear of surveillance, stops individuals from engaging in research and development activities, which create innovation. However, aside from data protection theorists and regulators, it is hard to find entrepreneurs, researchers and academics who claim that privacy promotes innovation. Innovation requires infrastructure, venture capital, freedom to experiment, cooperation between colleagues, communication webs, and access to databases, hardly personal data protection.

Aside from these theoretical arguments, reality shows that Europe with its strict regulation regime lags back in innovation against the United States (with a much more lenient personal data protection regime), especially in the field of digital information technology. Does anybody think that the GDPR will help Europe produce the equivalent of an innovation leader, such as Google, Facebook, Twitter, eBay or Amazon?

5.6. Big Data

Personal Data is said to be the new oil[168] and the way modern economies need oil, they also need 'Big Data'.[169] Big Data is a field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software. [170] It is collected primarily in an automated way, through myriads of devices,

[167] Julie Cohen, What is Privacy for, 126 Harvard Law review 2013 p.1918
[168] Lee Bygrave, Data Privacy Law, An international perspective, Oxford University Press (2014), p.4
[169] Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 SETON HALL L. REV. 996 (2017).
[170] Wikipedia, Big Data

sensors, applications, which record preferences, websites visits, physical movements, communications, transactions even biometrics. It is stored using sophisticated mechanisms on distributed databases and it is used in advanced analytical processes and thereafter applied in a variety of contexts. Big data has the potential to create vast amounts of value in many sectors, improving economies, determine new winners in the private sector and bring consumers benefits and conveniences.[171] It is already transforming the world and nobody can really predict the scope and nature of the impact of Big Data impact to the future.[172]

The GDPR indirectly addresses Big Data in the article 22, which introduces provisions regulating decision-making processes, which are both fully automated and substantially impact individuals, such as credit applications or recruiting. Article 22 provides the individual with the right not to be subjected to these processes and is the most characteristic rejection to the (mostly automated) extraction of Big Data. The American law has no equivalent to this right.[173]

More importantly Article 5(1)(b) and (c) of the GDPR sets forth the purpose limitation and the data minimization principles, which are clearly at odds with the prospect of Big Data analyses. When collecting Big Data, due to their nature, it is practically impossible for the controllers to predict or imagine methods, usage patterns, exact purposes and required volume of the data. To comply with the purpose limitation principle, processors have to inform their data subjects of the future forms of processing and closely monitor their practices to assure they did not exceed the permitted limits of analyses. Carrying out any one of these tasks in the realm of Big Data analytics is hardly realistic. [174] The contrast of the data minimization principle to Big Data needs not to be analyzed, as the principle is an explicit antithesis to the concept of Big Data.

Finally, article 25, which introduces the obligation of the controller to implement by design and by default appropriate technical and organisational measures such as data minimization is totally incompatible with Big Data procedures.

---

[171] Angela Byers, Big Data, Big Economic Impact, 10 ISJLP 764 (2015).

[172] Yuval Noah Harari, Homo Deus, Harper Collins 2016, especially the last chapter for a thought provoking and entertaining approach as the author claims the emergence of a 'data religion'

[173] Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 SETON HALL L. REV. 1015 (2017).

[174] Ibid., p.1005

Such obstacles and a hostile legal regime against Big Data is very likely to turn Big Data investment and enterprises away from Europe, which will not only effect in losses in profits and jobs but it will also leave the EU further behind in the 'next big thing' of progress.

5.7. Free speech-freedom of expression

When search results are delisted, the right to freedom to receive as well as impart information, the right to freedom of expression for short, is affected as well. When people publish information on the web and their publications are harder to find due to a delisting, their freedom to impart information is interfered with.[175]

Both the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights protect the right 'to receive and impart information and ideas without interference by public authority and regardless of frontiers.[176]

According to the ECtHR, Article 10 of the ECHR applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information. [177]

Similarly, as the Advocate General in the Google Spain case held, a "*search engine service provider lawfully exercises his freedom of expression when he makes available internet information location tools relying on a search engine*."[178]

5.8. Scientific Research

Concerns have also been expressed for a potential disruption to the scientific research, particularly in the field of social sciences, although not as convincing as in other fields.

It is claimed that negative implications may arise from the introduction of pseudonymous data as a subset of personal data[179] and that the GDPR may disrupt the access to administrative data for research which serves the public interest, especially

[175] Stefan Kulk; Frederik Zuiderveen Borgesius, Freedom of Expression and Right to Be Forgotten Cases in the Netherlands after Google Spain, 1 Eur. Data Prot. L. Rev. p.114 (2015).

[176] Art 11(1) of the Charter of Fundamental Rights of the European Union and art 10 of the European Convention on Human Rights.

[177] Autronic AG v Switzerland App no 12726/87 (ECHR, 22 May 1990) [47].

[178] Opinion of Advocate General Jaaskinen, Google Spain SL v. AEPD, par. 131

[179] Leslie Stevens, The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK, 1 Eur. Data Prot. L. Rev. p. 97 (2015).

as it adds some uncertainty as to the scope of processing of personal data that public authorities can undertake without the justification of a new, separate legal basis.[180]

However, several articles and recitals[181] clarify that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations, which seems to be adequate to remove uncertainty, provided that the fear of the accountability principle, especially among public servants will not stand in the way.

5.9. Transparency

The principles of GDPR may also conflict with the principle of transparency of the conduct of public authorities. The balancing of the two sides pose difficult and controversial issues, without a clear acceptance of the predominance of public transparency, as shown by the case-law of the CJEU.[182]

In Dennekamp Case a journalist was denied public access to European Parliament documents relating to a pension scheme for MEPs. The General Court held that no automatic priority can be conferred on the principle of transparency or access to information[183] over the right to protection of personal data and that the conflicting interests had to be balanced, or, in the words of the Court, *"weighed up"*. [184] Personal data shall only be disclosed to recipients "*if the recipient establishes the necessity of having the data transferred and if there is not the slightest reason to assume that the data subjects' legitimate interests would be prejudiced"*.[185]

The Court thus set the threshold high, allowing only the disclosure of the names of those MEPs who participated in such decisions, but not of those who although members of the pension scheme, did not participate in the vote for it.[186]

In ''ClientEarth and PAN Europe'' case the applicants were environmental NGOs. They applied for disclosure of the names of external experts who authored a European Food

[180] Ibid., p.98

[181] Art. 5 (1) (b) and (e), 9 (2) (j), 14 (5) (b), 17 (3) (d), 21 (6) 89 ; recitals 26, 52, 53, 62, 65, 71, 113, 156, 162, 163

[182] Jan Oster, Of Money, Poison and Secrets: Balancing Freedom of Information against Data Protection, 2 Eur. Data Prot. L. Rev. 272 (2016).

[183] Articles 1 and 11(2) TEU and Article 15(1) TFEU

[184] Case T-115/13 - Dennekamp v Parliament, par.116

[185] Case T-115/13 - Dennekamp v Parliament, par.117, 119

[186] Jan Oster, Of Money, Poison and Secrets: Balancing Freedom of Information against Data Protection, 2 Eur. Data Prot. L. Rev. 274 (2016)

Safety Authority (EFSA) guidance document on pesticides. The General Court had dismissed the applicants' action for annulment of EFSA's refusal to allow access to the relevant documents for reasons of protection of personal data of the external experts.[187] However, the ECJ balancing between data protection and transparency, set aside the General Court's decision and decided in favor of the disclosure, holding that the 'climate of suspicion of EFSA', which is *'often accused of partiality because of its use of experts with vested interests due to their links with industrial lobbies'*, resonates '*the necessity of ensuring the transparency of EFSA's decision-making process*', which increases public confidence.[188]

Another example is the case ''Manni''.[189] The CJEU examining the balancing between personal data protection against the principle of the free flow of and access to public registers, appeared to bend more towards transparency and the interests of third parties regarding information about companies, than to a right to be forgotten, but also found that such disclosures are subject *'on the basis of a case-by-case assessment*', avoiding to adopt a clear stance, even on the need for absolute transparency in the field of corporates, as in every liberal economy, anywhere outside Europe. [190]

Especially in Greece there is an overzealous protection of personal data, when it comes to public servants or politicians, taking advantage of the abstractness and extensive scope of the provisions.

An example was a public debate about the salaries of the employees of the public tv channels (ERT), which were rumored to be scandalously high in spite of the very low attendance figures of the channels. The salaries are paid by the tax-payers and some MPs officially asked for their disclosure. The competent minister refused, citing personal data. [191]

---

[187] Ibid., p.273

[188] Case C-615/13 P - ClientEarth and PAN Europe v EFSA par. 53, 56

[189] Case C-398/15 – Manni

[190] Case C-398/15 – Manni par. 49; Eike Michael Frenzel, Facilitating the Flow of Public Information: The CJEU in Favour of Distinctive Rule/Exception Regulations in Member States, 3 Eur. Data Prot. L. Rev. 283 (2017).

[191] Pashos Mandravelis, Kathimerini 9.11.2017
<https://www.kathimerini.gr/933854/opinion/epikairothta/politikh/ta-kryfa-dedomena>

Such practices are usual in Greece, so when the economy defaulted, the public conception was that a small group of powerful people ''stole the money'', instead of that there were widespread fiscal extravagances in the public sector.

5.10. Intimidation-exploitation

The complexity of the GDPR, the expansion of its scope to include every information related to an individual and the vagueness of the principles of the processing have another side-effect. They gave birth to an 'army of experts' selling GDPR compliance services.

According to a pertinent remark "*It seems the GDPR rhetoric is suffering from the famous Mark Twain quote, 'To a man with a hammer, everything looks like a nail.' We cannot call every problem in society a privacy or data protection issue nor should we attempt to: recently a privacy lawyer tried to convince me that contract law is a subset of privacy law because a contract contains personal data as the names of those signing are in it …The GDRP is mainly about exploitation and monetisation, with the famous 4%-of-global-turnover fine as its crown jewel. Many GDPR-ists behave like ambulance chasers and use it for scaring clients*." [192]

The "intimidating" nature of the provisions of the GDPR is also capable of deterring people from exposing illegal activities, in fear of infringing the limited understood data protection provisions.

There are also fears that actual intimidation may follow. Similar practices to the "Abmahnungen"[193] based on German unfair competition law - combined with a fee for the production of the letters - could follow to attack supposed privacy violations. Some warn of the launch of a new "Abmahnwelle"[194], as there are already law firms in Germany that are known for mass mailing of such letters, even for minor violations. The common practice of such law firms is to send copy-paste letters in very large numbers and profit from the chargeable fees which many intimidated recipients pay.

[192] Nico van Eijk, About Finding Practical Solutions (without the GDPR), 3 Eur. Data Prot. L. Rev. 311 (2017).
[193] Cease and desist letters
[194] Wave of such cease and desist letters

The GDPR, due to the complexity of its provisions but also the obscurity of the principles may be used as a tool for exploitation for such law firms. [195]

This is why others observe that law firms that once lobbied against the GDPR, are now opportunistically promoting the same elements of the GDPR, presented as benefits for the society.[196]

[195] Jan Henrich, German Unfair Competition Law and the GDPR - Courts Are Indecisive about Parallel Remedies, 4 Eur. Data Prot. L. Rev. 515 (2018).

[196] Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle, 2 Eur. Data Prot. L. Rev. 290 (2016).

Conclusions

In liberal states, the law usually provides rules about what it is forbidden so that the rest is allowed, unless it is in conflict to a general legal principle. Of course, there is also the other way around, that is, activities that because of their nature, they are forbidden per se, such as carrying firearms, and the law provides certain exceptions to the prohibition. For example, special and exceptional circumstances have to be present, in order for a person to acquire a permit to carry a gun.

Although the GDPR provides as one of its main objectives the facilitation of the free flow of personal data[197] the general impression extracted from the web of the provisions is that the GDPR rather intercepts the flow of information, instead of facilitating it. Like the example of the gun permit, it appears that in order to be able to process personal data, a controller has to fulfil exceptional preconditions, the principles of the GDPR, instead of merely avoiding to infringe them. The processing of personal data is generally prohibited, unless you have a right to do it, according to the principles.[198]

The view of this paper is that the caliber of the European regulation is excessive regarding the protection of personal data. The aspects of sensitive or special categories of data and the regulation of consent of the children were left outside of the analysis, because in these cases no criticism to a strict regulation could be supported. Processing of information about religion, political views, sexual preferences, health, criminal sentences, perhaps even private sector income and any information relating to children should be absolutely exceptional under few strict and specific conditions.

But as for the rest of the personal data, laws such as against illegal interception of telecommunications, surveillance in private places, defamation, breach of the confidentiality of correspondence and telecommunications or banking secrets, should be sufficient to protect the right to privacy.

Therefore, the regulation instead of describing when the processing of personal data is lawful, should have rather enumerated the few exhaustive and specific exceptions.

[197] See recitals 3, 9, 53, 123 especially 170 and article 51

[198] Daniel Rücker, Tobias Kugler, New European general data Regulation, Beck-Hart-Nomos 2018, p.51

It is understood that such views are against the mainstream perspective, somewhat ironically highlighted by the submitting of this paper 3 days after the annual international data privacy day.

Bibliography

BOOKS

1. Daniel Rücker, Tobias Kugler, New European general data Regulation, Beck-Hart-Nomos (2018)
2. European Union Agency for Fundamental Rights and Council of Europe, 'Handbook on European data protection law' (2014) <https://rm.coe.int/16806b294a>.
3. Franziska Boehm, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Springer (2012)
4. Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer (2014)
5. Lee Bygrave, Data Privacy Law, An international perspective, Oxford University Press (2014)
6. Yuval Noah Harari, Homo Deus, Harper Collins (2016)

JOURNALS

1. Alessandro Acquisti, Laura Brandimarte, George Loewenstein, Privacy and human behavior in the age of information, Science vol. 347 (2015) 509.
2. Angela Byers, Big Data, Big Economic Impact, 10 ISJLP (2015) 757.
3. Anita L. Allen, Debating Ethics and Digital Life, 5 Eur. Data Prot. L. Rev. (2019) 7.
4. Arthur Allen Leff, The Leff Dictionary of Law: A Fragment, 94 Yale L. J. (1985) 1855
5. Bart van der Sloot, Editorial, 3 Eur. Data Prot. L. Rev. (2017) 1.
6. Bart van der Sloot, Editorial, 5 Eur. Data Prot. L. Rev. (2019) 1.
7. Catherine Jasserand, Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation, 4 Eur. Data Prot. L. Rev. (2018) 152.
8. Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017) 5

9. Christopher Hodges, Delivering Data Protection: Trust and Ethical Culture, 4 Eur. Data Prot. L. Rev. (2018) 65.
10. Daniel Solove, Conceptualizing Privacy, California Law Review (2002) 1087
11. Daniel Solove, Fourth Amendment Pragmatism, 2010 Boston College Low Review (2010) 1519
12. David J. Stute, Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, 36 Mich. J. Int'l L. (2015) 649.
13. David Lazer; Victor Mayer-Schoenberger, Statutory Frameworks for Regulating Information Flows: Drawing Lessons for the DNA Data Banks from Other Government Data Systems, 34 Journal of LAW MED. & ETHICS (2006) 366
14. EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation (2018).
15. Eike Michael Frenzel, Facilitating the Flow of Public Information: The CJEU in Favour of Distinctive Rule/Exception Regulations in Member States, 3 Eur. Data Prot. L. Rev. (2017) 283.
16. Elena Kaiser, Monitoring Employees with Hidden Surveillance Cameras Breaches Their Right to Privacy, 4 Eur. Data Prot. L. Rev. (2018) 396.
17. Frederike Zufall, Challenging the EU's Right to Be Forgotten: Society's Right to Know in Japan, 5 Eur. Data Prot. L. Rev. (2019) 17.
18. Gary T. Marx, A Less Perfect but Freer Society, 4 Eur. Data Prot. L. Rev. (2018) 418.
19. Herke Kranenborg, Google and the Right to Be Forgotten, EDPL (2015) 70.
20. James Q. Whitman, The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale L.J. (2004) 1151
21. Jan Henrich, German Unfair Competition Law and the GDPR - Courts Are Indecisive about Parallel Remedies, 4 Eur. Data Prot. L. Rev. (2018) 515.
22. Jan Oster, Of Money, Poison and Secrets: Balancing Freedom of Information against Data Protection, 2 Eur. Data Prot. L. Rev. (2016) 272.
23. Jessica Bell; Stergios Aidinlis; Hannah Smith; Miranda Mourby; Heather Gowans; Susan E. Wallace; Jane Kaye, Balancing Data Subjects' Rights and Public Interest Research, 5 Eur. Data Prot. L. Rev. (2019) 43.

24. Johannes Eichenhofer, Internet Privacy at Work - the EctHR Barbulescu Judgment, 2 Eur. Data Prot. L. Rev. (2016) 266.
25. Julie Cohen, What is Privacy for, 126 Harvard Law review (2013) 1904
26. Kirsty Hughes, A Behavioural Understanding of Privacy and Its Implications for Privacy Law, 75 Mod. L. Rev. (2012) 806.
27. Kurt Wimmer, Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers, 68 SYRACUSE L. REV. (2018) 547
28. Leslie Stevens, The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK, 1 Eur. Data Prot. L. Rev. p. (2015) 97.
29. Matthew White, Immigration Exemption and the European Convention on Human Rights, 5 Eur. Data Prot. L. Rev. (2019) 26.
30. Nico van Eijk, About Finding Practical Solutions (without the GDPR), 3 Eur. Data Prot. L. Rev. (2017) 310.
31. Paul De Hert, Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules: Piercing the Veil of Stability Surrounding the Principles of Data Protection, 3 Eur. Data Prot. L. Rev. (2017) 160.
32. Raphael Gellert, On Risk, Balancing, and Data Protection: A Response to van der Sloot, 3 Eur. Data Prot. L. Rev. (2017) 180.
33. Sabine Davis, Why Germans are so private about their data <https://www.handelsblatt.com/today/handelsblatt-explains-why-germans-are-so-private-about-their-data/23572446.html?ticket=ST-855776-drIUHOli4Cr0ITOmTLsf-ap4>
34. Samuel D. Warren, Louis D. Brandeis, 'The right to privacy', Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), 193.
35. Sheng Yin Soh, Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour, 5 Eur. Data Prot. L. Rev. (2019) 65.
36. Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle, 2 Eur. Data Prot. L. Rev. (2016) 290.
37. Spiros Simitis, Privacy - An Endless Debate, 98 Calif. L. Rev. (2010) 1989.

38. Stefan Kulk; Frederik Zuiderveen Borgesius, Freedom of Expression and Right to Be Forgotten Cases in the Netherlands after Google Spain, 1 Eur. Data Prot. L. Rev. (2015) 113.
39. Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 SETON HALL L. REV. (2017) 995
40. Tal Z. Zarsky, The Privacy-Innovation Conundrum, 19 LEWIS & CLARK L. REV. (2015) 115
41. Theodore Grossman & Aaron M. Grossman, Understanding Internet Privacy: The US Perspective, 29 Int'l Bus. Law. (2001) 391
42. Viviane Reding, The European data protection framework for the twenty-first century, International Data Privacy Law, vol2, No3, (2012) 119
43. Wim Nauwelaerts, GDPR - The Perfect Privacy Storm: You Can Run from the Regulator, but You Cannot Hide from the Consumer, 3 Eur. Data Prot. L. Rev. (2017) 251.
44. Zarine Kharazian, Yet Another French Exception: The Political Dimensions of France's Support for the Digital Right to Be Forgotten, 3 Eur. Data Prot. L. Rev. (2017) 452.

COMMAND PAPERS AND LAW COMMISSION REPORTS

1. Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (2014)
2. Article 29 Working party, Guidelines on consent under Regulation 2016/679 [2017]
3. Article 29 Working party, Guidelines on transparency under Regulation 2016/679 [2017]
4. Ethics Advisory Group of the European Data Protection Supervisor, 2018 report (2018) <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>
5. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (upd.2013)

<https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

CASE LAW

1. Cases C-92/09 and C-93/09 Volker und Marcus Schecke GbR and Hartmut Eifert v Land Hessen [2010] EU:C: 2010:662
2. Case C-131/12 Google Spain SL and Google Inc. v Agencia Espatiola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez, [2014] EU:C: 2014:317
3. Opinion of Advocate General Jaaskinen, Google Spain SL v. AEPD
4. Case T-115/13 - Dennekamp v Parliament, [2015] ECLI:EU:T:2015:497
5. Case C-615/13 P - ClientEarth and PAN Europe v EFSA, [2015] ECLI:EU:C:2015:489
6. Case C-201/14, Bara and Others [2015] EU:C:2015:638
7. Case C-496/17, Deutsche Post AG v Hauptzollamt Köln [2019] ECLI:EU:C:2019:26
8. Lopez Ribalda And Others v Spain App nos 1874/13 and 8567/13 (ECHR) [2019).
9. Koepke vs Germany App no 420/07, (ECHR) [2010]
10. Niemietz v. Germany, App no 72/1991/324/396, (ECHR) [1992]
11. Antovic and Mirkovic vs Montenegro, App. No. 70838/13 (ECHR) [2017]
12. Barbulescu vs Romania, App no 61496/08 (ECHR) [2017]
13. Autronic AG v Switzerland App no 12726/87 (ECHR) [1990]
14. Rechtbank Amsterdam, 18 September 2014, ECLl:NL:RBAMS:2014:6118 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:6118
15. Rechtbank Amsterdam, 13 February 2015, ECLI:NL:RBAMS:2015:716 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2015:716

GREEK PATA PROTECTION AUTHORITY

1. Directive 1/2011

2. Decision 53/2011
3. Decision 136/2011
4. Decision 44/2019

WEBSITES

1. Anne Hardy, Spiros Simitis: Es geht um Eure Daten! Marketing und Kommunikation Goethe-Universität Frankfurt am Main, <https://idw-online.de/de/news635029>
2. Anonymous, Deutsche Welle <https://www.dw.com/en/times-change-but-german-obsession-with-cash-endures/a-43718626>
3. CIPL & AvePoint, 2nd GDPR Organisational Readiness Survey Report, accessible at <https://www.informationpolicycentre.com/global-readiness-benchmarks-for-gdpr.html>
4. Holly Lenny, Why don't the Dutch like to use curtains? <https://dutchreview.com/culture/why-dont-the-dutch-like-to-use-curtains/>
5. John Lichfield, How France fell out of love with Minitel, The Independent, 9 June 2012 <https://www.independent.co.uk/news/world/europe/how-france-fell-out-of-love-with-minitel-7831816.html>
6. Pashos Mandravelis, Kathimerini 9.11.2017 <https://www.kathimerini.gr/933854/opinion/epikairothta/politikh/ta-kryfa-dedomena>
7. The Centre for Information Policy Leadership & AvePoint, 'Organisational Readiness for The European Union General Data Protection Regulation' (AvePoint 2017), downloadable after registration at <http://www.informationpolicycentre.com/ global-readiness-benchmarks-for-gdpr.html>
8. Wikipedia, Big data
9. Xenophobe's Guides: Open curtains <https://www.expatica.com/nl/living/household/xenophobes-guides-open-curtains-107782/