Regulating risk profiling by law enforcement

van Schendel, Sascha

Publication date:
2024

Document Version
Publisher's PDF, also known as Version of record

REGULATING RISK PROFILING BY LAW ENFORCEMENT:
A TASK FOR DATA PROTECTION LAW, NON-DISCRIMINATION LAW AND CRIMINAL PROCEDURAL LAW

Sascha van Schendel

Regulating Risk Profiling by Law Enforcement: A task for data protection law, non-discrimination law and criminal procedural law

Sascha van Schendel

ISBN: 978-94-93353-55-8
Cover, layout & print: Proefschrift-AIO

Regulating Risk Profiling by Law Enforcement: A task for data protection law, non-discrimination law and criminal procedural law

Proefschrift ter verkrijging van de graad van doctor aan Tilburg University

op gezag van de rector magnificus, prof. dr. W.B.H.J. van de Donk, in het openbaar te verdedigen ten overstaan van een door het college voor promoties aangewezen commissie in de Aula van de Universiteit op

vrijdag 15 maart 2024 om 13.30 uur

door

Sascha van Schendel,
geboren te Breda, Nederland

Promotores:

prof. dr. E. Kosta (Tilburg University)
prof. dr. E.J. Koops (Tilburg University)

Co-promotor:

mr. dr. C.M.K.C. Cuijpers (Tilburg University)

Leden promotiecommissie:

prof. dr. F. Boehm (FIZ Karlsruhe)
prof. mr. J.E.J. Prins (Tilburg University)
prof. dr. B.W. Schermer (Leiden University)
prof. dr. L. Stevens (Vrije Universiteit Amsterdam)
dr. J. Purshouse (University of Sheffield)

Acknowledgements

This dissertation would not be mine if it did not come with a list of acknowledgements and expressions of gratitude, as there is nothing that I value more than all the support and kindness I received during my PhD years. The PhD project has simultaneously been the loneliest time of my life (partly due to Covid lockdowns and working from home) as well as the time in which I met the most wonderful people and made some friends for life.

First, I would like to thank my PhD supervisors. Eleni, thank you for believing in me, even though I certainly did not always do so myself and for giving me the space I needed. Thank you for your patience, advice, and for offering me opportunities to develop myself as a researcher within and beyond the PhD. Thank you, Bert-Jaap, for always offering me a perspective whether on a topic within research or on my career and just life in general, and for helping me through all my struggles with writing and structuring (and grammar). A big thank you to Colette, for if it was not for her, I would not have chosen the Master Law & Technology which set me on the path to work at TILT and do this PhD trajectory. Thank you, Colette, for co-writing my first academic publication with me, for being there with me through all the highs and lows in the past years, for spontaneous coffee meetings and all the mentoring. Also, of course, thank you Ronald, for 'convincing' me to do a PhD and for supporting me at the start of my PhD while I was still figuring out what I wanted to do.

Second, I would like to thank the members of my fantastic PhD committee for their time and for providing thorough comments and analysis, as well as for their own inspirational work which was often an important source of knowledge for my own research. Thank you, prof. F. Boehm, prof. J.E.J. Prins, prof. B.W. Schermer, prof. L. Stevens, and dr. J. Purshouse.

Next a big thank you to all the amazing colleagues at TILT over the years, especially all the PhD's; you all made me feel so welcome at TILT and are all so brilliant. I can't list all our current and past colleagues, but thank you all! In particular, I want to thank the following people. Thank you 'Tilburg Ladies': Karine, Claudia, Jingze, Anna, Silvia, Magda, Irene and Mara. I am so glad we were able to have many dinners, drinks, lunches and many other meet ups throughout my years as a student assistant and early PhD years; Thank you Karine for being a great role model, in and outside of work. Thank you Claudia for all our open and wonderful conversations, podcast/ music recommendations and beautiful walks; Thank you Jingze for all our wonderful conversations and for making me laugh; Thank you Anna for all the sunshine and

energy you bring and all your wonderful advice. Thank you Silvia for tolerating all the memes I send your way and for all the empowering and positive energy you send my way, you know me so well; Thank you Magda for all your kindness, compliments and warmth, for the interesting discussions on everything data protection & law enforcement (and of course wishing me a good breakfast always). I especially want to thank my (ex)roomies and paranymphs: dear Mara and Irene, thank you for all your emotional support, advice, gezelligheid, for helping me see where I wanted to be after the PhD and helping out with the last steps to the defense.

A big thank you as well to my 'bookclub buddies', Tineke, Leonie, Suni and Brenda, for all the wonderful times we have together laughing and listening, reading (although actually rarely) and for supporting my unhealthy love for Starbucks and for providing access to my best support buddy Scout. Thank you Lisa (the OG Lisa), for sharing my humor and humoring me, for listening to my rants and for the fun discussions on non-academic high quality literature. Thank you Riek, for getting me through very long days in the office, making me smile when I'm feeling blue, and for always being proud of me.

Thank you Bart (vdr Sloot), for all your support and patience in the projects that we worked on together, for challenging me in the best ways, and for the hard work and enthusiasm you put in on your end. Thank you Saskia, for all the wonderful opportunities you offered me and for your support, as well as for creating such a vibrating energy team comprised of wonderful people. And a big thanks to (ex)roomies Joan and Jasper (so many roommates over the years but all awesome), for indulging my horrid PhD mind maps on the whiteboard in our office, for fruitful brainstorms and for discussions on the important aspects of life such as food and coffee. A big thank you to my 'new' close colleagues. Most of you are either also not new to TILT but new to the energy sector, or recently joined TILT: Max, Olga, Shanya, Jasper, Shakya, Laura, Léo (and again Brenda). Thanks for helping me find my way in this new chapter of my career and for helping me see that together we can figure it out.

Dankjewel Valerie, Tom, kleine Rowan, oma Anneke en opa Toon (en natuurlijk opa Jan en oma Rieni, al zijn zij helaas niet meer bij ons om dit boek te mogen zien) voor alle steun en interesse. Al kan ik me voorstellen dat je de helft van de tijd denkt 'waar is zij mee bezig?!'.

I would like to dedicate this book to my loving parents, Veronique and Hans. If it were not for the both of you none of this would have been possible. You were always there when I needed a reality check, some good food, bird cuddles, a sunny destination, a

(Catan) break, or your help, especially in pandemic times when my social and mental batteries ran very low. You really helped me find myself during the PhD trajectory and have always been supportive of everything I do, as long as it makes me happy. I'm looking forward to many more adventures together in the future and to hopefully becoming an equally open and supportive parent myself.

Scientific summary

The ever expanding amount of data and improvement of automated analysis have enhanced the profiling process. So much so that profiles are increasingly used to estimate future behaviour of people and score and rank individuals and groups and base law enforcement action on expected risks. Risk profiles are used by law enforcement for various purposes ranging from mapping which locations are prone to which type and frequency of crime and at what time of day; to filtering through huge volumes of data, searching for individuals who match risk profiles; to assessing the chances (based on data from similar individuals and based on past data to make assumptions about the future) that individuals will re-offend. While techniques such as risk profiling bring possibilities mostly in terms of efficiency, they also fundamentally shift the relation with data and people represented in this data. For example, there is a shift towards pattern and correlation detection instead of focusing on individual behaviour and mentality, towards pre-emptive actions by law enforcement agencies instead of reactive actions, and towards putting the emphasis on groups rather than individuals. These shifts can be seen in the broader paradigm of a risk mitigating society and create tensions with the fundamental rights framework.

The use of risk profiles creates several challenges from a fundamental rights point of view, these are challenges of and for: fairness, bias, probabilistic systems, opacity, discrimination, privacy, and due process. Given these challenges it is crucial to scrutinize the legal framework to assess how it regulates risk profiling. This is all the more important given opacity of the law enforcement sector itself, that comes from safeguarding criminal investigations and security of others, as well as the severity of the consequences in cases of errors or violations of rights such as the right to privacy, fair trial and non-discrimination. This dissertation assessed the regulation of risk profiling conducted by national law enforcement actors under European data protection law, European non-discrimination law and Dutch criminal procedural law.

While each of these regulatory frameworks brings important safeguards and each regulatory framework has its own role to play in creating fundamental rights protection

against negative effects of risk profiling for those subjected to it, there are also issues in each of the frameworks in offering this protection and issues that become apparent when viewing the frameworks together in its entirety. Below I will outline the basic aspects of some of these issues, as they are discussed in detail in the dissertation itself.

First of all, looking at European data protection law, there is an issue with the scope of this framework when it comes to regulating risk profiling. The scope of European data protection law is intertwined with the concept of personal data. At the same time the concept of personal data is at times difficult to reconcile with the regulation of practices such as risk profiling, as profiles are also reliant on non-personal data. Personal data in turn also has a strong focus on the individual, while in profiling practices the emphasis is more on the group dimension by seeing individuals as part of a group or relying on aggregated or group data. This limitation becomes even more clear in the scope of article 11 of the Law Enforcement Directive, which awards extra protection for individual decisions rather than the entire profiling process. A related blind spot is that of contextuality, where the legislation does not pay attention to the fact that often data or tools for profiling originate from completely different contexts or from different individuals than the one that the profile is applied to. A last point of unclarity is the status of the profile itself under data protection law.

Second, if we look at European non-discrimination law, the scope of this system is challenged as it relates to categories of protected characteristics which are difficult to maintain with risk profiling activities. This is on the one hand because risk profiling is an opaque and complex process which can make it either difficult to pinpoint which characteristics are used in the analysis or blur distinctions between protected characteristics or create intersectional discrimination. On the other hand, risk profiling also introduces new characteristics that can be relevant in discriminatory treatment, for example because these are new vulnerabilities or because proxies are used to circumvent using existing protected characteristics. Next, risk profiling creates a tension in the role of statistics and in objectivity. This is because on the one hand statistics are necessary data in non-discrimination cases to prove discriminatory treatment by law enforcement actors, while on the other hand statistics are used in the profiling process to extract patterns and create estimations while referring to statistics as objective reasoning to justify indirect discrimination. Lastly, the probabilistic aspect of risk profiling and space for assumptions adds another layer of complexity as it is unclear how to treat discrimination based on assumed characteristics which might or may not be correct; here there is a role for discrimination by association to be further explored.

Third, if we look at Dutch criminal procedural law there is again an issue of scope. It is unclear to what extent the different risk profiling activities fall within the scope of the criminal investigation and thus related safeguards and to what extent some data collection or analysis activities are covered under specific legal bases in the criminal procedural scope or fall within the general police competency. Furthermore there are unclarities in the regulation of the data analysis especially, when putting the criminal procedural code next to the legislative framework for processing of police- and judicial data. Next, the shift that we see within risk profiling from reactive policing to pre-emptive and predictive risk-based policing creates tensions with criminal procedural law, such as when it comes to questions of proportionality and the concept of reasonable suspicion. Finally, moving away from the criminal investigation, risk profiling also has consequences for the right to fair trial that the legal framework struggles to cope with.

In this dissertation, I propose recommendations in four categories of solutions to close gaps and diminish conflict or unclarity. These categories are: regulation of oversight, regulation of contextuality, regulation of data analysis, and regulation of profiling beyond the individual interest. The categories of recommendations overlap with one another, as some recommendations contribute towards more than one of the overarching categories. Ultimately, the categories are bound together by the idea of practical alignment, meaning that in practice these solutions also need to be aligned especially between different actors and different fields of law.

Wetenschappelijke samenvatting

De steeds groter wordende hoeveelheid gegevens en de verbetering van geautomatiseerde analyse hebben het profileringsproces verbeterd. Zozeer zelfs dat profielen steeds vaker worden gebruikt om toekomstig gedrag in te schatten en individuen en groepen te scoren en te rangschikken en strafrechtelijke handhaving en opsporing te baseren op verwachte risico's. Risicoprofielen worden door politie gebruikt voor verschillende doeleinden, variërend van het in kaart brengen van welke locaties kwetsbaar zijn voor welk type en welke frequentie van criminaliteit en op welk tijdstip van de dag; tot het filteren van enorme hoeveelheden gegevens, op zoek naar individuen die voldoen aan risicoprofielen; tot het inschatten van de kans (op basis van gegevens van vergelijkbare individuen en op basis van gegevens uit het verleden om aannames te doen over de toekomst) dat individuen opnieuw in overtreding zullen gaan. Hoewel technieken zoals risicoprofilering vooral mogelijkheden bieden in termen van efficiëntie, verschuiven ze ook fundamenteel de relatie met gegevens en mensen

die in deze gegevens vertegenwoordigd zijn. Er is bijvoorbeeld een verschuiving naar patroon- en correlatiedetectie in plaats van focus op individueel gedrag en mentaliteit, naar preventieve acties door politie in plaats van reactieve acties, en naar het leggen van de nadruk op groepen in plaats van op individuen. Deze verschuivingen kunnen worden gezien in het bredere paradigma van een risicobeperkende samenleving en zorgen voor spanningen met het kader van de grondrechten.

Het gebruik van risicoprofielen creëert verschillende uitdagingen vanuit het oogpunt van de grondrechten, dit zijn uitdagingen van en voor: eerlijkheid, vooringenomenheid (bias), probabilistische systemen, ondoorzichtigheid, discriminatie, privacy en een eerlijk proces. Gezien deze uitdagingen is het cruciaal om het wettelijk kader onder de loep te nemen om te beoordelen hoe risicoprofielen worden geregeld. Dit is des te belangrijker gezien de ondoorzichtigheid van de straf(proces)recht sector zelf, die voortkomt uit het beschermen van strafrechtelijke onderzoeken en de veiligheid van anderen, evenals de ernst van de gevolgen in geval van fouten of schendingen van rechten zoals het recht op privacy, een eerlijk proces en non-discriminatie. In dit proefschrift is de regulering van risicoprofilering gebruikt door politie en justitie getoetst aan het Europese gegevensbeschermingsrecht, het Europese non-discriminatierecht en het Nederlandse strafprocesrecht.

Hoewel elk van deze regelgevingskaders belangrijke waarborgen biedt en elk regelgevingskader zijn eigen rol speelt bij het creëren van grondrechtelijke bescherming tegen negatieve effecten van risicoprofilering voor degenen die eraan worden onderworpen, zijn er ook problemen in elk van de kaders bij het bieden van deze bescherming en problemen die duidelijk worden wanneer de kaders in samenspel worden bekeken. Hieronder zal ik een aantal van deze probleempunten basaal schetsen, aangezien deze in detail worden besproken in het proefschrift zelf.

Allereerst is er, kijkend naar de Europese wetgeving inzake gegevensbescherming, een probleem met de reikwijdte van dit kader als het gaat om het reguleren van risicoprofilering. De reikwijdte van de Europese wetgeving inzake gegevensbescherming is verweven met het concept van persoonsgegevens. Tegelijkertijd is het concept van persoonsgegevens soms moeilijk te verenigen met de regulering van praktijken zoals risicoprofilering, omdat profielen ook afhankelijk zijn van niet-persoonlijke gegevens. Persoonsgegevens zijn op hun beurt ook sterk gericht op het individu, terwijl bij profileringspraktijken de nadruk meer ligt op de groepsdimensie door individuen te zien als onderdeel van een groep of door te vertrouwen op geaggregeerde of groepsgegevens. Deze beperking is nog duidelijker te zien in de reikwijdte van artikel 11 van de Politierichtlijn, waarin extra bescherming

wordt geboden alleen voor individuele beslissingen in plaats van het gehele proces van profilering. Een verwante blinde vlek is die van de contextualiteit, waar de wetgeving geen aandacht besteedt aan het feit dat gegevens of hulpmiddelen voor het opstellen van profielen vaak afkomstig zijn uit heel andere contexten of van andere personen dan degene waarop het profiel wordt toegepast. Een laatste punt van onduidelijkheid is de status van het profiel zelf onder de gegevensbeschermingswetgeving.

Ten tweede, als we kijken naar de Europese non-discriminatiewetgeving, wordt de reikwijdte van dit systeem in twijfel getrokken omdat het betrekking heeft op categorieën van beschermde kenmerken die moeilijk te handhaven zijn met activiteiten op het gebied van risicoprofilering. Enerzijds omdat het opstellen van risicoprofielen een ondoorzichtig en complex proces is waardoor het moeilijk kan zijn om te bepalen welke kenmerken in de analyse worden gebruikt of waardoor het onderscheid tussen beschermde kenmerken vervaagt of intersectionele discriminatie kan ontstaan. Aan de andere kant introduceert risicoprofilering ook nieuwe kenmerken die relevant kunnen zijn bij discriminerende behandeling, bijvoorbeeld omdat het om nieuwe kwetsbaarheden gaat of omdat proxy's worden gebruikt om het gebruik van bestaande beschermde kenmerken te omzeilen. Daarnaast creëert het opstellen van risicoprofielen een spanning in de rol van statistieken en in objectiviteit. Aan de ene kant zijn statistieken namelijk noodzakelijke gegevens in non-discriminatiezaken om discriminerende behandeling door rechtshandhavingsinstanties te bewijzen, terwijl aan de andere kant statistieken worden gebruikt in het profileringsproces om patronen te extraheren en schattingen te maken, terwijl naar statistieken wordt verwezen als objectieve redenering om indirecte discriminatie te rechtvaardigen. Tot slot voegt het probabilistische aspect van risicoprofilering en ruimte voor veronderstellingen nog een extra laag complexiteit toe, aangezien het onduidelijk is hoe discriminatie op basis van veronderstelde kenmerken, die al dan niet correct kunnen zijn, moet worden behandeld; hier is een rol weggelegd voor discriminatie door associatie, die verder moet worden onderzocht.

Ten derde is er, als we kijken naar het Nederlandse strafprocesrecht, opnieuw een kwestie van onduidelijkheden in de reikwijdte van het kader. Het is onduidelijk in hoeverre de verschillende activiteiten op het gebied van risicoprofilering binnen de reikwijdte van het strafrechtelijk onderzoek en de daarmee samenhangende waarborgen vallen en in hoeverre sommige activiteiten op het gebied van gegevensverzameling of -analyse vallen onder specifieke rechtsgrondslagen in het strafprocesrecht of onder de algemene politiebevoegdheid. Verder zijn er onduidelijkheden in de regulering van de gegevensanalyse, vooral wanneer het Wetboek van Strafvordering naast het wetgevingskader voor de verwerking van politiële en justitiële gegevens wordt gelegd.

Daarnaast leidt de verschuiving die we zien binnen risicoprofilering van reactief politiewerk naar preventief en voorspellend risicogericht politiewerk tot spanningen met het strafprocesrecht, bijvoorbeeld als het gaat om kwesties van proportionaliteit en het concept van een vermoeden van redelijke verdenking. Tot slot heeft het opstellen van risicoprofielen, als we buiten het strafrechtelijk onderzoek kijken, ook gevolgen voor het recht op een eerlijk proces waar het wettelijk kader mee worstelt.

In dit proefschrift stel ik aanbevelingen voor in vier categorieën van oplossingen om kloven te dichten en conflicten of onduidelijkheid te verminderen. Deze categorieën zijn: regulering van toezicht, regulering van contextualiteit, regulering van gegevensanalyse en regulering van profilering breder dan het individuele belang. De categorieën van aanbevelingen overlappen met elkaar, aangezien sommige aanbevelingen bijdragen aan meer dan één van de overkoepelende categorieën. Uiteindelijk worden de categorieën met elkaar verbonden door het idee van praktische afstemming, wat betekent dat deze oplossingen in de praktijk ook op elkaar moeten worden afgestemd, vooral tussen verschillende actoren en verschillende rechtsgebieden.

Table of contents

List of abbreviations

Attorney General (Procureur-Generaal, PG)
Area of Freedom Security and Justice (AFSJ)
Artificial intelligence (AI)
Artificial intelligence Act (AI Act)
Charter of Fundamental Rights of the European Union (CFREU)
Code of Criminal Procedure (CCP)
Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)
Council Framework Decision 2008/977/JHA (FD)
Council of Europe (CoE)
Court of Justice of the European Union (CJEU)
Crime and Victimization Risk Model (CVRM)
Crime Anticipation System (CAS)
Data Protection Authority (DPA)
Data Protection Directive (DPD)
Dutch Research and Documentation Centre (WODC)
EU Agency for Fundamental Rights (FRA)
European Commission against Racism and Intolerance (ECRI)
European Convention on Human Rights (ECHR)
European Court of Human Rights (ECtHR)
European Data Protection Board (EDPB)
European Social Charter (ESC)
European Union (EU)
General Data Protection Regulation (GDPR)
Harm Assessment Risk Tool (HART)
Joint investigation team (JIT)
Knowledge Discovery in Databases (KDD)
Law Enforcement Directive (LED)
Recidivism estimation scales (RISc)
Science and technology studies (STS)
Strategic Subject List (SSL)
Subject Assessment and Information Dashboard (SAID)
System Risk Indication (SyRI)

Chapter 1

Introduction

1.1 Balancing new technologies and regulation in the criminal justice system

According to the European Court of Human Rights (ECtHR), states claiming a pioneer role in the development of new technologies bear a special responsibility for striking the right balance between the use of modern scientific techniques in the criminal justice system and important private-life interests.[1] The use of data driven technologies and practices such as artificial intelligence (AI), Big Data, data mining, automated decision-making and profiling, continue to offer opportunities in criminal justice systems to make policing, criminal prosecution, and sentencing more efficient. At the same time, the data driven nature of these processes introduces challenges for fundamental rights frameworks applicable in criminal justice systems.[2]

On the European Union (EU) level, the legislator took action to regulate aspects of AI with the proposed EU Artificial intelligence Act (AI Act).[3] The proposal aims at proposing a legal framework for trustworthy AI and in this context introduces extra fundamental rights safeguards such as monitoring and transparency obligations, where the measures to be taken depend on the level of risk that an AI application entails.[4] National legislators have to consider whether the balance that has been struck between interests of the criminal justice system -such as fighting crime, safeguarding a secure society, protecting the safety of individuals and groups- and fundamental rights of those being in any way impacted by the criminal justice system is still the correct balance. For example, in the Netherlands, the legislator has been revising the main regulatory instrument for the criminal justice inter alia to create adequate safeguards accompanying new technologies.[5]

---

1 ECtHR, *S. and Marper v. the United Kingdom* (Applications nos. 30562/04 and 30566/04), para 112.

2 See for example: Schermer, B. W. (2017). Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, *Tijdschrift voor Bijzonder Strafrecht & Handhaving* (4).

3 Proposal for a Regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final.

4 Explanatory memorandum to the Proposal for a Regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final. Note that the use of AI for individual risk assessment purposes in the law enforcement sector is considered high risk, based on article 6 of the proposed AI Act and its Annex III.

5 Draft bill 'Wetsvoorstel Wetboek van Strafvordering', 30 July 2020, available at: https://www.rijksoverheid.nl/documenten/publicaties/2020/07/30/ambtelijke-versie-juli-2020-wetsvoorstel-wetboek-van-strafvordering.

With the fast developments in technology there is the possibility that national legislation of the criminal justice sector has not kept up with these developments, for example in the regulation of digital investigation methods[6] or of digital sentencing tools[7], which can lead to gaps in regulation, fragmented regulation, or legal uncertainty in ad hoc regulation through case law. The same hypothesis applies to regulation of data-driven technologies, such as legislation regulating data: previous research indicated that while the collection of data is regulated, there is a lack of regulation of the analysis and use of data.[8] These risks call for an analysis of the adequacy of different regulatory frameworks pertaining to the use of new technologies in the criminal justice sector in safeguarding fundamental rights.

1.2. The data driven society and risk paradigm

As the world becomes datafied[9] and tools for analysing and extracting information from the data become more enhanced, such as the use of machine and deep learning to develop algorithms and generative AI, it becomes significantly easier to gather information on people's behaviour and to find patterns and interesting correlations there. For example, the use of video surveillance and facial recognition facilitates tracking individuals on the street; the use of mining of open source social media data can map connections between people; the use of smartphone data can quickly give a detailed view of someone's life. As analytical tools become more advanced, statistical data can be used in new meaningful ways to find patterns and ultimately to make estimations about future behaviour based on the past. The premise is that patterns can be found everywhere, so law enforcement agencies and intelligence agencies have started collecting large volumes of data to pre-empt criminal or terrorist activity, while private organizations equally gather information to track users and profile their interests.[10]

---

6 Hirsch Ballin, M., & Galič, M. (2021). Digital investigation powers and privacy: Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure. *Boom Strafblad*, 2(4), p. 148.

7 See for example: Department of Corrections, State of Wisconsin, on the Correctional Offender Management Profiling for Alternative Sanctions tool, available at: https://doc.wi.gov/Pages/AboutDOC/COMPAS.aspx; And for OxRec, information is available via: https://oxrisk.com/oxrec-nl-2-backup/.

8 *Big Data in een vrije en veilige samenleving*, Dutch Scientific Council for Government Policy (WRR), Amsterdam University Press 2016.

9 The 'transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis', see: K. Cukier & V. Mayer-Schönberger, The Rise of Big Data: How It's Changing the Way We Think About the World, *Foreign Affairs*, Vol. 92, No. 3 (2013), p. 29.

10 I. Rubinstein, R. Lee, P. Schwartz, Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, *The University of Chicago Law Review* (75) 2008, p. 261.

One process that has taken flight with all these developments surrounding data and tools is profiling. Profiling is a widespread practice existing in almost every sector of society, deployed for various purposes. Profiling conducted by governmental entities can for example be aimed at detecting suspects of terrorism or possible future terrorists. In the private sector, profiles are used for instance to determine the features that individuals in a group share to offer personalized advertisements, offers and services. Profiling has become a prominent practice in society and has caught the attention of the European legislator. With the reform package of the European data protection legislation introducing the General Data Protection Regulation (GDPR)[11] and the Law Enforcement Directive (LED)[12], profiling is now explicitly regulated as part of the right against automated decision making.[13] The Article 29 Working Party[14] adopted in 2017 Guidelines on automated decision-making, including profiling, and emphasized that profiling is increasingly being used in all sectors of society, both public and private, such as banking and finance, healthcare, taxation, insurance, marketing and advertising.[15] The Article 29 Working Party attributed the increase in profiling and automated decision-making to advances in technology such as big data analytics and machine learning, which enable the drafting of profiles and the process of automated decision-making, as well as to the increased availability of personal data allowing for determination, analysis and prediction of characteristics of individuals and groups.[16]

---

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

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

13 Article 22 GDPR and article 11 LED.

14 The Article 29 Working Party was established by Directive 95/46/EC, the predecessor to the GDPR, and acted as an advisory body providing guiding documents on the Directive 95/46/EC such as opinions and guidelines. The Article 29 Working Party documents were, and still are, very influential in the understanding of key concepts of data protection law in academic discourse and data protection practice. The role of the Article 29 Working Party was taken over by the European Data Protection Board (EDPB) under the GDPR.

15 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01.

16 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01.

A new component to the availability of data and AI tools is the ability to conduct risk analysis more accurately and on a bigger scale than previously possible. It is now possible to quite accurately analyse how likely it is that an offender might re-offend, decide which locations to send police patrols to, or get insight into organized crime networks. The idea seems to be that the more data there is, the more possibilities there are to prevent crime from taking place, the more opportunities to disrupt criminal networks, or the more opportunities to mitigate the negative consequences or harm from crimes.[17] Thus, a concept of *risk profiles* emerges in the criminal justice sector. The use of risk profiles in criminal justice can be used as a guiding point for a discussion on the balancing of fundamental rights with the introduction of data-driven and AI driven technologies. This balance is a crucial topic of research, as violations of fundamental rights, or tensions between the technology of risk profiling and fundamental rights, have a serious impact given the far-reaching powers of the criminal justice system that people can be subjected to.

The use of risk assessment has traditionally been an important tool to national law enforcement agencies to efficiently make use of their limited capacity. Risk assessment has now become very popular in all sectors of society, including in the prevention against crime. The use of large-scale data and analysis tools allow more accurate assessments of risk and for risk to play a more prominent role in criminal justice decision-making and data analysis.[18] The emphasis on risk also has consequences for the aims of the criminal justice system, where risk management is prioritized over the traditional rehabilitative focus.[19] The emphasis on prevention of crime and risk control does not only stem from developments in technology and data, it is a policy direction that was already visible after terrorism threats at the start of the 2000s.

---

17 See for example: A.G. Ferguson, 'Policing Predictive Policing' (2017) 94 *Wash U L Rev* 1109; H. Kemshall, *Understanding risk in criminal justice*, Crime and Justice Series, Open University Press UK, 2003.

18 See for example H. Kemshall, *Understanding risk in criminal justice*, Crime and Justice Series, Open University Press UK, 2003; Feeley, M. M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, 30(4), 449-474; N. Reichman, Managing crime risk: towards an insurance based model of social control, *Research in Law and Social Control* 8: 151-72, 1986; B. E. Harcourt, *Against Prediction Profiling, Policing, and Punishing in an Actuarial Age*, The University of Chicago Press 2007; R. V. Ericson & E. Haggerty, *Policing the Risk Society*, Clarendon Press 1997; for possibilities of 'big data policing' see also: De Hert, P., & Sajfert, J. (2021). The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680. Available at SSRN 4016491, p. 5 & 6.

19 H. Kemshall, *Understanding risk in criminal justice*, Crime and Justice Series, Open University Press UK, 2003.

For a period, the term 'Big Data' increasingly received much attention in government policies and practices[20], peaking in 2015-2016, enabling to some extent a form of techno optimism or data optimism.[21]

Having the tools to analyze huge volumes of data and extract information from them, possibly completely by automated means, facilitates processes such as the creating and analysis of risk profiles. Now that prevention and risk control have been taken to a completely new level, this presents fundamental differences in the way in which the criminal justice sector functions. Large-scale data analysis lends itself better to a model of actuarial justice –relying on statistics and predictions- than to individualized criminalization.[22] Previously, the use of offender profiles was prominent, where criminal investigators composed profiles of unknown suspects and psychologists compiled profiles of people with specific personality disorders.[23] However, with risk profiles, analysis and application of the profiles become more complicated and more opaque than with traditional offender profiles.

For the purpose of this dissertation, the following working definition of profiling by Hildebrandt is useful to illustrate what we are talking about: "*The process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category*".[24] Profiles can serve different purposes in the law enforcement context, ranging from selection of individuals (for example to be further investigated), detection of a crime, and to a limited extent as a decisional tool.[25] A crucial element in risk profiles specifically is the pre-emptive trait, of profiles being based on inductive reasoning to cluster data and look for statistical patterns, going from the known characteristics of a certain type of criminal in general to a specific suspect or offender.[26]

---

20 B. van der Sloot & S. van Schendel, *International and Comparative Study on Big Data*, Working Paper no. 20, Dutch Scientific Council for Government Policy (WRR) 2016.

21 *Big Data in een vrije en veilige samenleving*, Dutch Scientific Council for Government Policy (WRR), Amsterdam University Press 2016, p. 136.

22 A. Marks, B. Bowling & C. Keenan, Automatic justice? Technology, Crime and Social Control. In: *R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology*, OUP 2017.

23 M. Hildebrandt, Defining Profiling: A New Type of Knowledge?. In: *Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth*, Springer 2008, p. 23.

24 M. Hildebrandt, Defining Profiling: A New Type of Knowledge?. In: *Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth*, Springer 2008, p. 19.

25 B. Custers, Risicogericht toezicht, profiling en Big Data, *Tijdschrift voor Toezicht* 2014 (5) 3.

26 R. van Brakel & P. De Hert, Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies* 2011-3, no. 20, Maklu, ISBN 978-90-466-0412-0, p. 173.

1.3 Fundamental rights challenges

While there are arguments to make in favor of law enforcement agencies making their practices more efficient by using risk profiles,[27] this development is not without societal challenges and fundamental rights concerns. In the USA, data driven policies and practices, such as risk-profiling, have been experimented with for years. Big technological companies work together with governmental and public services, allowing a new stream of data to be used.[28] I would argue that in the EU such applications are a bit newer and regulated differently, most prominently from EU data protection and privacy law. Nonetheless, also in the EU risk-profiling will likely expand, becoming more similar to examples from the USA.

First of all, the use of new data-driven analysis and policy intensifies the need for transparency of police processes for an adequate protection of fundamental rights, as the complexity and opaqueness of law enforcement practices increase. For example, if those affected by the use of risk profiles want to contest the profile or use thereof, transparency of the profile and decision-making process is necessary to exercise such a right.[29] It can be problematic that criteria used for scoring and profiling citizens and the applicable margins for error are in some cases only known to the persons applying them.[30]

Second, most of the profiles are probabilistic, describing "the chance that a certain correlation will occur."[31] In most cases the individuals included under the profile do not share all the attributes or characteristics of the group profile.[32] This means that there is always an inherent risk of errors in the use of profiles, as it might include people erroneously within a profile or might miss certain individuals, leaving them out of scope, the first category being false positives, the second situation false negatives.[33]

---

27 Such as in E.T. Zouave & T. Marquenie, An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling, *2017 European Intelligence and Security Informatics Conference*.

28 Such as Microsoft developing PredPol, predictive policing software, for the US police forces.

29 M. Hildebrandt, E.J. Koops, The Challenges of Ambient Law and Legal Protection in the Profiling Era, (2010) *Modern Law Review* 73(3) 428-460.

30 Prins, C., & Roest, J. (2018). AI en de rechtspraak: Meer dan alleen de 'robotrechter'. *Nederlands Juristenblad* 93(4), 260-268.

31 M. Hildebrandt, Defining Profiling: A New Type of Knowledge?. In: *Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth*, Springer 2008, p. 21-22.

32 M. Hildebrandt, Defining Profiling: A New Type of Knowledge?. In: *Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth*, Springer 2008, p. 21.

33 M. Hildebrandt, E.J. Koops, The Challenges of Ambient Law and Legal Protection in the Profiling Era, (2010) *Modern Law Review* 73(3) 428-460.

It has been shown already in discourse on other types of profiling in the past that this is an inherent issue for profiling.[34]

Third, the trend of risk management combined with the strong focus in politics on terrorism prevention can push law enforcement to target specific groups. Combined with this the reliance on data can create new challenges in the law enforcement sector when it comes to bias. The technology now takes over the job of detecting the patterns, creating the profiles and finding correlations.[35] As these technologies are not fool proof (just as police officers' instincts and human observation and logic are not foolproof) this poses a threat of discrimination and stigmatization of certain groups, as technology might 'over target' specific groups. It has been shown already that risk-based policing particularly targets certain (societal) groups within different EU countries, such as North African youths, soccer supporters, Roma, and Muslims.[36] Thus the technology might unintentionally increase racial or ethnical profiling. For example, in the Netherlands, ethnic profiling by police officers has been a topic of societal debate for years. While these types of debates were mainly targeted at racial profiling based on 'police instinct', automated profiling possibly increases racial profiling.[37] Profiling in itself is a discriminatory process based on classifications and groupings, which is not illegal in itself, but can become illegal discrimination if based to a certain extent on factors such as race or religion.[38] To illustrate this, in 2017, a court in the Netherlands ruled that the use of a risk profile, of single men of 55 years or older, was in violation of the principle of non-discrimination due to, inter alia, the profile leading to a decision based on the factor of age.[39]

Fourth, in the information society decisions are increasingly made based on group profiles.[40] In literature on data protection and privacy there are increasingly more debates on the possibilities for collective procedures to address types of data processing

---

34 Allo, P. "The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020.

35 E.J. Koops, Technology and the Crime Society: Rethinking Legal Protection, (2009) 1 *Law Innovation and Technology*, p. 105.

36 M. Leese, The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue* 2014, Vol. 45(5) 494–511; B.E. Harcourt, Muslim profiles post-9/11: Is racial profiling an effective counter-terrorist measure and does it violate the right to be free from discrimination? In: *Goold BJ and Lazarus L (eds) Security and Human Rights*. Oxford and Portland, OR: Hart Publishing, 2017, pp. 73–98.

37 M. Leese, The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue* 2014, Vol. 45(5) 494–511.

38 B.W. Schermer, The limits of privacy in automated profiling and data mining, *Computer Law & Security Review* 27 (2011) 45-52.

39 Centrale Raad van Beroep, 21 November 2017, ECLI:NL:CRVB:2017:4068.

40 M. Hildebrandt, E.J. Koops, The Challenges of Ambient Law and Legal Protection in the Profiling Era, (2010) *Modern Law Review* 73(3) 428-460.

such as Big Data analytics and group profiling.[41] This shift from a strong focus on the individual to targeting groups –as well as the shift to ubiquitous analysis and profiling, implicitly targeting almost all citizens- raises questions as to whom fundamental rights protection should be directed at and whether the current fundamental rights approach in that sense is still adequate.

Lastly, all of this data collection for the construction of profiles and the ubiquitous analysis can have an impact on the dynamic between citizens and law enforcement. For instance, it can have a chilling effect on citizens, as they are aware there is quite a bit of data collection but it is not clear in which ways they are being surveilled or the subject of a risk analysis.[42] In this way risk profiling contributes to a privacy paradox where citizens become increasingly transparent to law enforcement actors, while the law enforcement practices become more complicated and opaque to the citizens and society.[43] The extensive data collection, analysis and use raise questions about the protection of privacy and personal data of citizens.

All of these points of concern are reasons motivating the relevance and necessity of this research topic. At the same time, these fundamental rights challenges are also starting points to reflect on and structure the research.

1.4 The legal framework

There are multiple fundamental rights at stake when it comes to risk profiling in the criminal justice sector. The first one is the right to data protection, enshrined in article 8 of the Charter of Fundamental Rights of the European Union (CFREU)[44].
The right to data protection creates rights and obligations when it comes to the processing of personal data, which is data about identified or identifiable individuals. Thus, data protection regulation regulates the resource of profiles, data, and it regulates the process of profiling through specific provisions.

---

41 L. Taylor, L. Floridi & B. van der Sloot (eds.), *Group Privacy: New Challenges of Data Technologies*, Springer 2017; A. Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, *Computer Law & Security Review*, Volume 32, Issue 2, April 2016, P. 238-255.

42 T. Zarsky, Transparent Predictions, *University of Illinois Law Review* (2013) 4.

43 *Big Data in een vrije en veilige samenleving*, Dutch Scientific Council for Government Policy (WRR), Amsterdam University Press 2016.

44 Charter of Fundamental Rights of the European Union (2016) Official Journal C202, 7 June, pp. 389-405.

Several pieces of secondary legislation need to be introduced at this point: in 2016 the reform package for data protection legislation on the EU level was adopted, introducing the GDPR and the LED. The GDPR replaced the Data Protection Directive (DPD)[45] and applies from 25 May 2018; the LED had to be transposed in national law by 6 May 2018. The GDPR, just as its predecessor, is applicable to the processing of personal data, with one of the main exceptions to its material scope being processing of personal data for the purposes of criminal law and national security. The LED is solely applicable to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This directive is a significant change in the Area of Freedom Security and Justice (AFSJ) (the former Third Pillar in EU law). Before the introduction of the LED, data protection in this area was left in part to national legislation, partly standardized by Convention 108 of the Council of Europe (CoE)[46], and in part regulated by a variety of specialist and sector specific instruments, creating a very fragmented landscape.[47] The LED repealed the Council Framework Decision 2008/977/JHA (FD)[48], which was very narrow in scope, only applying to personal data that *"are or have been transmitted or made available between Member States"* (article 1.2(a) FD).[49] Therefore it only applied to cross-border transfers and exchanges of personal data, excluding domestic processing of personal data.[50] In contrast, the LED applies to cross-border processing, as well as processing in domestic situations. The introduction of a directive with such a broad scope created some harmonization. In addition, it could be argued that the LED raised the general data protection standards in the law enforcement area and it is enforceable by national courts.[51] Nonetheless, as the regulation of the processing of personal data by national law enforcement agencies has not been fully harmonized, a wide margin is still left to the law of Member States to lay down requirements and safeguards. Combined with the nature of the LED, being a directive requiring implementation, the LED needs to be seen together with the

45 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, L 281/31.

46 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

47 P. De Hert & V. Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and analsyis', *Computers & Law Magazine of SCL* 2012, vol. 22, issue 6.

48 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, L 350/60.

49 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, L 350/60, article 1.2 (a).

50 T. Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security Review* 33 (2017) 324-340.

51 T. Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security Review* 33 (2017) 324-340.

safeguards and requirements following from Member States' legislation that arranges the competences of these law enforcement actors.

Processing of data that is not considered personal data falls outside of the scope of all above-described data protection instruments. With the advent of Big Data and data science, data that is not personal data in itself can still be very useful for analysis. However, it is even argued by some that the distinction between personal and non-personal data is not viable anymore.[52] Profiles as such are usually not traceable to unique persons, either because the data used is anonymized or because the correlations in the profile happen at a generic level.[53] This raises interesting questions as to when personal data comes into play and when the data protection provisions apply.

Another fundamental right that is crucial when it comes to profiling is the non-discrimination, laid down in article 21 of the CFREU and in article 14 of the European Convention on Human Rights (ECHR).[54] Profiling is focused on classification, grouping and group characteristics, creating an inherent risk that profiles focus on traits or characteristics protected by law, such as gender, ethnicity, or religion. In addition, individuals get treated based on the group characteristics of the group they are placed in, creating risks of discriminatory treatment. Lastly, risk profiles often rely to a considerable extent on statistical data and historic police data, which come with their own history of bias and possible discrimination against minority groups in society.[55] Non-discrimination is therefore a crucial fundamental right to take into account when it comes to risk profiling. As there is no specific piece of secondary anti-discrimination law specifically applicable to law enforcement profiling, the analysis will focus on the primary provisions of article 21 CFREU and article 14 of the ECHR. As the principle of non-discrimination is not in any way specifically designed with data-driven practices in mind -unlike data protection legislation-, it is important to assess how it nonetheless interplays with a practice like risk profiling.

---

52 I. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, 2013, p. 5; van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y.

53 M. Hildebrandt, E.J. Koops, The Challenges of Ambient Law and Legal Protection in the Profiling Era, (2010) *Modern Law Review* 73(3) 428-460.

54 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

55 Williams, P. and Kind, E. (2019) Data-driven Policing: The hardwiring of discriminatory policing practices across Europe. Project Report. European Network Against Racism (ENAR); Žliobaitė, I. Measuring discrimination in algorithmic decision-making. *Data Min Knowl Disc* 31, 1060–1089 (2017). https://doi.org/10.1007/s10618-017-0506-1.

Other important fundamental rights in the context of profiling in the criminal justice sector are the right to privacy and fundamental rights of criminal suspects, mainly the presumption of innocence and the right to a fair trial. These two types of fundamental rights, the right to privacy and defence rights, come together in national criminal procedural legislation. For this dissertation the choice was made to analyze Dutch criminal procedural legislation, for three reasons. First, in the Netherlands there are examples available of risk profiling tools relevant to this research, such as OxRec and the use of EncroChat data, and also accompanying relevant case law. Second, the Netherlands offers an interesting system, as there has already been the Police Data Act[56] since 2007 and the Judicial Data and Criminal Records Act[57] since 2002. As the landscape for data protection has been so fragmented, in national law the relevant safeguards are dispersed and also need to be searched for in the Code of Criminal Procedure (CCP)[58]. Also, since the legislation for data collection and processing for the Dutch police has been around already for many years before the introduction of the EU law enforcement directive, it is pre-eminently an interesting jurisdiction to assess for already established practices of processing of police data under data protection safeguards. Third, the Dutch legal framework for criminal procedural law is interesting to assess as it is currently under revision, offering ideas on how to modernize this field of law vis–à-vis data-driven policing.

Criminal procedural law regulates predominantly the data collection aspects of the risk profiling process: it determines which powers national law enforcement actors have to gather data for risk profiling. The conditions and safeguards of criminal procedural law that create boundaries for the law enforcement actors to gather data or deploy the use of profiles stem from several fundamental rights that criminal procedural law builds on, such as the right to respect for private and family life (article 8 ECHR) as well as the freedom of expression (article 10 ECHR), and the right to liberty and security (article 5 ECHR) as well as the right to a fair trial (article 6 ECHR). In contrast to data protection legislation, and similar to non-discrimination law, criminal procedural law does not regulate profiling as a practice as such. However, the CCP regulates investigatory powers, such as pertaining to data collection and sometimes data analysis, which can be relevant in the context of the risk profiling process, as well as provisions on checks and balances in executing those powers.

---

56 Wet Politiegegevens, available in Dutch at: https://wetten.overheid.nl/BWBR0022463/2022-10-01/0/informatie.

57 Wet Justitiële en Strafvorderlijke gegevens, available in Dutch at: https://wetten.overheid.nl/BWBR0014194/2022-07-01.

58 Wetboek van Strafvordering, available in Dutch at: https://wetten.overheid.nl/BWBR0001903/2023-01-01.

Just as many other legal instruments pertaining to data, the CCP and its later amendments stem from a time when there were fewer possibilities to gather and analyze data. With the use of risk profiling tools, enabling or enhancing the identification of suspects, gathering evidence, forecasting of crime, or conducting of a risk assessment for sentencing, tensions can arise with the fundamental rights protection awarded to those subjected to risk profiling, exactly because the legal framework is not drafted with such technological capabilities in mind. Therefore, in the context of this thesis, it is essential to also explore criminal procedural law.

1.5 Research questions and aims of the research

The central question of the research is: How does the regulatory framework comprising of European data protection law, European non-discrimination law and Dutch criminal procedural law, regulate risk profiling conducted by national law enforcement actors and to what extent does it provide adequate fundamental rights protection to those subject to the risk profiling?

In order to provide an answer to this question the following sub-questions will be discussed:

1. What is risk profiling and what does it entail? How is the latter deployed by national law enforcement agencies?
2. What are the challenges from a fundamental rights perspective created by the use of risk profiling by national law enforcement actors?
3. How is risk profiling by national law enforcement actors regulated under European data protection legislation, and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?
4. How does European non-discrimination law regulate risk profiling by national law enforcement actors, and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?
5. How do Dutch criminal procedural law, and accompanying data protection law related to criminal matters, regulate risk profiling by national law enforcement actors and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?

The research has three aims. The first aim is to outline risk profiling as a concept and describe its practical applications. The research examines the deployment of data enabling risk assessment and analysis in the criminal justice sector and explores what this means for the traditional ideas of criminal justice. This sets the stage for the rest of this research, and also enables other scholars to build on this thesis. The second aim is to analyze and evaluate the three different legal frameworks in their respective regulation of risk profiling to assess fundamental rights protection for each of the three legal fields. This analysis is interesting for scholars, policy makers and practitioners who want to know more about the regulation of a data-driven practice such as risk profiling, as well as for scholars, policy makers and practitioners who are experts in only one of the studied legal domains. The third aim is to assess the adequacy of the fundamental rights framework in protecting individuals and groups while looking at the fundamental rights protection as a whole, so combining insights from data protection law, non-discrimination law and criminal procedural law. With this the dissertation adds important insights to scholarship in the field of law and technology, as well as important reflections for societal and regulatory debate.

1.6 Methodology

This thesis employs a combination of desk research and legal doctrinal research. First, desk research, primarily of academic literature but also of policy documents, is used to describe the use of risk profiles, placing this practice in the larger debate on pre-emptive policing and predictive analytics. The literature consists of legal literature, pertaining to European data protection law, European non-discrimination law and Dutch criminal procedural law in general and to these fields of law and specific topics such as AI, algorithms, profiling, and automated-decision making. In addition to legal literature, to understand risk profiling, it is also crucial to rely on literature that describes the technical aspects and societal impact of such processing, which is where some references to computer science, socio-legal research, criminology, and science and technology studies (STS) literature come in, for example pertaining to bias in algorithms, or discriminatory effects of data-driven tools.[59]

[59] In chapters 2 and 3, but also for a part in chapter 5 when discussing societal issues around data such as (racial) bias.

As the term 'risk' profiles suggests, the use of these profiles can be seen in the broader discussion on the risk society and predictions of possible risks to the safety of society, enabled by developments such as Big Data analytics.[60] I would argue this view on society, and more specifically on the criminal justice sector, is important to keep in mind throughout the research as it raises questions on the relationship between such a pre-emptive and actuarial view and the approach of fundamental rights, which is the regulatory framework assessed in this dissertation.

Second, legal doctrinal research – which lies at the heart of many legal research projects- is used, retrieving the scope and meaning of legal constructs by systematically analyzing all components of a legal construct.[61] In the legal research domain, a descriptive methodology is part of doctrinal legal research. Legal doctrinal research is not just a reflection of positive law in the sense of describing the law, but also offers some normative elements in choosing how to structure that discussion and how the present the systematization.[62]

Often describing the current state of the law is the first step in legal doctrinal research. In this dissertation I do this by singling out the pieces of legislation applicable to risk profiling and going through potentially relevant provisions to describe how each regulates risk profiling, creating an overview of relevant provisions in data protection legislation, non-discrimination legislation and criminal procedural law, as well as a description of their scope and their meaning using literature, explanatory opinions and case law. The description angle depends on the other goals and methods of the dissertation,[63] which for this dissertation means that the description feeds into assessment and evaluation objectives in the course of the research. Therefore, it is important to note that the description angle for the legislation is to enable analysis of whether the scope of application of said provisions addresses the challenges posed by risk profiling.

---

60 *Big Data in een vrije en veilige samenleving*, Dutch Scientific Council for Government Policy (WRR), Amsterdam University Press 2016; A. Marks, B. Bowling & C. Keenan, Automatic justice? Technology, Crime and Social Control. In: *R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology*, OUP 2017; Ericson & E. Haggerty, *Policing the Risk Society*, Clarendon Press 1997.

61 Kestemont, L. (2018). *Handbook on legal methodology: from objective to method*. Intersentia. p. 9 & 10; See also M. van Hoecke, *Is de rechtswetenschap een empirische wetenschap?*, The Hague, Boom juridische uitgevers, 2010, p. 19; H. Tijssen, *De juridische dissertatie onder de loep*, The Hague, Boom juridische uitgevers 2009, p. 58.

62 Smits, J. M. (2012). *The mind and method of the legal academic*. Edward Elgar Publishing, p. 18.

63 For more on description angles see: Kestemont, L. (2018). *Handbook on legal methodology: from objective to method*. Intersentia. p. 20.

The description structure[64] corresponds to the existing legal frameworks, describing legal provisions first on the primary EU level and CoE level, moving on to secondary legislation, and to national legislation. The data protection discussions are structured along the order of the main provisions as they appear in the law and per provision, rather than per topic. For the non-discrimination provisions, within each provision the discussion is structured step by step following the structure of how the provision is applied in case law. For criminal procedural law the provisions are more scattered, so those will be grouped around topics of risk profiling rather than their order of appearance in the law. Within the different topics, the structure follows as much as possible the order of the phases of risk profiling in the criminal justice procedure.

The interpretation used to explain and analyze different legal provisions is a mix of different forms of interpretation: a systematic interpretation (interpreting provisions in relation to others and in their place in a specific law), a legal historical interpretation (for some provisions it is crucial to understand previous versions of the provision or a previous legal instrument), interpretation based on jurisprudence and interpretation based on doctrine.[65] It is important to note that also in descriptive research choices are made, making it an 'expository'[66] exercise. Therefore, each chapter explains why the discussed legal instruments or provisions have been chosen and why the selected literature and jurisprudence are relevant.

The use of risk profiles as a topic is still quite broad. Therefore, the research looks at the use of risk profiles in two phases, which each comprise different issues. The first phase is that of detecting possible suspects, targeting a large or potentially unlimited group of people. Detecting high risk individuals can be a starting point for further measures. The second phase is when a suspect has already been identified or when there is already a conviction. In this scenario the profile is used to determine the risk that this specific individual will commit another crime if released. For both stages I use examples from practice to make the discussions more concrete. The examples are based on Dutch practice, as the analysis of criminal procedural law is that of Dutch criminal law, making the legal analysis directly applicable on the case studies.

---

64 For more on description structures see: Kestemont, L. (2018). *Handbook on legal methodology: from objective to method*. Intersentia. p. 20.

65 For more on interpretation see: Kestemont, L. (2018). *Handbook on legal methodology: from objective to method. Intersentia*. p. 21-31.

66 Smits, J. M. (2012). *The mind and method of the legal academic*. Edward Elgar Publishing, p. 13.

The other examples I present are from the USA, where risk profiling in criminal justice has been developed very significantly, offering a wide variety of examples. The examples that were selected are as varying as possible, using the Diverse Cases approach, in order to elucidate as many salient aspects of the studied issue, as possible.[67]

In addition to the descriptive aim, the dissertation includes an evaluative objective. An evaluative objective aims to assess the legal construct from the perspective of a specific norm.[68] Note that this evaluation should be seen as distinct from formulating recommendations, which goes a step further in also assessing how the legal construct should be formulated.[69] In this dissertation I evaluate the provisions from data protection law, non-discrimination law and criminal procedural law from the descriptive part of the thesis and assess to what extent they attain fundamental rights protection of individuals and groups. This evaluation uses internal criteria, as derived from the system itself, to allow an assessment to the standard set by law itself[70]: in this case protection of the fundamental rights of data protection, non-discrimination and criminal procedural rights. It should be noted that while fundamental rights can be seen as cornerstones for deciding 'what ought to be', that does not mean that the content of those rights is undisputed.[71] Therefore in each chapter I also pay attention to what aims or goals the fundamental right in question has or what its underlying principle or idea is. Nonetheless, fundamental rights have a certain universal importance and value, making them an important benchmark.[72]

Lastly, the dissertation has a recommendatory research objective. In order to meet this objective, the concluding chapter will first explain the findings of the evaluation, to identify and explain where recommendations are necessary. As recommendations are a normative reflection,[73] I describe what should be done to provide more adequate protection from the perspective of data protection, non-discrimination and criminal procedure, for safeguarding fundamental rights of those subjected to law enforcement risk profiling.

---

67 J. Seawright & J. Gerring, Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options, *Political Research Quarterly* 2008 61:294.

68 Kestemont, L. (2018). *Handbook on legal methodology: from objective to method*. Intersentia. p. 17; H. Tijssen, De juridische dissertatie onder de loep, The Hague, Boom juridische uitgevers 2009, p. 58.

69 Kestemont, L. (2018). *Handbook on legal methodology: from objective to method*. Intersentia. p. 17.

70 For more on description structures see: Kestemont, L. (2018). *Handbook on legal methodology: from objective to method*. Intersentia. p. 60-61.

71 Smits, J. M. (2012). *The mind and method of the legal academic*. Edward Elgar Publishing, p. 70-72.

72 Hirsch Ballin, E. (2020). *Advanced introduction to legal research methods*. Elgar Advanced Introductions, p. 55-57.

73 For more on legal recommendations see: Kestemont, L. (2018). H*andbook on legal methodology: from objective to method*. Intersentia. p. 63-74.

1.7 Relevance of the research

This research builds on existing research in the field of profiling, which was for many years most notably a data protection and privacy law discussion.[74] Although most of these discussions are from ten or twenty years ago, when profiling first emerged, many of the challenges surrounding profiling and fundamental rights still exist today: either those have still not been resolved or warrant research from a different angle with the introduction of AI, shifting the focal point and upping the scale of the data and processes at stake. Rather than attempting to reinvent already existing concepts, I want to acknowledge the value of those existing scholarly debates and build on them. In addition to scholarship from a privacy and data protection perspective, there is also increasingly an academic debate on non-discrimination in profiling, further propelled by AI developments.[75]

---

74 For example scholarship on the former Data Protection Directive: Bygrave, L. A. Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling'(2001). *Computer Law & Security Report*, 17, 17; Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1), 45-52. Scholarship on the GDPR and LED in regulating profiling, such as: Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International journal of law and information technology*, 27(2), 91-121; Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation". *AI magazine*, 38(3), 50-57; Kaminski, M. E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, 34(1), 189-218; Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law;* Mendoza, I., & Bygrave, L. A. (2017). The right not to be subject to automated decisions based on profiling. In *EU Internet Law* (pp. 77-98). Springer, Cham; Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, 34(2), 398-404; Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, 7(2), 76-99; Selbst, A., & Powles, J. (2018, January). "Meaningful Information" and the Right to Explanation. In Conference on Fairness, Accountability and Transparency (pp. 48-48). And scholarship on profiling in relation to the fundamental right to privacy and data protection: Hildebrandt, M. (2009). Who is profiling who? Invisible visibility. In *Reinventing data protection?* (pp. 239-252). Springer, Dordrecht; Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), 162-176; Gutwirth, S., & De Hert, P. (2008). Regulating profiling in a democratic constitutional state. *In Profiling the European citizen* (pp. 271-302). Springer, Dordrecht.

75 See for example: S. Barocas and A. Selbst "Big data's disparate impact" *California Law Rev* vol. 104 no. 3 pp. 671-729 Jun. 2016 [online] Available: https://ssrn.com/abstract=2477899; Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567; Frederik J. Zuiderveen Borgesius (2020) Strengthening legal protection against discrimination by algorithms and artificial intelligence, *The International Journal of Human Rights*, 24:10, 1572-1593, DOI: 10.1080/13642987.2020.1743976; Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719895805; Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, 45(5), 494–511. https://doi.org/10.1177/0967010614544204; Xenidis, R. (2020). Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. *Maastricht Journal of European and Comparative Law*, 27(6), 736–758. https://doi.org/10.1177/1023263X20982173; Naudts, L. (2019). Criminal Profiling and Non-Discrimination: On Firm Grounds for the Digital Era?. Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. Cambridge, Antwerp, Chicago: Intersentia, 63-96.

There is less scholarship on the criminal justice perspective when it comes to law enforcement profiling in the EU context, but because it has such a strong national focus, literature on this is likely to have been published in national journals in the native languages of specific countries. For that reason, my research builds upon Dutch scholarship on criminal law related to profiling.[76] Altogether, by building upon and combining three different bodies of literature, this thesis contributes to the academic debate on risk profiling, particularly in the law enforcement sector but potentially useful also for the debate about risk profiling in other domains.

On a societal level, the research provides an important contribution as there have been numerous illustrations of risk profiling processes that caused fundamental rights violations. For example in the Dutch context, a much-debated example was the System Risk Indication (SyRI), for which the legal basis was struck down in court because of fundamental rights violations[77]; another example concerns the Dutch Tax Authorities that regularly make news headlines for problems with risk profiles and blacklists[78]. By foregrounding and analysing the standards set in case law, such as by the ECtHR, and set by the EU and CoE legislators through fundamental rights, this research on risk profiling offers important insights for academic, societal and legislative debates.

1.8 Outline

The first part of the dissertation revolves around the concept of risk profiling. Chapter 2 focuses on the first research question: *What is risk profiling and what does it entail? How is the latter deployed by national law enforcement agencies?*

---

76 See for example: Van Dijck, G. (2020). Algoritmische risicotaxatie van recidive. Over de Oxford Risk of Recidivism tool (OXREC), ongelijke behandeling en discriminatie in strafzaken. *Nederlands Juristenblad*, 95(25), 1784-1790; Van der Auwera, J., & Van de Velde, L. (2021). Risicoprofiling of risicovolle profiling tijdens grenscontroles? Naar een verantwoord gebruik van proactieve risicoprofielen door rechtshandhavingsinstanties. *Tijdschrift voor Veiligheid*, 20(3), 1-17; Stevens, L., Hirsch Ballin, M., Galic, M., Buisman, S., Groothoff, B., Hamelzky, Y., & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2021(4), 234-245; Schermer, B. W., & Oerlemans, J. J. (2020). AI, strafrecht en het recht op een eerlijk proces. *Computerrecht*, 2020(3); Galič, M. 'Bulkbevoegdheden en strafrechtelijk onderzoek', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2022, p. 130-137; Das, A., & Schuilenburg, M. (2018). Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht. *Strafblad*, 2018(4), 19-26.

77 District Court The Hague, 5 February 2020, ECLI:NL:RBDHA:2020:865.

78 Autoriteit Persoonsgegevens, Report 17 July 2020. *Belastingdienst/Toeslagen. De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag*. Available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_belastingdienst_kinderopvangtoeslag.pdf.

Chapter 2 describes the concept of risk profiling, the use of risk profiles and their role in criminal justice systems, giving the reader a general sense of how and why risk profiles are used by law enforcement. The chapter also describes the shift to risk based law enforcement, illustrating how risk profiles emerged from this shift, situating the concept of risk profiling in a societal and scientific context. Examples of the use of risk profiles from the Netherlands and the USA are given to make the discussion more concrete and connected to challenges of the use of risk profiling in practice, and to offer examples that will be revisited from different legal domains throughout the thesis.

Chapter 3 focuses on the second research question: *What are the challenges from a fundamental rights perspective created by the use of risk profiling by national law enforcement actors?* After a literature study, chapter 3 discusses the fundamental challenges of risk profiling from the perspective of concerns underlying such processes, ranging from the data that goes into risk profiling and the analysis in risk profiling processes to the use of risk profiles. Specifically, the chapter discusses fairness of risk profiling systems, bias in data and in risk profiling systems, probabilistic risk profiling systems, opacity of risk profiling systems, discrimination in the use of risk profiling systems, privacy of data collection and data use in risk profiling systems, and due process in risk profiling systems.

These challenges feed into the legal analysis for the second part of the thesis, as they played a role in selecting the relevant fundamental rights frameworks to discuss, and they offer a yardstick for which challenges the law should be able to mitigate or address negative consequences for those impacted by risk profiling.

Next, the dissertation delves into the regulatory framework selected for this research of European data protection law, European non-discrimination law and Dutch criminal procedural law. In chapters 4 to 6, the legal analysis builds on risk profiling as described in chapter 2 and takes into account the challenges described in chapter 3.

Chapter 4 focuses on the third research question: *How is risk profiling by national law enforcement actors regulated under European data protection legislation, and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?*

The chapter starts with the CoE data protection landscape, analyzing the Convention 108+[79], the CoE Police Recommendation[80], and the CoE Profiling Recommendation[81]. Next the chapter goes through the EU data protection landscape, moving from the DPD and the FD to the LED and the GDPR, discussing the general data protection principles in their application to profiling as well as specific provisions relevant for profiling. The discussion is structured per instrument and per provision.

Chapter 5 focuses on the fourth research question: *How does European non-discrimination law regulate risk profiling by national law enforcement actors, and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?* The chapter starts with an exploration of discrimination in risk profiling, offering illustrations and an explanation of the problem and relevance. Subsequently, the chapter discusses discrimination in the law enforcement context: why is there a specific focus in debates on certain protected grounds when it comes to law enforcement profiling? And what are different discrimination risks in different law enforcement practices pertaining to risk profiling?

Next, the chapter analyzes CoE and EU non-discrimination law, focusing on articles 14 ECHR and article 21 CFREU to structure the discussion and apply it to risk profiling. In order to do so I discuss the system of protected grounds, direct and indirect discrimination, objective justifications and the margin of appreciation, and discrimination by association, all in relation to risk profiling.

Chapter 6 focuses on the fifth research question: *How do Dutch criminal procedural law, and accompanying data protection law related to criminal matters, regulate risk profiling by national law enforcement actors and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?* The chapter first explores to what extent risk profiling can be considered to be a part of the criminal investigation, a crucial scoping concept in criminal procedural law. Subsequently, the chapter looks at specific investigative powers for data collection and analysis that are relevant to risk profiling, using police operations and case law on EncroChat data to structure and illustrate the discussion.

---

79 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, No. 108.

80 Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

81 Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

Next, the chapter looks beyond criminal investigation and discusses the regulation of risk profiling in the criminal justice process in sentencing decisions. The next part of the chapter is dedicated to the specific national legislation on the processing of police data, criminal procedural data, and judicial data, to assess the storage of, access to, analysis of, and sharing of the data in the risk profiles. The last part of the chapter analyzes the difficulties in applying the legal framework to risk profiling, more specifically through the shift from reactive policing to pre-emptive and predictive risk-based policing; the interplay between different legal frameworks of the CCP and the Police Data Act; and the difficulties of due process regulation of risk profiles in the criminal trial.

Chapter 7 is the concluding chapter of this dissertation. First, the chapter presents the main findings in answering the research question, using the concepts, legal and doctrinal analysis from the other chapters of the thesis. The chapter discusses the answers to the research question following the general structure of the dissertation, starting with a discussion on definitions, moving to a discussion on the findings related to the regulatory frameworks, and finishing with providing answers to the main question related to challenges of risk profiling. Lastly, the concluding chapter offers reflections on how to move forward to offer better fundamental rights protection, addressing the regulatory gaps that were identified through the research. These reflections take the form of recommendations, focused on the regulation of data analysis, regulating profiling beyond the individual interest, regulation of contextuality, regulation of oversight, and lastly practical alignment of regulation.

1

Chapter 2

Risk Profiling

2.1 Introduction

Profiling is a practice that has been taking place for years but has really expanded in the past years due to technological developments in Big Data analytics, data mining and complex automated algorithms. As profiling is a widespread practice in almost every sector of society, profiling is deployed for various purposes. Profiling conducted by governmental entities can for example be aimed at detecting suspects of terrorism or possible future terrorists. In the private sector profiles are used to determine the features that individuals in a group share to offer personalized advertisements, offers and services. A profile can be used to make a general rule, for instance to make an organizational or policy decision. Alternatively, a profile can be applied in a concrete case to decide to offer something to a particular group or not, to decide what to offer to an individual, or whether to grant a request to an individual.[82]

The Article 29 Working Party emphasized, in its guidelines on automated decision-making, including profiling, that profiling is increasingly being used in all sectors of society, both public and private, such as banking and finance, healthcare, taxation, insurance, marketing and advertising.[83] The Article 29 Working Party attributed the increase in profiling and automated decision-making to advances in technology such as Big Data analytics and machine learning, which enable the drafting of profiles and the process of automated decision-making, as well as to the increased availability of personal data allowing for determination, analysis and prediction of characteristics.[84] Another development is the simultaneous datafication of society, 'the transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis'[85], creating an enormous data pool. As a consequence, assessments of all types of behaviour are possible based on statistics and aggregated data: the likelihood that people will file a claim with their insurance, the likelihood that someone is interested in an offer, or the likelihood that a person will (re)commit crime. The premise is that patterns can be found everywhere, so that law enforcement agencies and intelligence agencies have started collecting large volumes of data to preempt criminal activity, while private organizations equally gather information to track users

82 Koops, E.J., Some Reflections on Profiling, Power Shifts and Protection Paradigms, p. 326-337. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

83 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01

84 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01

85 Cukier, K. and Mayer-Schönberger, V., "The Rise of Big Data: How It's Changing the Way We Think About the World". *Foreign Affairs* 92, no. 3 (May/June 2013): 28-40, p. 29.

and profile their interests.[86] This move towards assessing all kinds of risks through data mining has been labelled as entering a 'risk society'.[87]

The use of risk profiles has traditionally been an important tool for national law enforcement agencies to efficiently make use of their limited capacity. Previously, before computers and digital data became prominent, criminal investigators composed profiles of unknown suspects and psychologists compiled profiles of people with specific personality disorders for the purposes of identifying suspects.[88] This type of profiling, criminal profiling, aims at getting inside a criminal's mind; it is very different from the profiling that is prevalent nowadays.[89] Nowadays, the focus is not to get into the criminal's mind, but to have an overview of people's current or possible future behaviour through data and to get an overview of their social networks.

Risk assessment has now become very popular: some scholars have described the emphasis on risk as entering into an era of actuarial justice[90], or the rise of 'the logic of risk'[91] in criminal justice practice. An example of this development is prioritizing risk management and the public protection agenda in policies on probation, over the traditional rehabilitative focus.[92] Koops has described a similar development in 'the new paradigm of criminal law', which for example contains a focus on prevention, risk, groups, profiling, and statistics.[93] The emphasis on prevention of crime and risk control is not new in itself: it is a development that already took off in the early 2000s. However, especially after the terrorist attacks in the USA on 11 September 2001, countries around the globe significantly stepped up legislation and measures

---

86 Rubinstein I., Lee, R., Schwartz, P., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, *The University of Chicago Law Review* (75) 2008, p. 261.

87 H. Kemshall, *Understanding risk in criminal justice*, Crime and Justice Series, Open University Press UK, 2003.

88 Hildebrandt, M., Defining Profiling: A New Type of Knowledge? In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008, p. 23.

89 Pap Andras, L., 'Profiling, Data Mining and Law Enforcement: Definitions' (2009) 50 *Annales U Sci Budapestinensis Rolando Eotvos Nominatae* 277.

90 H. Kemshall, *Understanding risk in criminal justice*, Crime and Justice Series, Open University Press UK, 2003; Feeley, M. M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, 30(4), 449-474; Reichman, Managing crime risk: towards an insurance based model of social control, *Research in Law and Social Control* 8: 151-72, 1986; Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*, The University of Chicago Press 2007.

91 Ericson & E. Haggerty, *Policing the Risk Society*, Clarendon Press 1997.

92 H. Kemshall, *Understanding risk in criminal justice*, Crime and Justice Series, Open University Press UK, 2003.

93 Koops, E.J., Technology and the Crime Society: Rethinking Legal Protection, (2009) 1 *Law Innovation and Technology*, p. 116.

to counter and prevent terrorism.[94] A big shift has taken place in the sense that with new policing practices,[95] rather than focusing on individual cases where a specific suspect is targeted and where queries are clear in advance, Big Data analysis lends itself better to a model of actuarial justice – relying on statistics and predictions – than to individualized criminalization.[96]

In the USA data-driven policies and practices, such as risk-profiling, have been experimented with for years. Big technological companies work together with governmental and public services, allowing a new stream of data to be used.[97] The use of algorithms for risk assessment and the focus on data have already created issues with due process and discrimination in the USA[98], creating an interest in how to deal with similar issues in the EU as well. Although the USA and EU use different legal frameworks in regulating profiling, challenges comparable to those in the USA are becoming visible in the EU. Therefore, illustrations of the use of profiling in the USA are useful even for an analysis that is focused on the European legal framework, to demonstrate the possible challenges of profiling.

This chapter explains the concept of profiling and its specific application of risk profiling as a basis for further analyzing its challenges and regulatory framework in later chapters. In order to do so, a few preliminary steps are necessary.
First, profiling will be discussed as a general concept. The concept of profiling can be approached from the process itself, drawing from research on the workings of profiling to explain the concept through an understanding of how it functions. Profiling can also be explained through its legal meaning, examining data protection legislation that offers a definition of profiling.

---

94 De Goede, M., De Graaf, B., Sentencing risk: Temporality and precaution in terrorism trials, *International Political Sociology* 7 (3), 313-331.

95 Koops, E.J., Technology and the Crime Society: Rethinking Legal Protection, (2009) 1 *Law Innovation and Technology*, p. 117.

96 Marks, B. Bowling & C. Keenan, Automatic justice? Technology, Crime and Social Control. In: *R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology*, OUP 2017.

97 Such as Microsoft developing PredPol, predictive policing software for the US police forces.

98 For example the Loomis vs Wisconsin case *(Loomis v. Wisconsin, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017)* about automated profiling in determining probation and sentencing and the question whether this hinders due process; or the regulation of a New York task force to examine the automated decision-making systems used in the city's public services (see: *Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force," AI Now Institute, December 4, 2019, https://ainowinstitute.org/ads-shadowreport-2019.html*).

The main legal framework to explore for definitions of profiling is European data protection law, which regulates the resource of profiling, namely (personal) data. Dutch criminal procedural legislation[99] does not regulate specifically how data is processed or used through profiling,[100] so that no descriptions of the concept of profiling can be found there. The same applies to European anti-discrimination law. Therefore, the analysis of the legal meaning of the concept of profiling will focus particularly on data protection law.

Subsequently, the discussion of profiling will be narrowed down to a specific goal, namely that of assessing risk, in the specific sector of law enforcement. In this sense, the chapter is structured like a funnel, gradually narrowing down the topic. Regarding risk profiling in the law enforcement sector, the chapter explains what the concept of risk profiling entails and the different types of risk profiling used in practice. To make the explanation of risk profiling more concrete, it is combined with examples from practice, more specifically examples from law enforcement practices of the USA and the Netherlands. The USA is a country where the use of profiling technology in law enforcement and courts emerged early[101], and the use of algorithms, predictions and profiles is already well-established practice.[102] The use of some types of risk profiles is still minimal in the Member States of the European Union but might become more prominent following the USA's example. Dutch examples of SyRI, Crime Anticipation System (CAS) and OxRec, three risk profiling systems, are chosen to illustrate its use in Europe. These Dutch examples of risk profiling have substantial public information about them and one system, SyRI, has even been under judicial scrutiny, offering an interesting court case on the matter to discuss.[103] Together these US and Dutch cases illustrate different possible applications of risk profiling in the law enforcement domain.

---

99 See for example the Dutch Criminal Procedural Code which covers data collection in combination with article 3 of the Police Act 2012.

100 Schermer, B.W., 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017, p. 207-216.

101 Already since the late 2000s, see Brayne, S., Rosenblat, A., and Boyd, D. "Predictive Policing". Data & Civil Rights: a new era of policing and justice. October 27, 2015. https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf ; Ferguson, A. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press; Werth, Risk and punishment: The recent history and uncertain future of actuarial, algorithmic, and evidence based penal techniques. *Sociology Compass*. 2019; 13:e12659. https://doi.org/10.1111/soc4.12659.

102 Brayne, S., Rosenblat, A., and Boyd, D. "Predictive Policing". Data & Civil Rights: a new era of policing and justice. October 27, 2015. https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf; Angèle, C., Rosenblat, A., and Boyd, D. "Courts and Predictive Algorithms". Data & Civil Rights: a new era of policing and justice. October 27, 2015. https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf; Whittaker et al., AI Now Report 2018, December 2018, available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf.

103 District Court the Hague, 5 February 2020, ECLI:NL:RBDHA:2020:865.

2.2 The concept of profiling

Profiling is a phenomenon that has been discussed extensively over the years, the first definitions of profiling stemming from the 1980s and 1990s. Already in 1984, Marx and Reichman provided a description of profiling as a method of systematic data searching that allows to correlate a number of distinct data items in order to assess how close a person or an event comes to predetermined characterization or model infraction.[104] Marx and Reichman place their description of profiling in the context of criminal investigations. They describe profiling as a practice that serves to increase the probability of discovery of violations of the law compared to random searches.[105] Investigators can, through data analysis, assess how many data points or more specifically how many characteristics a person displays that match with a characterization or model of the investigated crime.[106] Models are developed by comparing data of patterns and characteristics of violators with presumed non-violators, distilling the points that refer to violations.[107] Marx and Reichman see the value of profiling in this way as creating red flags, steering the investigation process, as the more red flags a person displays the more interesting it is to start a proper investigation involving this person. Interestingly, Marx and Reichman also emphasize that profiling is an indirect activity following inductive logic.[108] According to their conceptualization, indicators need to be seen together to present whether they can be associated with an increased probability that a criminal violation will occur or has occurred.[109]

Marx and Reichman distinguish between singular and aggregative profiling, which in the current day and age is not really used[110], where singular profiling refers to discrete

---

104 Marx G.T. & Reichman N. (1984) 'Routinising the Discovery of Secrets' *Am. Behav. Scientist* 27,4 (Mar/Apr 1984) 423-452.

105 Marx G.T. & Reichman N. (1984) 'Routinising the Discovery of Secrets' *Am. Behav. Scientist* 27,4 (Mar/Apr 1984) 423-452.

106 Schakel, Rienks, and Ruissen refer to this part of Marx and Reichman's description as a 'select before you collect' principle or theory. See: Schakel, R. Rienks and R. Ruissen, Knowledge-Based Policing: Augmenting Reality with Respect for Privacy, p. 178. In: *B. Custers, T. Calders, B. Schermer, T. Zarsky (eds.), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Springer 2013.

107 Marx G.T. & Reichman N. (1984) 'Routinising the Discovery of Secrets' *Am. Behav. Scientist* 27,4 (Mar/Apr 1984) 423-452.

108 Compared to what they describe earlier in their paper as matching, which is an activity of direct nature.

109 Marx G.T. & Reichman N. (1984) 'Routinising the Discovery of Secrets' *Am. Behav. Scientist* 27,4 (Mar/Apr 1984) 423-452.

110 Instead a distinction between individual profiles and aggregated or group profiles is more common. See for example, Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by B. A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

characteristics that are meaningless in themselves and where aggregative profiling refers to the frequency with which these factors appear across cases.[111]
Marx and Reichman point towards the specific use of predictive profiling, which was already being used in practice in the 1980s in the USA at least, according to their examples.[112]

In the following decades, scholars from different disciplines have proposed many other definitions of profiling, whether regarding the criminal investigation context, such as the one above, or one without a specific context, referring to profiling in various possible sectors and scenarios. One of these is the definition by Clarke in 1993 of profiling being "(…) *a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data - holdings are then searched for individuals with a close fit to that set of characteristics*."[113] Another is the description of profiling in 2013 by Custers: "*Profiling is the process of creating profiles. Although profiles can be made of many things, such as countries, companies or processes (…) we focus on profiles of people or groups of people. Hence, we consider a profile a property or a collection of properties of an individual or a group of people*".[114] I merely show these two definitions here to illustrate the possible definitions.

Diving deeper into definitions, Ferraris et al. assessed various definitions of profiling in legal and sociological literature. Their work contains an extensive literature review culminating in a comprehensive overview. Ferraris et al. conclude that the most prominent definitions of profiling share the following four elements: a central role of data and quantitative techniques; categorization as one of the main characteristics; the deduction of new information from something already known; and the use of this information for some purposes in specific domains of application.[115] The descriptions of profiling researched by Ferraris et al. highlight different perspectives on the concept of profiling. On the one hand, the term profiling is used to describe a concrete practice, focusing on the workings or mechanisms of profiling such as 'use of correlations'. On the other hand, the term is used to refer to profiling more as a general phenomenon, discussing different characterizations or trends and domains of application.

---

111 Marx G.T. & Reichman N. (1984) 'Routinising the Discovery of Secrets' *Am. Behav. Scientist* 27,4 (Mar/Apr 1984) 423-452.

112 Such as early warning detection systems for arson, predictive profiling used to prevent welfare fraud, or even systems that can allow law enforcement to intervene before acts take place such as with airline skyjacking.

113 Clarke, R. "Profiling: A Hidden Challenge to the Regulation of Data Surveillance". *Journal of Law, Information and Science* 4, no. 2 (1993): 403-419.

114 Custers, B. "Data Dilemmas in the Information Society: Introduction and Overview". In: *Discrimination and Privacy in the Information Society. Studies in Applied Philosophy, Epistemology and Rational Ethics*, vol. 3, Edited by Bart Custers, Toon Calders, Bart Schermer, Tal Zarsky, 3-26. Berlin, Heidelberg: Springer 2013.

115 Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI p. 6, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf

The first element of profiling definitions, the central role of data and quantitative techniques, points to the current nature of profiling being very data driven compared to profiling in for example the 1980s or 1990s. Quantitative techniques allow analyzing large amounts of data in the Big Data era and correlate characteristics. The second element of profiling definitions, categorization, is indeed central to profiling, as will be discussed more extensively later in this chapter. The categorization allows for seeing which elements make an individual or group unique and allow for comparisons. The third element of profiling definitions, deduction of new information from already known information, is at the core of profiling. This is the element that makes profiling go beyond a mere categorization or ranking. The fourth element of profiling definitions, of the use of this information in a specific domain, is readily apparent, but it is useful to bear in mind that profiling can be used for different purposes and by different actors in different domains. The element of using information from profiling in a specific domain also implies there is a use or application of the profile, for example with regard to a specific individual or to a specific decision.

While many definitions of profiling have been presented throughout the years, Hildebrandt's work on profiling is very extensive and seminal.[116] Hildebrandt's foundational work on profiling can therefore be used here to provide a basic first understanding of the concept of profiling. According to Hildebrandt, the term profiling is used "*to refer to a set of technologies, which share at least one common characteristic: the use of algorithms or other techniques to create, discover or construct knowledge from huge sets of data*".[117] The term profiling here refers to both a practice and the technology as such at the same time.[118] As a technology and as a practice, profiling is essentially a way to cope with information overload. As exponentially more data become available, means are necessary to be able to work with that quantity of data and extract meaningful information.[119] Therefore, Hildebrandt focuses on the aspect of deriving information from data sets.

---

116 For example, see Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52; Mittelstadt, B. "From individual to group privacy in big data analytics." *Philosophy & Technology* 30, no. 4 (2017): 475-494.; Mendoza, I., and L.A. Bygrave. "The right not to be subject to automated decisions based on profiling." In *EU Internet Law*, pp. 77-98. Springer, Cham, 2017.

117 Hildebrandt, M., Defining Profiling: A New Type of Knowledge? In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008, p. 17.

118 Hildebrandt M., Backhouse J. (2005), Descriptive analysis and inventory of profiling practices. In FIDIS Project Deliverable 7.2., p. 51, Available at: http://www.fidis.net.

119 Hildebrandt & Gutwirth, General Introduction and Overview. *In: M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008, p. 1.

Although there are data processing methods or techniques that process large amounts of data, this does not necessarily imply that this results in meaningful information, such as relevant patterns or commonalities. Viewing profiling as a coping mechanism also explains the increase in profiling applications along with the increase in data through datafication. Hildebrandt concludes that profiling is "*the process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category*".[120] The seminal part of Hildebrandt's definition is that an image or a representation of reality is made: reality is assumed to be reflected in the profile, which may for example include an assumption that an individual has all the characteristics attributed to them in the profile. This assumption of reality together with the possibility to compare different individuals and groups easily enables mastering large quantities of data.

Hildebrandt's definition concerns different possible subjects of profiling, as profiles can be made of people, such as customers or criminal suspects, but also of locations[121] or processes and objects. The definition of profiling presented by Bygrave, an often quoted definition as well[122], is similar but more focused on people solely: "*(…) profiling is the process of inferring a set of characteristics (typically behaviour) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics*".[123] Bygrave's definition centers on the same concept, namely attributing characteristics and using that image of reality for some action or process.

---

120 Hildebrandt, Defining Profiling: A New Type of Knowledge? In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008, p. 19.

121 Think for example of hotspot policing where a risk profile of a specific area is created.

122 To list a few: Bosco, F. , Creemers, N., Ferraris, V., Guagnin, D., and Koops, E.J. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities". In: *Reforming European Data Protection Law. Law, Governance and Technology Series*, vol 20. Edited by S. Gutwirth, R. Leenes, and P. de Hert, 3-33. Dordrecht: Springer, 2015; Kamarinou, D. and Millard, C. and Singh, J., Machine Learning with Personal Data (November 7, 2016). *Queen Mary School of Law Legal Studies Research Paper* No. 247/2016, Available at SSRN: https://ssrn.com/abstract=2865811; J.M. Dinant, C. Lazaro, Y. Poullet, N. Lefever, A. Rouvroy: Application of Convention 108 to the profiling mechanism Some ideas for the future work of the consultative committee, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-Pd) 24th meeting 13-14 March 2008 Strasbourg, G01 (TPD), Secretariat document prepared by the Council of Europe Directorate General of Human Rights and Legal Affairs, Strasbourg, 11 January 2008 T-PD(2008)01. Available at: https://rm.coe.int/16806840b9.

123 Bygrave, L.A. "Automated Profiling: Minding the Machine: article 15 of the EC Data Protection Directive and Automated Profiling". *Computer Law & Security Review* 17, no. 1 (January 2001): 17-24. https://doi.org/10.1016/S0267-3649(01)00104-2, p. 17.

Both definitions cover the discovery or inferring of characteristics of the subject to be used in some action related to the profiled subject: Hildebrandt talks about the application of the profile to represent that subject, while Bygrave mentions treating a person in the light of their characteristics.

It is interesting to see how these seminal definitions by Hildebrandt and Bygrave match the general four elements of profiling definitions described above, being, the central role of data, categorization, deduction of new information, and the use of information in a specific domain. Hildebrandt does not focus much on the amount of data or its role, but she does mention data and databases. Bygrave does not even use the term data in his definition. Although, on the other hand, it can be argued that the use of data is implicit, for example in "the process of inferring [from data sets] (…)", and does not require explicit mentioning. It does appear that both these authors do not see a prominent role for Big Data analytics or require intricate data analysis tools such as deep learning algorithms, as a necessary element of profiling. Ferraris et al. mention categorization as a central concept; the process of inferring information or characteristics is something that Bygrave explicitly mentions in agreement with Ferraris et al., while Hildebrandt does not use the literal term in her definition but does describe the same act. The last element Ferraris et al. mention, the use of that information, is something that both Hildebrandt and Bygrave explicitly list: Hildebrandt talks about applying a profile and Bygrave about treating a person in the light of that information. In contrast to Ferraris et al. who talk about using inferred information, Hildebrandt phrases it more in terms of treating someone based on their assumed characteristics or profile, an important nuance that is otherwise missing. Bygrave's definition is closer to the definition of Ferraris et al., in the sense that Bygrave focuses on the person that the profile is being created of. That person is the starting point and central point in Bygrave's definition. To make decisions, or apply the profiling in another way, inference of their characteristics is necessary, but Bygrave does not mention assumed characteristics or treating a person in a specific way simply because they are part of a group.

These are general descriptions of the concept of profiling, describing it as a practice or technology that infers or attributes characteristics of subjects and subsequently treats the subjects according this inference or attribution. This general understanding of profiling can be said to be neutral in terms of disciplinary background: the description fits the concept of profiling regardless of whether one looks at it from the perspective of for example a computer scientist or a legal scholar. The authors of the descriptions above do not base themselves on a specific legal text or an information science technique.

2.3. The process of profiling

Besides having a general idea of what profiling is or aims to do conceptually, it is interesting to go more into depth in how profiling works technically. A basic understanding of how profiling works adds to the understanding of profiling, for which the definitions described above lay the foundation. Nonetheless, it should be noted that a basic understanding of such a complex and technological rapidly evolving practice does not provide a state of the art description. Nor is it necessary for a further legal analysis to have a state of the art overview of the technology behind profiling. This section merely aims to distinguish basic concepts of profiling that are important for a legal analysis of the process as well as for an analysis of the challenges connected to profiling. First, the different steps of the profiling processes will be distilled. Subsequently, the technology used for profiling will be described, starting with the older concepts of Knowledge Discovery in Databases (KDD) and data mining moving to newer concepts of machine learning and deep learning. Lastly, useful distinctions between various possible modalities of profiling will be drawn.

2.3.1 The steps in the profiling process

First of all, the profiling process can be split into phases or steps. For example, Koops distinguishes three phases in the profiling process.[124] The first phase is the pre-profiling stage, this is the phase in which the data are collected and stored. The second phase is the profile-making phase, in which the data are analyzed and profiles are created, which can either be individual profiles or group profiles. The third phase is the use of the profile, in which a profile is applied to a concrete case.[125] This general distinction of the process into phases allows for a compartmentalization of profiling. Instead of understanding profiling in a broad way that can refer to various actions, one can say something about the types of data collected and the different gathering methods; something about the different ways in which data are analyzed and types of tools used; and something about the different goals for which profiling is used or how the outcome of the analysis can be used. Other authors propose a distinction of profiling into phases as well, for example Pap describes the three phases of profiling slightly differently.

---

124 Koops, E.J., Some Reflections on Profiling, Power Shifts and Protection Paradigms, p. 326-337. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

125 Koops, E.J., Some Reflections on Profiling, Power Shifts and Protection Paradigms, p. 326-337. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

The first phase is labelled by him as 'observation', including collection and anonymization of data. The second stage is that of 'data mining', using statistical methods to establish correlations between variables.[126] These correlations are used to categorize individuals into groups, which Pap describes as the outcome of the second stage.[127] Pap labels the third and final stage 'inference'. In the inference phase, data representing already known characteristics of a person, are used to determine new, previously unknown, characteristics. In more simplistic terms, the profile is applied to the individual. According to Pap, often only this last stage of the process is incorrectly referred to as profiling instead of the whole process as such.[128]

Comparing the phases of profiling as set out by Koops and Pap, the first phase comprises the same activity, namely the gathering of information. The term observation is a bit broader than data gathering, as it could also include simply gathering information through sight or information that is not digitalized. However, the addition of the reference to 'data' implies that Pap also has the digital type of information in mind. Comparing the second stage as described by both authors, Koops's second stage is more generic, leaving the exact way in which data is analyzed and the profile compiled open. On the other hand, it is more expansive than Pap's second stage. Koops includes the analysis of the data, the label given to the subject of the profiling, and the placement of the subject in a category or group, in the same stage. For Pap these actions could be seen as separate components of the profiling process; he distinguishes between the data mining and placing of individuals in groups as the outcome of that analysis. Although it can be argued that in doing so, Pap places the same activities as Koops does in the data analysis stage, so there is not really a difference there. In the third stage, Pap makes the extra distinction of inference of new information based on the classification applied. Pap therefore does not explicitly mention application of the profile or decision-making based on the profile as a stage. However, it can be argued that adding new information based on the categorization is already an action of application or decision in itself. Therefore, inference and applications that Koops refers to such as decision-making, can be included in the same stage.

---

126 Pap, L.A., 'Profiling, Data Mining and Law Enforcement: Definitions' (2009) 50 *Annales U Sci Budapestinensis Rolando Eotvos Nominatae* 277.

127 Pap, L.A., 'Profiling, Data Mining and Law Enforcement: Definitions' (2009) 50 *Annales U Sci Budapestinensis Rolando Eotvos Nominatae* 277.

128 Pap, L.A., 'Profiling, Data Mining and Law Enforcement: Definitions' (2009) 50 *Annales U Sci Budapestinensis Rolando Eotvos Nominatae* 277.

To conclude, the profiling process can be seen as consisting of several steps. There is some overlap between them as actions often take place simultaneously, but for theoretical purposes, it is useful to distinguish between five actions and three stages, as pictured below. The first stage is gathering data, the second performing analysis on the data and the third is applying the profile. In the phases of analysis and application, multiple activities take place but not always in the same order and not always distinguishable from each other. In the process of analyzing the data profiles will be constructed and groups or classifications will be formed, but these two activities feed into each other. Profiles are partly based on or derived from existing groups or classes, but on the other hand, groups and classes are also formed by viewing profiles. In the phase of application of the profile, the profile is used to infer additional information concerning the subject of the profile and decisions can be made by applying the profile.

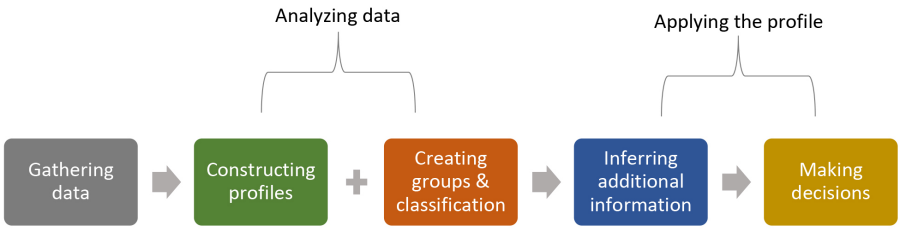

Figure 1. Steps in the profiling process.

2.3.2. KDD and data mining

In addition to the different activities in the stages of the profiling process, there is also a variety in the tools or techniques used. The traditional tool for profiling is data mining or KDD as a technical method for extracting information from data. Data mining can be seen as a technique useful for profiling for analyzing and interpreting large amounts of data to obtain knowledge.[129] Data mining focuses on finding new patterns and correlations in data, profiling focuses on ascribing characteristics to individuals and groups.[130]

[129] Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by B. A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

[130] Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by B. A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

Data mining focuses on identifying valid, novel, potentially useful and understandable patterns in data.[131] In the current information society, it is a necessary process to cope with the data or information overload. Some argue that data mining and profiling are separate technologies, profiling can be done without the use of data mining and vice versa, although often data mining and profiling are used together in practice.[132] Profiling without data mining will in practice however refer to non-automated profiling, such as manually writing up psychiatric profiles. It is difficult to imagine an instance of automated profiling that does not include some form of data mining.

Data mining is an automated analysis of data, using mathematical algorithms to find patterns and information in the data.[133] A pattern in that sense is a statement describing relationships in a set of data; when that pattern is certain and interesting enough it can be called knowledge.[134] Therefore when we say patterns rely on correlations, the certainty pertains to the presence of a pattern, not to the certainty of there being a (relevant) causal connection. Data mining is one step in the KDD process. KDD provides the user of the system with answers to questions they did not ask[135]; meaning that it presents connections or patterns that the user did not see before, which give rise to questions such as 'why do these individuals share attribute x?' While KDD refers to an entire process of extracting information, data mining is a technique that rather forms one step in that process, i.e. the application of algorithms.[136] Data mining is different from other database techniques and statistical methods because it makes use of a bottom-up or data-driven approach, meaning that it is not required to have a preconceived idea of what the query is.[137]

---

131 Fayyad U., Piatetsky-Shapiro G., Smyth P. (1996) From Data Mining to Knowledge Discovery: an Overview, *In Fayyad U, Piatetsky-Shapiro G, Smyth P, Uthurusamy R. (eds) Advances in Knowledge Discovery and Data Mining*. AAAI Press / MIT Press, Cambridge.

132 Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by B. A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

133 Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by Bruce A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

134 Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by Bruce A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

135 Zarsky T. Z. (2002-2003), `Mine Your Own Business!`: Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion." *Yale Journal of Law & Technology* 5, pp. 1-56.

136 Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI p. 6, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf ; Custers, B., Data Mining and Group Profiling on the Internet (2001). Custers B.H.M. (2001), Data Mining and Group Profiling on the Internet. In: *Vedder A (red.) Ethics and the Internet*. Antwerpen: Intersentia. 87-104, 2001.

137 Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by Bruce A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

Alternatively, other methods work top-down or theory-driven, starting with a hypothesis or theory and searching through the data accordingly.[138]

The entire process of KDD can in general be described[139] as follows:
Step 1 – Recording/collecting/gathering the data;
Step 2 – Data warehousing and data cleaning/preparation;
Step 3 – Data mining, applying algorithms;
Step 4 – Assessing and evaluating the results;
Step 5 – Follow up (for example correcting);
Step 6 – Application of the profiles.

Custers lists the steps slightly differently, although they cover the same activities: 1) data collection; 2) data preparation; 3) data mining; 4) interpretation; 5) determining actions.[140] Connecting this to the stages of profiling as discussed before, it becomes clear that KDD takes part in all phases, such as collecting the data, analyzing, creating profiles and so forth. How much KDD, or data mining within that process, is used in profiling therefore depends on the level of machine involvement or automation in profiling. If I assume that profiling, for the purposes of this dissertation, involves a significant degree of automation, it can be seen as a process similar to, or partly overlapping with, KDD. According to Borking et al., data mining can be used for five kinds of action: associations, sequences, classifications, clusters and predictions.[141] According to Custers, data mining is most frequently used in classifications.[142] Classification is examining groups to see which characteristics can be used to identify or predict the group membership.[143]

---

138 Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by Bruce A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

139 See Hildebrandt, M., Defining Profiling: A New Type of Knowledge? In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008 and Zarsky T. Z. (2002-2003), `Mine Your Own Business!`: Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion." *Yale Journal of Law & Technology* 5, for their descriptions of the KDD process.

140 Custers, B. "Data Dilemmas in the Information Society: Introduction and Overview". In: *Discrimination and Privacy in the Information Society. Studies in Applied Philosophy, Epistemology and Rational Ethics*, vol. 3, Edited by B. Custers, T. Calders, B. Schermer, T. Zarsky, 3-26. Berlin, Heidelberg: Springer 2013.

141 Borking, J., M. Artz, and L. van Almelo, *Gouden bergen van gegevens. Over datawarehousing, datamining en privacy*. Achtergrondstudies en verkenningen 10, Den Haag: Registratiekamer, 1998.

142 Custers, B., Data Mining and Group Profiling on the Internet (2001). Custers B.H.M. (2001), Data Mining and Group Profiling on the Internet. In: *Vedder A (red.) Ethics and the Internet*. Antwerpen: Intersentia. 87-104, 2001.

143 Custers, B., Data Mining and Group Profiling on the Internet (2001). Custers B.H.M. (2001), Data Mining and Group Profiling on the Internet. In: *Vedder A (red.) Ethics and the Internet*. Antwerpen: Intersentia. 87-104, 2001.

Another frequent use is clustering, which is used to discover different groups within the data.[144] Both approaches identify groups, but there is a difference. Classification is the examination of already known groups to determine which characteristics can be used to identify or predict group membership, while clustering is the identifying of groups based on certain similar characteristics without reference to any predefined group information.[145]

A key point to note in discussing data mining as part of the profiling process is that there are two approaches to data mining, descriptive data mining and predictive data mining. Descriptive mining simply aims to provide more insight into or a better understanding of information.[146] The goal of descriptive data mining is to discover unknown relations between different subjects; descriptive data mining algorithms aim to uncover commonalities between objects and attributes.[147] By discovering the correlations between objects in a dataset, we gain insight into it.[148] No target is given to the system while data mining, therefore descriptive data mining can be labelled as unsupervised. It simply signals a correlation or relation, it does not describe it nor explain it.[149] In contrast, predictive data mining aims to provide new information of already collected data or to predict events or behaviour before they actually occur.[150] In the case of profiling that means that information about individuals is mined to determine whether they fit a pre-established profile.[151] Predictive data mining is considered supervised data mining, as the data, such as collections of individuals, contain annotations or labels, e.g. for example the label 'known terrorists'.[152]

---

144 Custers, B., Data Mining and Group Profiling on the Internet (2001). Custers B.H.M. (2001), Data Mining and Group Profiling on the Internet. In: *Vedder A (red.) Ethics and the Internet*. Antwerpen: Intersentia. 87-104, 2001.

145 Custers, B., Data Mining and Group Profiling on the Internet (2001). Custers B.H.M. (2001), Data Mining and Group Profiling on the Internet. In: *Vedder A (red.) Ethics and the Internet*. Antwerpen: Intersentia. 87-104, 2001.

146 Zarsky T. Z. (2002-2003), `Mine Your Own Business!`: Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion." *Yale Journal of Law & Technology* 5, pp. 1-56.

147 Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52.

148 Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52; Cocx, T. *Algorithmic tools for data-oriented law enforcement (diss.)*. Leiden: University of Leiden, 2009, ISBN 9789090248059.

149 Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52.

150 Zarsky T. Z. (2002-2003), `Mine Your Own Business!`: Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion." *Yale Journal of Law & Technology* 5, pp. 1-56.

151 Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52.

152 Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52.

Predictive mining is often used for classification, as it can be used to establish whether a new object fits the previously established class.[153] However, it remains a likelihood that an object belongs to the assigned class. Classes are based on input fields that contain the attributes associated with the class; the more attributes an object shares with the other objects of the class, the more likely it is that it indeed belongs to that class.[154] The descriptive mining for profiling is more interesting from the perspective of learning more about the specific set of characteristics an individual has, while the predictive mining can be applied for example in the context of predictive policing to assess the likelihood that someone will display the same behaviour as others in the same class.

While data mining is an automated part of the process, it is still influenced by humans who are part of the process.[155] The data can be collected by data scientists and be prepared by them for automated analysis, and the algorithm itself is also programmed by humans. The steps of interpreting the results and possibly correcting errors have varying degrees of input of humans, depending on how automated the process is.[156] The degree of human involvement in these last steps is key because it determines the explainability of the result.[157] The more complicated the process is, the more complicated it is to keep humans involved and to explain the process in human language.

2.3.3. Algorithms and machine learning

Next to data mining, another important technical component of the profiling process is the use of algorithms. An algorithm can be described as a set of instructions to execute a specific task.[158]

---

153 Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52.

154 Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52.

155 Ferraris et al. also draw this conclusion: Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf

156 Zarsky T. Z. (2002-2003), `Mine Your Own Business!`: Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion." *Yale Journal of Law & Technology* 5, pp. 1-56.

157 Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI p. 6, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf .

158 De Poorter & J. Goossens, Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad* 2019/2777, p. 3305.

Hill describes algorithms as "*mathematical constructs with a finite, abstract, effective, compound control structure, imperatively given, accomplishing a given purpose under given provisions*".[159] Or put more simply, one could say an algorithm is a "*technologically automated mathematical formula, a sequence of instructions that are carried out to transform the input to the output*".[160] The type of algorithm used in the profiling process is determined by the aim of the profiling process; different types of algorithms can be used from collecting data to application of the profile, depending on what that step within the process requires. Algorithms can roughly be divided into two groups: rule-based and case-based algorithms.[161] Rule-based algorithms use a set of given rules, based on a model, to come to a certain conclusion; these are algorithms with a fairly simple decision tree.[162] Case-based algorithms can learn to make predictions about the outcome of unknown cases, based on cases that they are trained on and already know.[163] In the case of the latter, terms such as machine learning, deep learning and self-learning come into play.[164] All of these terms connect to the ability of the system to learn, train, and develop; as a consequence systems with case-based algorithms can be seen as more complex than rule-based algorithms.

Machine learning has to do with the ability to train algorithms. In order for the algorithm to accomplish its purpose it needs to be developed. Machine learning can be defined by the capacity to define or modify decision-making rules in an autonomous way.[165] The most prominent type of a machine learning algorithm is a classifying algorithm.[166] Such an algorithm usually consists of two components, a learner and a classifier. The learner produces the classifier, with the intention to develop classes that

---

159 Hill, 'What an algorithm is', *Philosophy and Technology* 2015, 29, 1, p. 35.

160 Alpaydin, E., *Machine Learning*. Cambridge: MIT Press, 2016, p. 16; Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges .

161 De Poorter & J. Goossens, Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad* 2019/2777, p. 3305.

162 De Poorter & J. Goossens, Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad* 2019/2777, p. 3305.

163 De Poorter & J. Goossens, Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad* 2019/2777, p. 3305.

164 De Poorter & J. Goossens, Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad* 2019/2777, p. 3305.

165 Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* (July–December 2016), pp. 1–21.

166 Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms". *Big Data & Society*, 3 no. 1 (June 2016): 1-12. https://doi.org/10.1177/2053951715622512. For more on classification see: Kantardzic, M. (2011). *Data mining: concepts, models, methods, and algorithms*. John Wiley & Sons, p. 170.

can generalize beyond the training data.[167] Learning means that the algorithm defines rules to determine how new inputs will be classified.[168] The algorithm can learn the model via hand inputs labelled by humans, which is supervised machine learning; or the algorithm itself defines models and sorts inputs, which is unsupervised machine learning.[169] Nonetheless, whether it is supervised or unsupervised machine learning, it is the algorithm that defines decision-making rules to handle new inputs.[170]

The main difference between supervised machine learning or unsupervised machine learning is whether the data are labelled or not.[171] This distinction is the same as that explained for descriptive and predictive data mining. The prescriptive data mining is also called supervised as the data are labelled, while the descriptive mining is called unsupervised, as the data are not labelled.[172] In supervised learning, a learning system is presented with examples, while in unsupervised learning the system is not provided with explicit feedback or desired output.[173] In machine learning there is not a programmer acting as a literal teacher providing the machine with instructions,[174] rather 'the aim is to construct a program that fits the given data'.[175]

---

167 Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* (July–December 2016), pp. 1–21; Burrell, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms". *Big Data & Society*, 3 no. 1 (June 2016): 1-12. https://doi.org/10.1177/2053951715622512.

168 Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* (July–December 2016), p. 3. See also: Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52; Van Otterlo M (2013) A machine learning view on profiling. In: *Hildebrandt M and de Vries K (eds) Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*. Abingdon: Routledge, pp. 41–64.

169 Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* (July–December 2016), p. 3. See also: Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52; Van Otterlo M (2013) A machine learning view on profiling. In: *Hildebrandt M and de Vries K (eds) Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*. Abingdon: Routledge, pp. 41–64.

170 Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* (July–December 2016), p. 3. See also: Schermer, B. W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52; Van Otterlo M (2013) A machine learning view on profiling. In: *Hildebrandt M and de Vries K (eds) Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*. Abingdon: Routledge, pp. 41–64.

171 Corea, F. *An Introduction to Data: Everything You Need to Know About AI, Big Data and Data Science*. Springer, 2019, p. 31; Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361. There is also a third group that can be distinguished when it comes to robotics, namely reinforcement learning.

172 Schermer, B.W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52.

173 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

174 Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges.

175 Alpaydin, E., *Machine Learning*. Cambridge: MIT Press, 2016, p. 24.

Machine learning algorithms rely on pattern recognition.[176] When the algorithms search to recognize patterns, the use of training data gives the algorithm the opportunity to learn from feedback and refine its predictions based on past performance.[177]

Hildebrandt explains machine learning using the example of algorithms that are trained to predict the outcome of court cases.[178] The first part of machine learning is to create a machine readable task.[179] A target variable is set up, for example, the judge will deliver a guilty verdict, which must correlate with the input variable.[180] Then a subset of all the available variables is selected as the relevant features. In this way the training data can be refined.[181] Subsequently a model is constructed to 'detect potentially relevant correlations between the feature set and the target variable'.[182]

Zhou et al. distinguish three different stages of the machine learning process: data preprocessing, learning, and evaluation. [183] Data preprocessing is to prepare raw data for subsequent learning, as it is usually unstructured, noisy, incomplete, and inconsistent. The preprocessing contains steps such as data cleaning, extraction, transformation, and fusion.[184] In the next stage, learning algorithms are chosen and models are fine-tuned to parameters to generate the desired outputs using the preprocessed input data. [185]

---

176 Polson, N. and Scott, J., *AIQ: How Artificial Intelligence Works and How We Can Harness its Power for a Better World* (London: Bantam Press, 2018), p. 4; Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges.

177 Diakopoulos N., 'Accountability in Algorithmic Decision Making', Communications of the ACM (Vol. 59, No 2, 2016); Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges.

178 Hildebrandt, M., Data-Driven Prediction of Judgment. Law's New Mode of Existence? (2019). OUP Collected Courses Volume EUI Summer-school, 2019. Available at: http://dx.doi.org/10.2139/ssrn.3548504.

179 Hildebrandt, M., Data-Driven Prediction of Judgment. Law's New Mode of Existence? (2019). OUP Collected Courses Volume EUI Summer-school, 2019. Available at: http://dx.doi.org/10.2139/ssrn.3548504.

180 Hildebrandt, M., Data-Driven Prediction of Judgment. Law's New Mode of Existence? (2019). OUP Collected Courses Volume EUI Summer-school, 2019. Available at: http://dx.doi.org/10.2139/ssrn.3548504.

181 Hildebrandt, M., Data-Driven Prediction of Judgment. Law's New Mode of Existence? (2019). OUP Collected Courses Volume EUI Summer-school, 2019. Available at: http://dx.doi.org/10.2139/ssrn.3548504.

182 Hildebrandt, M., Data-Driven Prediction of Judgment. Law's New Mode of Existence? (2019). OUP Collected Courses Volume EUI Summer-school, 2019. Available at: http://dx.doi.org/10.2139/ssrn.3548504.

183 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

184 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

185 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

In the last stage, evaluation, the performance of the algorithm is evaluated. For example, when it is a classifying algorithm, there are dataset selection, performance measuring, error-estimation, and statistical tests to be evaluated.[186]

A subcategory of machine learning is deep learning, also referred to as deep neural network-based learning.[187] Neural networks are families "*of models inspired by biological neural networks that consist of interconnected neurons whose connections can be tuned and adapted to inputs*".[188] Deep neural networks are neural networks with many large hidden layers, or deep-layered architecture.[189] Deep neural networks can be trained in two ways that resemble general supervised and unsupervised machine learning. There is supervised learning, in which task-related labelled data is available, and unsupervised learning, in which training data can be automatically generated from unlabelled data without much human effort.[190] With the rise of Big Data analytics, more tools have become available to train these deep neural networks, lifting algorithms and machine learning to a new level and opening up new discussions on artificial intelligence.[191]

2.3.4. Some useful distinctions

Having outlined the steps and technologies in the process of profiling, it is useful to in addition present some specific distinctions that are used by prominent authors in the field of profiling. These distinctions demonstrate differences in how profiling practices are and should be regulated, which feeds into the legal analysis in the later chapters of this dissertation.

2.3.4.1 The degree of machine involvement

Besides detailing the different stages and activities that make up the profiling process, it is useful to distinguish between the different degrees of machine involvement. As profiling can refer to a hand-composed and written profile or a label by an automated system, there is a large variation in the degree of machine involvement. On the one end is non-automated profiling, being a completely analogue type of human reasoning. In

186 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

187 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

188 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

189 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

190 Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

191 For example: Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361; Corea, F. *An Introduction to Data: Everything You Need to Know About AI, Big Data and Data Science*. Springer, 2019.

the middle is partially automated profiling, including some machine involvement but not being a fully automated process,[192] where the machine involvement can be in various steps such as in aggregating data, analyzing data or in decision-making. At the other end of the spectrum is fully automated decision-making, which is a process driven entirely by a machine.[193] Thus in discussing profiling, one can be referring to a very simple process in which a human decides in what group to place a certain individual, or to a process in which an algorithm defines characteristics and sorts individuals all by itself. The degree of machine involvement creates important differences in challenges, for example in the level of complexity of the profiling process, and involves differences in the regulation[194] of different types of profiling, as the degree of machine involvement can create differences under data protection legislation.

Narrowing down the scope however, most literature on profiling discusses profiling in an automated sense, requiring some sort of machine involvement, while also not going as far as a profiling system that would function completely separately from any human instruction or intervention.[195] In that sense it seems correct to conclude that most discussion in legal literature focuses on Hildebrandt's idea of 'machine profiling'.[196]

2.3.4.2 The subject of profiling: individual vs. group profiling

Another distinction is to whom the profile is applied: individualized – also called 'personalized' – profiling and group profiling.[197] Individualized profiling entails combining data about an individual from different sources to find correlations between different data points and establish patterns in this individual's behaviour

---

192 Hildebrandt M. (2006), Profiling: from Data to Knowledge. The challenges of a crucial technology, in DuD *Datenschutz und Datensicherheit*, 30(9), pp. 548-552

193 Hildebrandt M. (2006), Profiling: from Data to Knowledge. The challenges of a crucial technology, in DuD *Datenschutz und Datensicherheit*, 30(9), pp. 548-552. Note that Hildebrandt does not use the terms partially and fully automated profiling, but instead respectively refers to those as automated and autonomic profiling.

194 For a discussion on the regulation of profiling through the data protection lens, see chapter 4.

195 Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI p. 6, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf; Hildebrandt, Defining Profiling: A New Type of Knowledge? In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008; Bygrave, L.A., "Automated Profiling: Minding the Machine: article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law & Security Review* 17, no. 1 (January 2001): 17-24. https://doi.org/10.1016/S0267-3649(01)00104-2; Marx G.T. & Reichman N. (1984) 'Routinising the Discovery of Secrets' *Am. Behav. Scientist* 27,4 (Mar/Apr 1984) 423-452.

196 Hildebrandt, M., Defining Profiling: A New Type of Knowledge? In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

197 Hildebrandt, M., Defining Profiling: A New Type of Knowledge? In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008, p. 20; Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI p. 6-7, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf.

or preferences. Individualized profiles are popular in any sector where offering personalization is important, for example in offering targeted advertisements. Group profiling can be used to identify or create a new group or it can be applied to an already known or existing group.[198] A profile is made of the characteristics that people in a group share; in that way it is clear what the commonalities within a group are. In addition, by linking individuals with commonalities together, a group can be formed. Group profiling is interesting when you want to compare or rank an individual, when you want to make predictions about behaviour individuals might display based on people with the same attributes, or simply when you want to target more than one individual. Vedder and Hildebrandt both classify group profiling in two types.[199] Distributive group profiling assumes that individuals share all the same attributes in a group. In non-distributive group profiling, a group is created of which all the individuals share (at least) one attribute. In this case, there are discrepancies between the different individuals, so treating the individuals of that group as the same might create errors. The non-distributive type is the most common: usually, people within a group do not share all of the same attributes.[200]

2.3.4.3 Direct vs indirect profiling

Jaquet-Chiffelle proposes that the traditional distinction between group profiling and individual profiling is not precise enough and can be refined by introducing the concepts of direct and indirect profiling.[201] He proposes the following definitions: "*Direct profiling occurs when the end user and the original data subject used to define the virtual person with its profile are the same. Indirect profiling aims at applying profiles deduced from other data subjects to an end user*".[202] In Jaquet-Chiffelle's definition, the term end user might be confusing in the context of law enforcement. In common language, the end user of a profile would be the law enforcement actor using the profile in practice, that actor being the user that the profile is developed for. However, that is not the end user Jaquet-Chiffelle refers to: he simply means the person that the profile is applied

198 Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI p. 6, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf.

199 Vedder, A. KDD: The challenge to individualism. *Ethics and Information Technology* 1, 275–281 (1999). https://doi.org/10.1023/A:1010016102284; Hildebrandt, Defining Profiling: A New Type of Knowledge? *In: M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

200 Vedder, A. KDD: The challenge to individualism. *Ethics and Information Technology* 1, 275–281 (1999). https://doi.org/10.1023/A:1010016102284.

201 Jaquet-Chiffelle, D.O., Direct and Indirect Profiling in the Light of Virtual Persons, p. 40. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

202 Jaquet-Chiffelle, D.O., Direct and Indirect Profiling in the Light of Virtual Persons, p. 40. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

to. In other words, Jaquet-Chiffelle distinguishes between data subjects whose data is used in the process and the data subject that the profile is ultimately applied to. Comparing the types of direct and indirect profiling, it is clear that direct profiling is used to learn more about an already identified individual or group. Indirect profiling can be used to categorize individuals and groups. Using the distinction between group profiles and individual profiles, Jaquet-Chiffelle illustrates the different possible subtypes as follows. Direct group profiling occurs when data are collected concerning a pre-existing community, e.g. a church community, and processed to find shared features establishing a profile of this group and subsequently applying the profile to the community. Indirect group profiling can occur when data mining is used to find subsets of individuals within the church community, each subset having its own profile, and subsequently applying one of the profiles to a group that is related to the profile or a different community that is related to the profile. The case of direct individual profiling is simple: information about one individual is collected and processed to define their profile. That profile is then applied to the same individual for example to anticipate their preferences. In contrast, to produce indirect individual profiles, existing profiles are used as knowledge to infer probable profiles for an individual. For example, an insurance company can use group profiles to estimate the risk of a client who smokes, where the group profile associated with smokers is used to infer probable characteristics of that client.[203] Hildebrandt refers to this distinction between indirect and direct as a distinction with regard to the level of application of profiles.[204]

These three distinctions in profiling, the level of automation in profiling, the group as a target versus the individual, and the application of direct versus indirect profiling, are illustrated below.[205] This means that each profile has a technology (that ranges from non-automated to fully automated), an application that is either direct or indirect or a mix of both, and a target that is either a group or an individual.

---

[203] Jaquet-Chiffelle, D.O., Direct and Indirect Profiling in the Light of Virtual Persons, p. 40-43. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives.* Springer 2008.

[204] Hildebrandt, D.O., Profiling and AmI, p. 277. *In: K. Rannenberg, D. Royer, A. Deuker, The Future of Identity in the Information Society. Challenges and Opportunities*. Springer 2009.

[205] Hildebrandt proposes another distinction between the creation and use of profiles, but at the same time acknowledges the use of profiles can loop back and feed into the process of creating them, making the distinction in those cases relative: Hildebrandt, M., Profiling and AmI, p. 276. *In: K. Rannenberg, D. Royer, A. Deuker, The Future of Identity in the Information Society. Challenges and Opportunities*. Springer 2009. Hildebrandt also refers to the different steps in the KDD or data mining process, as described in section 2.3.2. of this dissertation, which provides a better insight into the process than distinguishing between the creation and use of profiles.

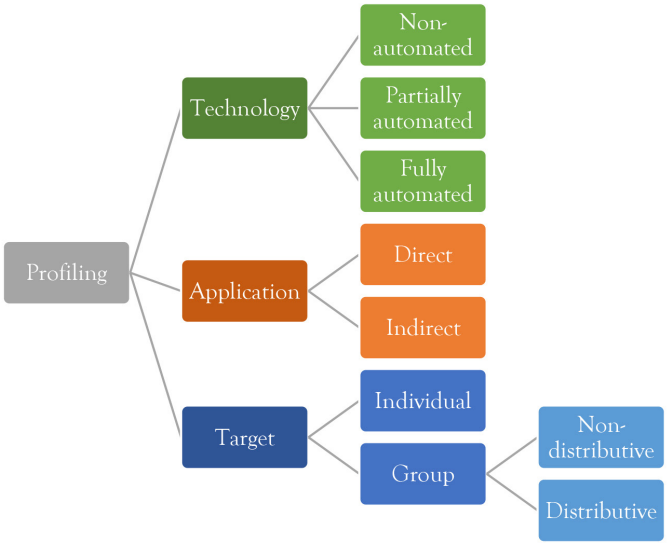

Figure 2. Distinctions in profiling.

The concept of profiling in this dissertation comprises most of these distinctions. Regarding the level of automation, this dissertation does not discuss non-automated profiling, as non-automated profiling does not use data processing technologies that nowadays are widespread and is therefore less relevant for this analysis. On the other hand, fully automated profiling (i.e., the completely automated process without any human assessment, decision-making, etc.) is mostly too futuristic at the time of writing this research. Most cases of profiling will have some component of human involvement. Therefore, when discussing profiling, this dissertation refers to partially automated profiling. Nonetheless, partially automated profiling simply means the involvement of some automated means. This still leaves open various possibilities regarding the level of such automation, whether for example deep learning is involved or not, or whether only a small part of the process is automated or the majority of the process, and so forth. The discussion in this dissertation will therefore cover a large part of the spectrum, ranging from somewhat automated to highly automated profiling.

2.4 The legal framing of profiling

After exploring the concepts of profiling found in various bodies of literature in section 2.2 and section 2.3, it is time to reflect briefly on the meaning of profiling in legal definitions. In addition to drawing from definitions of profiling from literature of various disciplines and descriptions of the process of profiling and technologies used, further meaning can be found in the way profiling is conceptualized in law. Law not only regulates but also provides definitions of its central concepts and expands on those in case law and explanatory documents, in the context of data protection such as Article 29 Working Party opinions and guidelines.[206]

In 1995 the DPD was introduced, regulating the processing of personal data in the EU. The DPD did not explicitly regulate profiling as such. However, the original proposal for the DPD did explicitly include the word 'profiling', stating that data subjects have the right not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality.[207] This original provision did require 'sole automatic processing' as the basis, seemingly excluding automated profiling that includes human involvement in the decision-making at any point. The final version of the DPD ultimately did regulate profiling to some extent by regulating automated decision-making in article 15:

> *Article 15 - Automated individual decisions*
>
> *1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. (…)*

Paragraph 1 of article 15 DPD mentioned automated processing of data for evaluation of personal aspects, which should be considered part of profiling. Other than that, the DPD did not mention profiling or explain what is meant by profiling. It at least excluded profiling that is a completely manual process, such as a handwritten list of characteristics, which is only logical, as the scope of data protection legislation requires processing of data.

---

206 For an analysis of the regulation of profiling, inter alia through data protection legislation, see chapter 4.

207 Commission Communication on the protection of individuals in relation to the processing of personal data in the community and information security, COM(90) 314 final SYN 287 and 288, Brussels, 13 September 1990.

Next to the data protection legislation of the EU, there is also the legislation by the CoE concerning personal data. The Convention 108[208] of 1981, updated in 2018 and now known as Convention 108+[209], regulates the processing of personal data. However, Convention 108+ does not mention profiling in the definitions or in any of the provisions. There is a provision regulating automated decision-making to some extent, which includes profiling[210], but the term profiling is not used or explained. Only in the explanatory report provided by the CoE is profiling explicitly mentioned. There profiling is not explained either, but some statements regarding automated decision-making are made that connect to profiling. For example, the individual has the right to challenge an automated decision on e.g. the basis of "(…) *the irrelevance of the profile to be applied to his or her particular situation* (…)."[211] This suggests that profiles can or will often be used to inform automated decision-making. And: "*Data subjects should be entitled to know the reasoning underlying the processing of data,* (…) *in particular in cases involving the use of algorithms for automated-decision-making including profiling. For instance in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a 'yes' or 'no' decision, and not simply information on the decision itself.*"[212]

Separate from Convention 108, in 2010 the Committee of Ministers of the CoE adopted a recommendation on profiling.[213] The recommendation outlines the impact of profiling and the relation to the rights of individuals but also recommends governments to ensure that the appendix and recommendation are applied in their laws and practices. The appendix to the recommendation provides the following definitions of the terms 'profile' and 'profiling':

> *" "Profile" refers to a set of data characterising a category of individuals that is intended to be applied to an individual";*

---

208 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, Strasbourg, 28/01/1981.

209 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223, Strasbourg, 10/10/2018.

210 Article 9 of Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223, Strasbourg, 10/10/2018.

211 Council of Europe, June 2018, *Convention 108+. Convention for the protection of individuals with regard to the processing of personal data*. para. 75. Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

212 Council of Europe, June 2018, *Convention 108+. Convention for the protection of individuals with regard to the processing of personal data*. para. 77. Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

213 Council of Europe, October 2011, The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 and explanatory memorandum. Available at: https://rm.coe.int/16807096c3.

> *" "Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."* [214]

Profile is here used to refer to a set of data. The set of data characterizes a category, so one could conclude it refers actually to a group profile. According to the definition that profile is intended to be applied to an individual. For data protection legislation that makes sense, as it concerns individuals. However, that does exclude the application of a profile to a group. Profiling is defined as a 'technique'. The Recommendation also describes three 'technically distinct' stages in the profiling process. They are, roughly, collection of data, analysis of data determining characteristics and the connections between them, and inferencing to determine or predict characteristics:

> *"– a stage during which digitised observations regarding individuals' behaviour or characteristics are collected and stored on a large scale (data warehousing). The resulting data may be nominative, coded or anonymous;*
> *– a stage during which these data are analysed and "probed" (data mining) permitting the determination of correlations between different behaviours/ characteristics and other behaviours or characteristics;*
> *– an inference stage during which, on the basis of certain observable behavioural variables or characteristics specific to a generally identified individual, new past, present or future characteristics or behavioural variables are deduced."*[215]

In the EU, in 2016 the data protection reform package was adopted, introducing the GDPR[216] and the LED[217]. The GDPR replaced the DPD and places more emphasis on profiling, regulating the practice of profiling explicitly and also providing for a specific definition. Article 4 under (4) of the GDPR gives the following definition:

---

214 Council of Europe, October 2011, The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 and explanatory memorandum, p. 9. Available at: https://rm.coe.int/16807096c3.

215 Council of Europe, October 2011, The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 and explanatory memorandum, p. 25. Available at: https://rm.coe.int/16807096c3.

216 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

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

> *"'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements(…)".*

The LED regulates profiling slightly differently but uses the exact same definition.[218] This definition found in the GDPR and LED contains several elements. First, the automated processing of personal data, excluding non-automated profiling. Second, the use of personal data to evaluate personal aspects. Third, it only concerns the data of a natural person. Lastly, it provides a non-exhaustive enumeration of characteristics that can be profiled, and states that it involves an analysis or prediction of these characteristics, such as a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[219]

To understand the definition of profiling as provided in the GDPR and the LED further, one can look at the Article 29 Working Party guidance. To further explain or illustrate the definition of profiling under the GDPR, The Article 29 Working Party offered the following description of profiling:

> *"Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar".*[220]

The Article 29 Working Party offered another description or further explanation of profiling:

> *"Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to*

---

218 Article 3 under (4) of the LED.

219 See also: Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, p. 7.

220 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, p. 7.

> *analyse and/or make predictions about, for example, their: ability to perform a task; interests; or likely behaviour."*[221]

These explanations of the Article 29 Working Party of the profiling definition under data protection legislation make clear, if it was not already, that profiling is a procedure highly focused on inferences. Most definitions or descriptions label profiling as a process or activity. In addition, they point out that statistical deductions can be used, which is indeed an important element of profiling. And they point to the focus on predictions and inferring information from statistically similar individuals. This highlights the fact that profiling is very reliant on probabilities and assumptions: individuals appear statistically the same but might not be in real life and behaviour or traits can be predicted or inferred instead of directly observed. That implies that inferred traits or behaviour may not actually occur or be true. Next, the Article 29 Working Party explained the term 'evaluating', from the definition of the GDPR, as profiling involving "some form of assessment or judgement about a person".[222] Lastly, the Article 29 Working Party made an interesting remark on the scope of profiling: "*A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification*".[223] So classification is seen as an often-occurring element of profiling, but classifying individuals in itself does not necessarily constitute profiling. As long as the classification does not lead to an evaluation, such as making predictions, or drawing conclusions about individuals, it does not serve as an assessment of individuals and is thus not profiling.[224] Classification can for example merely serve to create an overview for a company, but they might not make any assessment or decisions based on that categorization, nor use it to infer new information.

The Article 29 Working Party confirmed that the definition of profiling under the GDPR was inspired by the CoE Profiling Recommendation from 2010, but not identical to it, as the 2010 Recommendation specifically excluded processing that does not include inferences.[225]

---

221 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, p. 7.

222 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, p. 7.

223 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, p. 7.

224 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, p. 7.

225 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, p. 7.

2.5 Risk profiling in the law enforcement context

Profiling is used in many ways, as the legal and technical definitions of profiling display[226], to ascribe characteristics to individuals, groups or locations. This characterization and assessment function that profiling fulfills allows profiling to be used for example to determine which advertisements to display, which hiring decision to make, or which individuals to stop at border controls. One way in which profiling is deployed is to assess certain risks, in which the characteristics attributed to individuals or groups relate to a level of risk that the profiled subject poses. In both the public and private sectors, risk profiles are being used. In the private sector risk profiles are used to assess for example the risk of distributing credit to a customer[227], in the public sector to choose a target for policy or more specifically in criminal investigations to identify suspects, to assess and predict where crime will take place or to disclose criminal networks.[228] The level of risk can constitute for example a financial risk[229], a risk of pollution, or a risk of bodily harm. After having explored profiling in general, this section will focus on a specific application of profiling, namely that of risk profiling, more particularly in the sector of law enforcement, which has specific characteristics that will be detailed further in chapter 3. First, the concept of risk profiling will be explained, using definitions of profiling and of the concept risk to come to a working definition of risk profiling and tailor it to the specific law enforcement context. Subsequently the use of risk profiling in practice in the law enforcement domain is discussed using specific cases.

2.5.1. The concept of risk profiling in the law enforcement context

The focus of the concept of risk is to measure the chance of occurrence of future events and the impact thereof, and to allow decision-making on the basis thereof.[230] Risk has a negative connotation in the sense that it represents a future event that is to be monitored, mitigated, or controlled.[231]

---

226 See section 2.2.

227 Custers, B. "Data mining and Profiling in Big Data". *In: The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by Bruce A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

228 Custers, B. "Data mining and Profiling in Big Data". *In: The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by Bruce A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

229 See Swedloff, R., Risk Classification's Big Data (R)evolution (2014). Connecticut Insurance Law Journal, Vol. 21, 2014. Available at SSRN: https://ssrn.com/abstract=2566594, on the use of Big Data analytics in the insurance sector.

230 Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk, p. 34. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

231 Aradau, C., Lobo-Guerrero, L., and van Munster, R. "Security, Technologies of Risk and the Political: Guest Editors' Introduction". *Security Dialogue* 39, no. 2–3 (April 2008): 147-154. https://doi.org/10.1177/0967010608089159.

The concept of risk has a close connotation to notions such as probability and uncertainty. Risk is a quantitative phenomenon: it can be measured. One can make an assessment of the probability that a harmful event will occur and estimate the severity of the damage or the impact, or, risk is at least an attempt to tame uncertainty and contingency.[232] While probabilities form an inherent part of risk, uncertainty can be seen as a different concept. Uncertainty is a qualitative notion[233], it cannot be measured whether an uncertain event will occur. The only thing that can be said about an uncertain factor is that it is not 100% certain. On the other hand, risk is calculable, at least to some extent. Some authors nuance the quantitative nature of risk and its separation from uncertainty, due to the consideration that any predictions about future behaviour are inherently uncertain and speculative.[234] For example the likelihood or risk that someone will commit a crime is an uncertain prediction; one might try to calculate and evaluate chances and act accordingly, but it will still be an uncertain event.[235]

Risk is intrinsically linked to the first mathematical prediction tool, which is the theory of probability.[236] Probability theory acknowledges that some outcomes are more likely than others, creating weighted probability.[237] Weighted probability forms a part of decision-making, as it demonstrates the most probable outcome.[238] With the emergence of this probability theory, numerical assessment became possible through the science of statistics.[239] Statistics allow for a measurement and establishment of patterns of regularities in datasets, enabling the drafting of probabilities.[240] Today statistics play a prominent role in all sectors of society to assess risks and to cast predictions.

---

232 Aradau, C., Lobo-Guerrero, L., and van Munster, R. "Security, Technologies of Risk and the Political: Guest Editors' Introduction". *Security Dialogue* 39, no. 2–3 (April 2008): 147-154. https://doi.org/10.1177/0967010608089159.

233 Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk, p. 34. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

234 McCulloch, J., & Wilson, D., *Pre-crime: Pre-emption, precaution and the future*. Routledge Frontiers of Criminal Justice, Routledge: New York 2017, p. 37.

235 McCulloch, J., & Wilson, D., *Pre-crime: Pre-emption, precaution and the future*. Routledge Frontiers of Criminal Justice, Routledge: New York 2017, p. 37

236 For a complete discussion on risk and probability theory see Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk, p. 34-37. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

237 Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk, p. 36. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

238 Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk, p. 36. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

239 Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk, p. 34. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

240 Bernstein, P. L. *Against The Gods - The Remarkable Story of Risk*. New York: John Wiley & Sons Inc., 1996, p. 77.

Next to probabilities, the other component of risk is the impact. The chance that an event occurs is important but does not say anything about the scale of the event or the possible damage, while the consequences of an event are extremely important in determining priorities. One can distinguish different scenarios when combining the probability of the event and the impact: low-impact/low-probability, low-impact/high-probability, high-impact/low-probability and high-impact/high-probability. Risks that score low on both sides are usually not the focus of prevention, the same goes for a more probable event that has low impact. However, it depends on the type of impact whether an event is worth preventing and to what extent: for example, an event such as getting sick at the time of a holiday and canceling the trip is very much of interest to insurance companies and the person falling ill, but does not constitute the type of risk (assessment) that involves many people. When the event in question is a slight criminal offence, such as shoplifting, more people have an interest in that event being prevented. However, the risks that score high on the impact side are of interest to a possibly much larger group of people or to society, posing a higher risk of harm or of more severe harm. Preemption and security strategies focus most on the risks that have a high impact but have a low probability of occurrence.[241] Examples of such high-impact/low-probability risk events are pandemics, natural disasters and terrorist attacks.[242] Risk profiling by law enforcement falls into the category of high probability and relatively high impact, I would argue. While not all crime that is sought to be prevented through risk profiling has the same impact as terrorist attacks in high impact, it is still impact high enough in terms of impact on victims and society for police to want to prevent such events form taking place; for example burglaries, crimes of violence or organized crimes.

For the purposes of this research, risk will be understood as consisting of a descriptive part, describing statistics such as chances and predicted harm, and a normative part, reflecting the desirability of what is to be won or lost by making a decision.[243] With the element of decision-making public policy or business strategy comes into play. Decisions have to be made about what level of risk is desirable to provide insurance, which risk of harm to individuals or society is to be policed, which risk of harm to the environment is acceptable, and so forth.

---

241 De Goede, M., Simon, S., and Hoijtink, M. "Performing preemption." *Security Dialogue* 45, no. 5 (2014): 411-422.

242 De Goede, M., Simon, S., and Hoijtink, M. "Performing preemption." *Security Dialogue* 45, no. 5 (2014): 411-422.

243 Based on Bernstein, P. L. *Against The Gods - The Remarkable Story of Risk*. New York: John Wiley & Sons Inc., 1996, and, Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

A risk model will assist in determining the descriptive and normative part, or in cases of a fully automated process, rather than informing the process or outcome, the risk analysis can be the decision in itself.

Risk profiling can be used to identify individuals that match certain characteristics, or to predict people's behaviour. In the context of law enforcement, profiling is used to assess the risk that an individual poses to society, in terms of whether that person is likely to commit or re-commit crime. Identification and prediction are key factors for policing and justice. Risk profiling does not have a set definition, but looking at literature about risk in the law enforcement sector or criminal justice sector, multiple terms are frequently used. In the USA, 'risk assessment instruments' is a term used for tools analyzing the risk of crime that individuals pose.[244] More applications of analyzing risk in the criminal justice context are referred to as risk assessment or risk prediction.[245] In addition to risk assessment, there are applications that conduct risk ranking.[246] There are many instances of predictive policing, both in the USA and countries in the EU. Other terms to refer to similar practices are pre-emptive surveillance or pre-emptive policing and surveillance in the pre-crime society, used by van Brakel and de Hert.[247] In their book, McCulloch and Wilson make the distinction between a traditional criminal justice approach, a crime risk approach and a pre-crime approach.[248] The distinction between the latter two is not always very clear, and it can be questioned whether the difference between the risk and pre-crime approach is very relevant. However, it is interesting to see their description of the characteristics of these approaches to determine what risk profiling is and how it distinguishes itself from more traditional policing. McCulloch and Wilson perceive the traditional criminal justice approach to focus on past crime, while the crime risk and pre-crime approach are of a preventative or anticipatory nature.

---

244 Slobogin, C., Principles of Risk Assessment: Sentencing and Policing (February 27, 2018). *Ohio State Journal of Criminal Law*, Vol. 15, 2018; Vanderbilt Law Research Paper No. 18-09. Available at SSRN: https://ssrn.com/abstract=3131027.

245 Werth, R., Risk and punishment: The recent history and uncertain future of actuarial, algorithmic, and evidence based penal techniques. *Sociology Compass*. 2019; 13:e12659. https://doi.org/10.1111/soc4.12659; Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges.

246 Chicago Police Department Special Order S09-11, Subject Assessment and Information Dashboard (SAID), 9 January 2019, available at: http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html.

247 van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. in 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press; Van Brakel, R. & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies*. 20. 163-192.

248 McCulloch, J., & Wilson, D., *Pre-crime: Pre-emption, precaution and the future*. Routledge Frontiers of Criminal Justice, Routledge: New York 2017.

This shift is related to the perceived goal of the criminal justice system, which under the traditional approach is partially retribution and partly reparation, while under the other two approaches the goal is preventing harm. Another big difference between the traditional approach and the other two approaches is in how the suspect is perceived: traditionally it was important to understand the reasoning of a suspect or defendant that plays a role in the intent, but with the crime risk and pre-crime approach this is of less relevance. Records and statistics such as previous offences can inform the criminal justice process without understanding the reasoning of the suspect or requiring much causal relationships between acts in their past. This shift away from *mens rea* (the guilty mind) is a big difference between the criminal profiling as discussed before, where the aim is to get into the criminal's mind, and the modern type of profiling where risk is assessed based on potential relevant factors and statistics. As past offences are taken as a given, this also has consequences for the presumption of innocence and burden of proof when comparing the traditional approach with the crime risk or pre-crime approach.[249] The following table provided by McCulloch and Wilson displays the characteristics of said approaches clearly:

Table 1. Different approaches to criminal justice[250]

Traditional criminal justice	Crime risk	Pre-crime
Addresses past crime	Addresses identified crime threat	Addresses unidentified crime threat
Focuses on completed or imminent crime	Focuses on prior offending	Focuses on non-imminent crime
Aims to punish past crimes	Aims to prevent repeat offending	Aims to pre-empt anticipated crime
Past crimes are reconstructed in an attempt to understand and solve crimes	Prior convictions are used as a basis for understanding and assessing future crime risk	Anticipated crimes are preconstructed to give substance and form to non-imminent crimes
Guilty acts and guilty mind are essential elements for establishing criminal liability	Criminal history is the basis for coercive state interventions	Suspicious identity or outlawed associations are the basis for coercive state intervention and/or criminal liability

[249] McCulloch, J., & Wilson, D., *Pre-crime: Pre-emption, precaution and the future*. Routledge Frontiers of Criminal Justice, Routledge: New York 2017, p. 9.

[250] McCulloch, J., & Wilson, D., *Pre-crime: Pre-emption, precaution and the future*. Routledge Frontiers of Criminal Justice, Routledge: New York 2017, p. 9.

Table 1. Continued

Traditional criminal justice	Crime risk	Pre-crime
Process commences with the presumption of innocence	Process commences with a history of offending and suspicion that such offending could reoccur	Process commences with suspicion
Probative evidence that crime committed required as a basis of coercive state intervention	Prior convictions and belief that offender is likely to reoffend required for coercive state intervention	Speculative intelligence may be the basis of coercive state intervention
Beyond reasonable doubt burden of proof required as a basis for conviction and punishment	Past offending used to calculate the future probability of offending and basis for coercive state intervention	Uncertain possibilities and imagination underpin a precautionary approach and rationale for coercive state intervention
Actions that amount to criminal behaviour specified and clear	n/a	Acts that are potentially criminal may be unspecified and are unclear

This table makes clear that with the new technologies, the criminal justice sector has shifted more towards prevention and future events, instead of addressing already committed crimes, and towards more focus on criminal history combined with a precautionary approach versus only using evidence of the crime at hand or focusing on the guilty mind or guilty acts.

All of these terms, such as risk based policing, preemptive policing, predictive policing or risk assessment, refer to some type of (data) analysis to determine the risk of committing crime that individuals or groups pose or to determine the risk that a crime is committed in an area, and possibly acting upon that risk through policing or other interventions. Risk profiling sometimes overlaps with one of these terms, for example predictive policing can be a form of risk profiling, but in general risk profiling can be seen as a term on its own.

Risk profiling in the law enforcement context should also be distinguished from criminal profiling. With criminal profiling, the aim is to get inside and understand the criminal's mind.[251] An example of this are profiles that are made of serial killers,

[251] J.M. Dinant, C. Lazaro, Y. Poullet, N. Lefever, A. Rouvroy: Application of Convention 108 to the profiling mechanism Some ideas for the future work of the consultative committee, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-Pd) 24th meeting 13-14 March 2008 Strasbourg, G01 (TPD), Secretariat document prepared by the Council of Europe Directorate General of Human Rights and Legal Affairs, Strasbourg, 11 January 2008 T-PD(2008)01. Available at: https://rm.coe.int/16806840b9.

based on characteristics of the crime, to be able to identify them. With risk profiling the aim is not to understand the motives which (might) lead to criminal behaviour, but to establish a correlation between certain characteristics that the individual shares with other 'similar' individuals and a given behaviour which one wants to predict or influence.[252] While criminal profiling tends to require analysis conducted by humans, risk profiling relies more on statistical analysis and can be practiced by means of a computer with minimum human intervention.[253]

Risk profiling can also be separated from law enforcement descriptions of profiling. More often than not when people discuss profiling and law enforcement, outside of the data protection context, profiling is a synonym for ethnic profiling.[254] Profiling can have discriminatory effects, or target ethnicity; in that sense these issues play a role in later chapters. Using profiling definitions that solely focus on ethnicity are, however, too narrow for this research.

Fuster et al. propose a description for profiling in a specific context with a specific purpose, namely that profiling is used "*in contemporary security-related discussions as referring to the use of predictive data mining to establish recurrent patterns or 'profiles' permitting the classification of individuals into different categories*".[255] But they do not explicitly say if they mean risk profiling and if they mean 'crime' by security-related. Similarly, Vedder also discusses profiling for risk assessment purposes and applications to test for patterns in criminal behaviour, but does not explain what is meant by it or if he means

---

252 J.M. Dinant, C. Lazaro, Y. Poullet, N. Lefever, A. Rouvroy: Application of Convention 108 to the profiling mechanism Some ideas for the future work of the consultative committee, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-Pd) 24th meeting 13-14 March 2008 Strasbourg, G01 (TPD), Secretariat document prepared by the Council of Europe Directorate General of Human Rights and Legal Affairs, Strasbourg, 11 January 2008 T-PD(2008)01. Available at: https://rm.coe.int/16806840b9.

253 J.M. Dinant, C. Lazaro, Y. Poullet, N. Lefever, A. Rouvroy: Application of Convention 108 to the profiling mechanism Some ideas for the future work of the consultative committee, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-Pd) 24th meeting 13-14 March 2008 Strasbourg, G01 (TPD), Secretariat document prepared by the Council of Europe Directorate General of Human Rights and Legal Affairs, Strasbourg, 11 January 2008 T-PD(2008)01. Available at: https://rm.coe.int/16806840b9.

254 The list is endless, but see e.g.: Pap L. A., 'Profiling, Data Mining and Law Enforcement: Definitions' (2009) 50 *Annales U Sci Budapestinensis Rolando Eotvos Nominatae* 277; Ward, J. D. (2002). Race, ethnicity, and law enforcement profiling: Implications for public policy. *Public Administration Review*, 62(6), 726-735; Harcourt, B.E., *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*, The University of Chicago Press 2007.

255 Fuster G., Gutwirth S., Erika E. (June 2010), Profiling in the European Union: A high-risk practice. INEX Policy Brief, no. 10, p. 1-2.

risk profiling.[256] Custers comes closest to defining risk profiling, as it is a term that he uses in multiple papers[257], and in one paper offers a short description of risk profiles:

> *"The knowledge discovered [through data mining] may concern people, in which case it may result in profiles. These profiles may concern individuals, resulting in individual profiles, or they may concern groups, resulting in group profiles. When the knowledge reveals the probabilities of particular characteristics of individuals or groups, the profiles are generally referred to as risk profiles*".[258]

While risk profiles certainly revolve around probabilistic behaviour and traits, there is more to them. A working definition of risk profiling in the law enforcement sector can be useful to fine-tune what we are discussing and discuss separate elements of this concept and practice. To come to a working definition of risk profiling and subsequently further specify it to the law enforcement sector, the general definitions of profiling, and to some extent of profiling in the law enforcement sector, as discussed in section 2.2, section 2.4, and here in section 2.5, need to be fine-tuned. One of the components of Hildebrandt's definition of profiling (see section 2.2) is the process of discovering patterns that enable anticipation of future events.[259] In the context of law enforcement, future events matter just as much, sometimes even more than past events, as law enforcement actors can act reactively as well as proactively. Specifying further, examining the 'identifying' element from Hildebrandt's definition, risk profiling is concerned with identifying individuals in only one way, which is identifying suspects or perpetrators, so those other individuals involved in a crime. Treating an individual in the light of certain characteristics, as demonstrated in the definition of Bygrave (see section 2.2), means in the law enforcement context applying measures or decisions accordingly.

Based on these definitions and the discussions in this chapter, keeping the specific purpose of risk profiling in the law enforcement sector in mind, I propose the following

---

256 Vedder, A. KDD: The challenge to individualism. *Ethics and Information Technology* 1, 275–281 (1999). https://doi.org/10.1023/A:1010016102284.

257 For example in "Custers, B. Risk Profiling of Money Laundering and Terrorism Funding; Practical Problems of Current Information Strategies. In Proceedings of the 9th International Conference on Enterprise Information Systems 2007", Custers mentions risk profiling but does not explain what it is. In Dutch literature risk profiling ('risico profilering') is also used often to refer to practices of focusing policing on problematic individuals for example in terms of tax fraud or crime, in the administrative law sector and sometimes criminal law context. But also there it is common not to explain what is meant by risk profiling.

258 Custers, B. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by B. A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

259 Hildebrandt, M., Profiling and AmI, In: *K. Rannenberg, D. Royer, A. Deuker, The Future of Identity in the Information Society. Challenges and Opportunities*. Springer 2009, p. 289.

working definition of risk profiling. Risk profiling is the *categorizing or ranking* of individuals or groups, sometimes *including automated decision-making*, *using correlations and probabilities* drawn from combined and/or aggregated data, to *infer information used to evaluate or predict behaviour* or *identify individuals* in relation to the level of risk that is posed to the protection of interests and rights safeguarded by criminal law. To provide some more guidance, the core elements of the definition are briefly explained.

'categorizing or ranking'- Categorizing or ranking of individuals or groups is a phenomenon that is becoming common practice in all sectors of current society,[260] whether it concerns credit scores[261], insurance[262], admission rankings for universities[263], insurance policies categorizing on zip code, or ranking the crime risk of individuals based on social media profiles[264]. The possibility to link various databases in combination with the use of algorithms to make patterns visible facilitates the comparing of individuals or groups. In the context of risk profiling, individuals, groups or locations can receive a risk score or label assessing a specific type of risk compared to others. For the law enforcement context this means that individuals are ranked according their level of risk, individuals are categorized into different risk groups, or locations are given a ranking of being likely to have a certain type of crime taking place.

'including automated decision-making'- As described, risk profiling usually entails some decision component, and in some cases the decision-making will take place in an automated way. A good example is a system that not only assigns a risk score to an individual but also automatically connects a legal consequence to that score, such as sending a speeding ticket or determining the bail, taking an immediate decision. Here the analysis and decision form one integral act conducted by the system; there is no human making the decision based on the analysis outcome. Risk profiling in itself can simply constitute the compiling of risk profiles or risk assessments, it can be followed by a human-made decision to employ measures, or it can trigger a decision in itself constituting a form of automated decision-making. Therefore, the level of human

---

260 Zarsky, T., Understanding Discrimination in the Scored Society, *Washington Law Review*, Vol. 89:1375, 2014; Citron, Danielle Keats and Frank Pasquale. "The Scored Society: Due Process for Automated Predictions". *Washington Law Review* 89, no. 1 (March 2014): 1-34.

261 Zarsky, T., Understanding Discrimination in the Scored Society, *Washington Law Review*, Vol. 89:1375, 2014; D. Keats Citron and F. Pasquale. "The Scored Society: Due Process for Automated Predictions". *Washington Law Review* 89, no. 1 (March 2014): 1-34.

262 Swedloff, R., Risk Classification's Big Data (R)evolution (2014). *Connecticut Insurance Law Journal*, Vol. 21. Available at SSRN: https://ssrn.com/abstract=2566594.

263 O' Neil C., *Weapons of Math Destruction*, Crown publishers 2016, ISBN 0553418815.

264 van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. in 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press.

involvement will differ per system, which can have consequences for the opacity or understandability of the system and its results.[265]

'using correlations and probabilities'- Risk profiles depend highly on probabilities, as the notion of risk relies on a measurable chance of an outcome, which does not necessarily correspond to actual facts. For example, it could be possible to see a correlation between the neighborhood an individual lives in and the type of crime that an offender from that neighborhood commits, such as fraud, using that correlation to ascribe a probability of the crime of fraud to that individual. Or for example, the risk profiling algorithm can have learned which combination of characteristics in individuals correlates to a high chance of re-offending.[266]

'infer information used to evaluate or predict behaviour' or *'identify'*- As discussed in section 2.2, this is a key component of profiling. Placing individuals in groups or comparing them to others to rank them, allows for adding additional information based on that categorization. For example, because an individual lives in a specific area and has a juvenile record, they could be placed in a group of people likely to commit a misdemeanor; this likelihood can then be added to the individual's profile. The goal of identifying is similar to evaluating; risk profiles are used to indicate which individuals are likely to be involved in crime, most predominantly as the perpetrator.

2.5.2. The uses of risk profiling in the law enforcement sector

Risk profiling can pertain to different practices of law enforcement; therefore, this section aims to give further insight into different types of risk profiling practices. One category of the use of risk profiling is for general policing purposes, here the police uses its general mandate for maintaining law and order. A second category is the use of risk profiling in criminal investigation, entailing investigating a specific case, searching for a suspect or investigating a suspect further. A third category is the use of risk profiling after the investigation stage, to determine bail, for sentencing or to make a parole decision. Different practices rely on different legal bases and create different societal challenges.

---

265 Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* (July–December 2016), pp. 1–21.

266 Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges; Oswald Marion, Jamie Grace, Sheena Urwin & Geoffrey C. Barnes (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, 27:2, 223-250, DOI: 10.1080/13600834.2018.1458455.

At the same time it has to be acknowledged that it is difficult to present examples that solely pertain to one category: sometimes risk profiling programs span different stages of policing or of the criminal justice chain.

2.5.2.1 General policing: maintaining law & order

Risk profiling is used in general policing to enhance efficiency. Police cannot patrol, monitor or surveil everywhere at the same time. Examples of location-based policing, or hotspot policing, are numerous. These so-called predictive policing systems are targeted at efficient deployment of police patrols. In selecting a location various sources of data will be used, ranging from non-personal data such as the distance to the highway (for escape routes) to data about income of the inhabitants of the area and data about previous criminal activity in the area. Algorithms pinpoint the level of risk for areas, so that police officers can be deployed accordingly. This type of risk profiling is very well established in the USA, but also exists in Europe.[267] In the Netherlands, the CAS is used for the creation of a grid that is updated every 14 days; this grid shows what crime is likely to take place and on which time of day in every square of the targeted area. This system was first introduced in the capital, Amsterdam, but is now being tested across the country.[268]

Risk profiling that targets a location, such as predictive policing, is a type of risk profiling that allows for general policing and monitoring. However, while such a system is targeted at locations, it indirectly profiles the residents of that area.[269] A risk profiling system that targets areas attaches a risk label to a certain area and police patrols are sent there accordingly.

The deployment of police patrols can impact the perspective that residents and outsiders have on this area, as it can be deemed as an area with high criminality, or as a 'bad area'. In addition, sending police patrols to a specific area can lead to an increase in crime detection in that area: the more police officers are present there, the higher the chance that they will detect crime eventually.

---

267 Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges.

268 Mali, C. Bronkhorst-Giesen, M. den Hengst, Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot. Politie Academie, February 2017, available at: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93263.PDF.

269 This same argument was in the meantime published in: Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12, p. 231-232.

Detecting more crime will in turn further increase the number of patrols in that area and measures taken against residents of this area. In that sense a self-fulfilling prophecy can be created.[270] Since the areas that the system targets are traditionally seen by police as problematic areas, inhabitants can easily already be on the radar, but their risk level will fluctuate according to the risk score of the area and they might be labelled as high risk unfairly. On the other hand it can also be argued, for example by law enforcement deploying these type of systems, that sending more police officers to an area labelled as high risk will cause crime to go down in that area because of the heightened surveillance and deterrent effect. As a consequence, the risk level in that targeted area will go down and crime moves to other areas.[271]

2.5.2.2. Criminal investigation

In the age of Big Data, law enforcement has access to enormous amounts of data, making it difficult to detect patterns without automated means. However, when an algorithm searches for suspicious patterns and categorizes individuals or groups, it is attainable to search all the data at hand and easily find that one suspect in a haystack of data. Rather than searching for information about a specific person, the system creates a categorization specifying which individuals are high risk (based on the risk model or query that the algorithm works with) and who could be (further) looked into. This forms a major shift from traditional policing, in which a specific individual is usually the starting point for a query into sources, or in which a specific crime is the starting point and where human non-automated profiling can take a long time to detect a suspect. Alternatively, risk profiling can be used to assess the risk of individuals or groups that are being surveilled to determine whether to deploy further investigative powers against them.
Thus, when speaking of risk profiles used for criminal investigation, I refer to criminal investigation in a broad sense, both as risk profiling leading to the starting point of a criminal investigation, as well as risk profiling used in an ongoing criminal investigation (for example in evidence collection). The contrast with risk profiling discussed in section 2.5.2.1, for general policing purposes, is that it concerns a different policing task altogether; the former is aimed at maintaining the law and order, while the latter refers to criminal investigation, building a reasonable suspicion or determining which police powers to use against a specific suspect.

---

270 This same argumentation was in the meantime published in: Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12, p. 231-232; see also Robinson D (2017) The Challenges of Prediction: Lessons from Criminal Justice. I/S: A *Journal of Law and Policy for the Information Society*. https://ssrn.com/abstract=3054115. Last accessed 30 September 2018.

271 More on the possible self-fulfilling or -denying prophecies can be found in chapter 3, for example in section 3.3

An example of using risk profiling to find suspects of crime is the Dutch SyRI.[272] SyRI is used to monitor tax fraud, fraud with social benefits and fraud with labour legislation. SyRI was officially launched in 2014 and was employed by the Dutch Ministry of Social Welfare & Employment (hereafter the 'Dutch Ministry'). The system can be used by different parties: several governmental actors together can launch a request with the Dutch Ministry to make use of SyRI. SyRI contains large databases consisting of sources such as financial data of citizens, data on social benefits history of citizens, or data about education. SyRI works with a predetermined risk model in each instance of collaboration between governmental actors. The risk model set up for the specific collaboration and goal is run through the system and SyRI indicates which individuals are high risk and which are low risk for one or more of the three types of fraud. The results for low risk are deleted, while the citizens that receive a high risk label can be further investigated. This investigation can be conducted by the police, special law enforcement officers, supervisory authorities, municipalities, immigration authorities, or other relevant authorities. So although the police is not the main actor in this process, the outcome can lead to a criminal investigation into fraud. This type of system could obviously work differently in different jurisdictions and be more focused on the law enforcement domain in some countries or situations, as opposed to administrative sanctions in other countries or situations, making it still an interesting example for this research. The risk indication SyRI provides is stored in a register that relevant public bodies can access. Because SyRI is used in varying collaborations, SyRI works differently each time, scanning for a different risk profile each time. Due to the broad scope of the system and the large governmental database involved, it is possible that many people living in the Netherlands are analyzed in the system.

Even though SyRI has been used for years now, its use has not been without resistance. The program raises issues of transparency, awareness and contestability. In March 2017, several NGOs and two citizens launched a court case challenging the legality of the system, to test whether SyRI is compliant with EU data protection legislation, the right to privacy and the right to fair trial. One of the points that was debated in the case is the secrecy of the risk models, but also the lawfulness of the automated decision-making and the broadness of the legal mandate to use SyRI.

---

272 The explanation of SyRI in the following two paragraphs originates from my earlier work, already published in the meantime: Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12, p. 230-231.

On the fifth of February 2020, the District Court of the Hague ruled that the legal basis used for SyRI was indeed a violation of several legal provisions, and subsequently seen together with the use of SyRI itself in practice, ruled that the legislation is in breach of article 8 of the ECHR.[273] This means that new legislation, complying with the standards set out by the court, will have to be drafted to use the risk profiling program again.

In general, examples of investigatory tools in criminal investigations tend be not publicly known, to protect the investigations. Therefore it is challenging to find information on the use of risk profiles in those processes, let alone information about the workings of such risk profiling systems. One use context that is relevant in that regard to illustrate at least part of the process is the use of large-scale data from which individuals can come to the fore to look into as suspects, based on automated searches with pre-defined search terms. One illustration of such a practice is the use of bulk data from cryptophones.[274] In such data analysis the characteristic of risk profiling comes to the fore of starting out with data and collecting evidence and matching suspects to that evidence later when their identity becomes known, rather than starting out with a specific suspect and then gathering evidence on that person. This is an interesting and controversial shift, as will be further discussed in chapter 6.

Ranking individuals based on their risk can be called 'heatlisting'. The term heatlisting is similar to the term heatmapping, used to profile areas to show on a map which areas are 'heated', meaning having a high crime ratio or likely to have a lot of criminal activity. These are so-called hotspots. An example of heatlisting is the risk profiling tool used by the Chicago Police Department, the Strategic Subject List (SSL).

It is seen by many as the first experiment with a predictive risk assessment in the law enforcement context that unlike most predictive policing was not focused on locations.[275] Where risk assessments by police of locations can be called heatmaps enabling 'hot spot policing', the SSL can be seen as a heatlist ranking the most dangerous individuals.

---

273 District Court of the Hague, 5 February 2020, ECLI:NL:RBDHA:2020:1878.

274 See chapter 6; Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02; Stevens, L., Hirsch Ballin, M., Galic, M., Buisman, S., Groothoff, B., Hamelzky, Y., & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2021(4), 234-245.

275 Brayne, S., Rosenblat, A., and Boyd, D. "Predictive Policing". Data & Civil Rights: a new era of policing and justice. October 27, 2015. https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf.

In January 2019 the SSL has been redesigned to the Subject Assessment and Information Dashboard (SAID) with the Crime and Victimization Risk Model (CVRM) as a component of the SAID. The SAID and CVRM tool are targeted at early intervention. The SAID applies to both offenders and victims, focusing on preventing crime from a societal perspective, not particularly targeting repeat offenders. The Chicago Police Department released a Special Order[276] to enact this change, which provides some basic information concerning the workings of the CVRM and its organizational place. The SAID and its CVRM tool are seen as means for early intervention into possible crime through the Custom Notification Program. Custom notifications identify at-risk individuals and reach out to advise them of the risks and consequences of their actions should they engage in criminal conduct.[277] The SAID is a decision aid system, not an automated decision-making system. The CVRM should be seen as a research tool to assist police by enabling prioritization of individuals to target first. Ultimately not the CVRM itself but the District Commander determines which individuals are deemed the most dangerous individuals of the district. The Chicago Police Department stresses that placement of an individual on the SAID is not a factor in determining a reasonable suspicion or probable cause and the risk assessment of the individual will not be included in case documentation.[278] The CVRM is a statistical model that estimates an individual's risk of becoming a victim or offender in a shooting or homicide in the next 18 months, based on risk factors from the individual's criminal or victimization history. The analysis is based on the individual's history.[279] However, while the analysis is focused on predicting the individual's future involvement in certain crimes, the model to perform this assessment has to be trained based on historical or aggregated data in order to make predictions about the meaning and consequence of a pattern found in behaviour correlating to aggregated data. Therefore, even though the assessment is said to be based solely on files and other data concerning the specific individual, the analysis is still based on statistics and to some extent assumptions. The individual's data that are used for the assessment consist of six characteristics: whether the individual has been the victim of a shooting incident; the age during the most recent arrest; whether the individual has been the victim of an aggravated battery or assault; the trend in criminal activity; whether the individual has a record of unlawful use of a weapon; whether the individual has a history of

276 Chicago Police Department Special Order S09-11, Subject Assessment and Information Dashboard (SAID), 9 January 2019, available at: http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html.

277 Chicago Police Department Special Order S09-11, Subject Assessment and Information Dashboard (SAID), 9 January 2019, available at: http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html.

278 Chicago Police Department Special Order S09-11, Subject Assessment and Information Dashboard (SAID), 9 January 2019, available at: http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html.

279 Chicago Police Department Special Order S09-11, Subject Assessment and Information Dashboard (SAID), 9 January 2019, available at: http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html.

arrests for violent offenses.[280] As of 20 September 2019, there were 437 individual recipients of custom notifications in the system. Interestingly, these are not just the individuals that are ranked on the CVRM as 'very high risk', but they consist of a mixture of individuals ranked from 'low risk' to 'very high risk'. The inclusion of lower ranked individuals seems strange but is caused by the fact that the CVRM is only one component within the Custom Notification Program, therefore individuals who score lower on the CVRM can still receive a notification that they are likely to become the offender or victim of a crime based on other assessments. A supervisory authority found many issues with the SSL, especially concerning bias[281] and unreliability of the risk model, leading to the advice to shut down the SSL.[282] Ultimately, the program was shut down in January 2020.[283]

An example of a service enabling threat scores is Beware by the company Intrado.[284] Intrado Beware is a mobile, cloud-based application used in the USA, which gathers contextual information from social media, commercial data and criminal records, creating an immediate risk score –green, yellow, or red- for individuals.[285]

Intrado Beware has a very specific purpose. It is targeted towards providing police officers with information about the suspect they are about to encounter when they respond to a 911-call from a victim and identifying whether this person is high risk in the sense of posing a risk to the security of the police officer. In this way police officers will for example arrive with their firearms at the ready in case a high-risk individual is detected.

---

280 Chicago Police Department Special Order S09-11, Subject Assessment and Information Dashboard (SAID), 9 January 2019, available at: http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html.

281 Richardson, R. and Schultz, J. and Crawford, K., Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (February 13, 2019). 94 *N.Y.U. L. REV. ONLINE* 192 (2019). Available at SSRN: https://ssrn.com/abstract=3333423.

282 City of Chicago Office of Inspector General, Advisory concerning the Chicago Police Department's Predictive Risk Models, January 2020, available at: https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf.

283 Gorner, J., and Sweeney, A., Chicago Tribune January 24, 2020: https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html; City of Chicago Office of Inspector General, Advisory concerning the Chicago Police Department's Predictive Risk Models, January 2020, available at: https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf.

284 The explanation of Intrado Beware in this paragraph originates from my earlier work, already published in the meantime: Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12, p. 229.

285 van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. in 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press; Slobogin, C., Principles of Risk Assessment: Sentencing and Policing (February 27, 2018). *Ohio State Journal of Criminal Law*, Vol. 15, 2018; Vanderbilt Law Research Paper No. 18-09. Available at SSRN: https://ssrn.com/abstract=3131027.

According to Slobogin, the idea behind programs such as Beware and various others, is that they come into play after the police identify a possible wrongdoer using traditional means. Such a service is then used to figure out which action to take, such as surveilling, stopping and frisking, or arresting.[286]

2.5.2.3. Post investigation: Sentencing, bail & parole decisions

In the past years there has been an expansion from predictive analysis of locations, such as predictive policing or mapping, towards predicting behaviour of individuals.[287] There has also been an expansion, at least in the USA, from using individual risk assessment only in probation and parole procedures, to using it in bail hearings and sentencing as well.[288]

Risk profiling is thus used to determine whether someone is allowed bail or probation, whether that person is at risk of reoffending, or determining the duration of incarceration. The most prominent example of risk profiling to determine parole, bail, or a prison sentence, is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool.[289] While there is a range of risk profiling or assessment systems being used in the USA, COMPAS is interesting as it is widely used in the USA and highly data-driven: many data points are used and the algorithm fully determines the outcome, being the risk level. There is no human decision maker that determines the risk.

COMPAS is software that predicts a defendant's risk of committing a misdemeanor or felony within two years of assessment based on 137 factors pertaining to the individual in combination with data about the criminal record of the individual.[290] COMPAS is used in the trial or post-trial stage. The algorithm for the risk assessment was developed by the company Northpointe and the logic of the algorithm is kept secret by the company.

---

286 Slobogin, C., Principles of Risk Assessment: Sentencing and Policing (February 27, 2018). *Ohio State Journal of Criminal Law*, Vol. 15, 2018; Vanderbilt Law Research Paper No. 18-09. Available at SSRN: https://ssrn.com/abstract=3131027.

287 Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges.

288 Oswald M., Grace, J., Urwin, S. & Barnes, G.C, (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, 27:2, 223-250, DOI: 10.1080/13600834.2018.1458455.

289 The explanation of COMPAS in the following two paragraphs originates from my earlier work, already published in the meantime: Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12, p. 232-233.

290 Dressel J, Farid, H (2018) The accuracy, fairness, and limits of predicting recidivism. *Science Advances* 4; eaao5580.

COMPAS makes use of 137 factors such as factors relating to the criminal history of the individual; non-compliance in court, bail, or probation procedures; criminality among family members or friends; habits of alcohol and drugs use; residence and living environment; education history; work situation; feelings of social isolation; and feelings of anger.[291]

COMPAS was the subject of much controversy in 2016 due to a public research report[292] and a court case.[293] In the case Loomis v. Wisconsin, Loomis, who was sentenced to six years of imprisonment based on the analysis of COMPAS, petitioned[294] for a reconsideration of his sentence, as COMPAS would violate his right to due process. The issues raised in the petition were:

"*(1) Whether it is a violation of a defendant's constitutional right to due process for a trial court to rely on the risk assessment results provided by a proprietary risk assessment instrument such as the Correctional Offender Management Profiling for Alternative Sanctions at sentencing because the proprietary nature of COMPAS prevents a defendant from challenging the accuracy and scientific validity of the risk assessment; and (2) whether it is a violation of a defendant's constitutional right to due process for a trial court to rely on such risk assessment results at sentencing because COMPAS assessments take gender and race into account in formulating the risk assessment*."[295]

Ultimately, the Wisconsin Supreme Court denied the petition and due process claims, which led to criticism on the system from a broader perspective. First of all there are transparency concerns, as the methodology used to produce the assessment was not disclosed to the court or to the defendant.[296]

---

291 Angwin, J., Larson, J., Mattu, S., and Kirchner, L. "Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks." ProPublica. May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Together with their report, the researchers of ProPublica made several files publicly available, such as a list with the factors that COMPAS uses in scoring.

292 Angwin, J., J. Larson, S. Mattu, and L. Kirchner. "Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks." ProPublica. May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

293 Washington, "How to argue with an algorithm: Lessons from the COMPAS-ProPublica debate." *Colo. Tech. LJ* 17 (2018): 131.

294 Loomis v. Wisconsin, docket no. 16-6387, available at: http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/. Last accessed 28 March 2020.

295 Loomis v. Wisconsin, docket no. 16-6387, available at: http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/. Last accessed 28 March 2020.

296 Author unknown, Harvard Law Review, March 2017, Volume 130, No. 5, 'State v. Loomis, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing, available at: https://harvardlawreview.org/2017/03/state-v-loomis/. Last accessed 28 March 2020; Washington, "How to argue with an algorithm: Lessons from the COMPAS-ProPublica debate." *Colo. Tech. LJ* 17 (2018): 131.

Second, the procedural safeguard of the court to alert judges to the dangers of these assessments — a 'written advisement'[297] — can be criticized for not creating meaningful judicial skepticism.[298] Although the petition was denied, this case highlights the new questions judges are faced with concerning these type of systems and the open questions regarding the due process of using these systems.[299]

To illustrate the use of a risk based system for parole decision-making in a European context, the OxRec systems used in the Netherlands is a good example. Dutch probation authorities[300] use the Recidivism estimation scales (RISc) as a risk classification tool to advise them in an estimation of recidivism risk. RISc is used in all stages of the criminal trial: in arraignment before the Examining Magistrate, in the criminal trial, in decision-making in penitentiary programs, in decision-making about 'placement at the discretion of the state'[301], and in decision-making on the conditions of probation.[302] OxRec is used as an actuarial risk assessment tool within the RISc system relying on both static and dynamic risk factors.[303] OxRec was developed originally by Oxford University and is designed to make a statistical analysis of the risk of general recidivism and of recidivism for violent crimes. In 2017, OxRec was adapted for the Dutch criminal justice system with the use of data from Statistics Netherlands, the Dutch Research and Documentation Centre (WODC) and data from the three Dutch probation authorities.[304] Group risk profiles are applied to individuals to be assessed. In the use of OxRec in the Dutch system, the probation officer drafts an advice about the situation in question in addition to the advice that follows from the OxRec system. The probation officer's advice can deviate from the one resulting from OxRec.[305]

---

297 Pre-Sentence Investigation (PSI) report. The Wisconsin circuit court ordered a PSI report on the defendant in Loomis, which included a risk assessment generated by the COMPAS algorithm. See: Washington, "How to argue with an algorithm: Lessons from the COMPAS-ProPublica debate." *Colo. Tech. LJ* 17 (2018): 131.

298 Author unknown, Harvard Law Review, March 2017, Volume 130, No. 5, 'State v. Loomis, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing, available at: https://harvardlawreview.org/2017/03/state-v-loomis/. Last accessed 28 March 2020.

299 Which is discussed in chapter 3, section 3.8.

300 Reclassering Nederland, Leger des Heils jeugdbescherming & reclassering, and Stichting Verslavingsreclassering GGZ.

301 In Dutch referred to as TBS. It is a hospital order that a court can impose if an offender has a serious psychiatric disorder.

302 Probation Netherlands, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

303 Static factors are factors that cannot be changed by the suspect or offender, such as age or criminal history. Dynamic factors are factors that are prone to change, such as employment status, address, financial situation, and so forth.

304 Reclassering Nederland, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

305 Reclassering Nederland, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

Through RISc, the results from the risk analysis per aspect -such as finances, relationships, substance use- are shown in a traffic light model, ranging from green to orange to red, next to the risk estimation from the OxRec.[306] Risk assessment tools, such as OxRec, are generally labelled as an assisting tool, meaning that it is not a form of fully automated decision-making but merely advisory in the decision-making process.[307] The Dutch example is definitely not the only such system used; another well-known system is the Harm Assessment Risk Tool (HART) system used in the UK to assist in risk based decision-making for predicting whether suspects and offenders are a low, moderate or high risk of (re)committing crimes in a two years period and apply measures or sentencing in accordance.[308]

2.6 Conclusions

This chapter analyzed the practice of risk profiling in the law enforcement sector. Profiling is a practice that has taken place for years but has really expanded in the past years due to technological developments in Big Data analytics, data mining and complex automated algorithms. The premise is that patterns can be found everywhere, so that law enforcement agencies have started collecting large volumes of data, not only to investigate but also to preempt criminal activity. Nowadays, the focus is not to get into the criminal's mind, but to have an overview of people's behaviour through data.

Examining profiling from a technical perspective, the process can be seen as consisting of several steps, one can distinguish between five actions and three stages. The first stage is gathering data, the second performing analysis on the data and the third is applying the profile. In the process of analyzing the data profiles will be constructed and groups or classifications will be formed, but these two activities feed into each other. Profiles are partly based on or derived from existing groups or classes but on the other hand, groups and classes are also formed by viewing profiles. In the phase of application of the profile, the profile is used to infer additional information concerning the subject of the profile and decisions can be made by applying the profile.

306 Reclassering Nederland, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

307 Van Wingerden, S. G. C., Leonardus Martinus Moerings, and J. A. Van Wilsem. *Recidiverisico en straftoemeting*. No. 2011-3. Sdu Uitgevers, 2011.

308 Oswald M., J. Grace, S. Urwin & G. C. Barnes (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, 27:2, 223-250, DOI: 10.1080/13600834.2018.1458455.

Profiling is reliant on data mining or KDD and nowadays on algorithms and machine learning. Profiling can range from being non-automated, to partially automated, to being a fully automated process. This research does not consider non-automated profiling.

However, most cases of profiling will have some component of human involvement. Therefore, when discussing profiling, this dissertation refers mostly to partially automated profiling.

Profiles can be applied to individuals or groups. For group profiling one can distinguish between distributive and non-distributive profiles. Distributive group profiling assumes that individuals share all the same attributes in a group. In non-distributive group profiling, a group is created of which all the individuals share (at least) one attribute. In this case, there are discrepancies between the different individuals. The non-distributive type is the most common: usually, people within a group do not share all of the same attributes. One can also distinguish between profiling where data is derived from individuals and groups and then profiles are applied to those same subjects, and profiling where this is not the case. This is the difference between direct and indirect profiling.[309]

To get a better understanding of profiling, it is useful to examine legal definitions of profiling. Legal definitions of profiling can be found in data protection legislation, more specifically in the DPD, the GDPR, the LED and the Convention 108, Convention 108+ and accompanying 2010 Recommendation on profiling. The analysis of the relevant literature on definitions of profiling revealed that there is a big difference in scope between general definitions of profiling in literature and definitions of profiling under data protection legislation. The scope of data protection legislation is limited to automated processing of data pertaining to natural persons; this naturally also limits the definition of profiling along those lines. Profiling can be non-automated or automated, while data protection legislation only considers automated profiling. The legal framework does not specify in definitions if any specific level of automation or a specific technique or technology is required. In line with the conceptualizations of profiling found in literature, the legal framework remains technology neutral in that it does not require for example the presence of a particular type of data mining, algorithms, deep learning, AI, and so forth. How the profiling process is conducted is left open in the definitions of data protection.

---

309 Jaquet-Chiffelle, D.O., Direct and Indirect Profiling in the Light of Virtual Persons. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008, p. 40.

When focusing on humans as the subjects of profiles, most definitions include both individual and group profiling.
One can distinguish between the use of groups or group profiles and application of those to individuals, and the application of group profiles to groups. Convention 108+ and the GDPR and LED speak of individuals in the profiling definitions. Mentioning individuals as the subject of inference, characterization and so forth, does not exclude the use of groups or group profiling in the stage of analysis, but it seems to imply that the data protection frameworks focus on individual profiling or the application of profiles on individuals.

Based on the definitions of profiling and personal data, the Convention 108+, GDPR and LED only include the use of personal data in the profiling process, while outside of these legal frameworks profiling can also mean the use of anonymized or aggregated data to create profiles before they are applied to an identified individual or group of identified individuals.[310] With regard to the application of profiling, the legal framework does not seem to distinguish between indirect profiling and direct profiling. The definitions of data protection legislation do not specify whether the profile has to be built using data solely concerning the data subject. However, the 2010 Recommendation offers a specific definition of a profile, in addition to the definition of profiling. From the definition of profiling alone, the 2010 Recommendation seems to focus on direct individual profiling, but the explanation of a profile makes clear that this includes situations in which there was an activity of grouping individuals previously and that information was applied to the individual in case, meaning that information about other individuals is used, so that we can also speak of indirect individual profiling.

Based on the definitions of profiling under data protection legislation, it does not appear that any of the stages in the process are not covered by legislation. The definitions do not explicitly mention the gathering of data in the profiling process, but this can be assumed to be present. The Article 29 Working Party explicitly mentioned the gathering of data as part of the profiling process and the CoE recommendation mentions all three stages of the profiling process explicitly in their explanation. Regarding the analysis phase, the definition from the GDPR and LED explicitly mention analysis, the Convention 108+ does not explicitly mention it but the CoE Recommendation does. All legal definitions mention decision-making based on the profile, and/or application of the profile and/or inference, and/or evaluating behaviour, and/or predicting behaviour, thus covering the application stage.

[310] As this chapter concerns definitions only, this conclusion can appear over-simplified. For an analysis of the legal framework and its scope, especially for data protection law, see chapter 4.

Overall, the definitions of profiling found in literature and the technical descriptions of profiling can be seen as complementary; one does not really limit or expand the scope of profiling compared to the other. These descriptions of profiling generally concur with the legal definitions on the combination of elements. Simply categorizing individuals for example will not be enough to speak of profiling, whether viewed from a legal standpoint or not. Important is the purpose, as the Article 29 Working Party stated, and the definitions from literature confirm. Profiling is not just about placing individuals in groups, or groups in broader groups; it is also not simply ranking individuals in a list. The key is inferring information and doing something with this information vis-à-vis certain people, whether it be evaluating or predicting certain aspects relating to them.

One way in which profiling is deployed is to assess certain risks, in which the characteristics attributed to individuals or groups relate to a level of risk that the profiled subject poses. For the purposes of this research, risk will be understood as consisting of a descriptive part describing statistics such as chances and predicted harm and a normative part reflecting the desirability of what is to be won or lost by making a decision.[311] Risk profiling can be used to identify individuals that match certain characteristics, or to predict people's behaviour. In the context of law enforcement, profiling is used to assess the risk that an individual poses to society, in terms of whether that person is likely to commit or re-commit crime. Identification and prediction are key factors for policing and justice. Risk profiling does not have a set definition, but the following working definition of risk profiling is proposed: risk profiling is the *categorizing or ranking* of individuals or groups, sometimes *including automated decision-making*, *using correlations and probabilities* drawn from combined and/or aggregated data, to *infer information used to evaluate or predict behaviour* in relation to the level of risk that is posed to the protection of interests and rights safeguarded by criminal law. Risk profiling can be deployed by law enforcement actors in different ways. Risk profiling can be used for general policing purposes, where the police uses its general mandate for maintaining law and order. Risk profiling can also be used in criminal investigations, entailing investigating a specific case, searching for a suspect or investigating a suspect further. Finally, risk profiling can also be used after the investigation stage, to determine bail or sentencing or to make a parole decision.

311 Based on Bernstein, P. L. *Against The Gods - The Remarkable Story of Risk*. New York: John Wiley & Son Inc., 1996, and, Gellert, R. (2017). *Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk*. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

In general policing, risk profiling is used for example to pinpoint where and when crime might take place, or which areas are high risk. In criminal investigations, risk profiling can be used to create a heatlist of individuals likely to commit crime, such as with the SSL system in Chicago. Or, for example, a risk model can be used to determine who is likely to be committing fraud, such as SyRI used in the Netherlands. The most prominent example of risk profiling used post investigation is the COMPAS tool used in the USA; for European examples we can look at tools such as OxRec.

The explanations of risk and risk profiling serve as basic knowledge for the rest of this dissertation. The examples of risk profiling used in the law enforcement sector are not meant as exhaustive, but rather to demonstrate the different types of risk profiling used in practice. The working definition of risk profiling in the law enforcement sector is also not set in stone, it is simply a means to understand which phenomenon I am talking about. The different applications of risk profiling show that there are different goals to the applications, some aiming at multiple goals at the same time, such as maintaining order in areas and deterrence of crime; managing resources; preventing reoffending, which can both be seen as preventing crime but also as rehabilitation; and determining sentencing as determining retribution, and restitution.

In this chapter of the dissertation, key concepts were explained and examples of risk profiling were given that return later throughout the dissertation. The different challenges that different aspects of risk profiling create will be discussed in chapter 3. Chapters 4 to 6 discuss the regulatory frameworks of data protection law, non-discrimination law, and criminal procedural law. In the concluding chapter, I reflect back on the concepts of chapter 2, to give a more critical analysis of the regulation of risk profiling after having discussed the relevant laws.

Chapter 3

The challenges of risk profiling by law enforcement actors

3.1 Introduction

Risk profiling definitely has an appeal in improving law enforcement practices, especially when it comes to efficiency. Some scholars see the practice of risk profiling or the increasing use of Big Data and algorithms in various scenarios as boosting not only efficiency but also accuracy or neutrality of decision-making.[312] Data-driven analysis and the use of algorithms were presented as an objective solution to bias in human decision-making and policy.[313] There is certainly something to be said, especially in the context of justice and fundamental rights, for creating a system that is not only more efficient but also less biased and more accurate, which would be favourable to those individuals subjected to such systems. However, while it seems likely there is potential for data-driven practices in the law enforcement sector such as risk profiling, it does not mean it is without its challenges and that there can be no criticism towards such developments. Since this research is focused on fundamental rights, a critical approach is especially important, for it allows to see beyond the promises of risk profiling to the actual impact on fundamental rights. Therefore, this chapter functions as a counterpart to the more techno optimism-oriented position, for example as displayed by proponents[314] found in computer science, technology vendors and policymakers, and discusses the challenges that risk profiling in the law enforcement context poses.

An example to critically reflect on the idea of algorithms and data-driven processes bringing objectivity is the introduction of the COMPAS system. COMPAS was introduced under the guise of improved neutrality or decreased bias in decision-making, compared

---

312 Zouave and Marquenie acknowledge that there are advantages in terms of creating more efficient policing, E.T. Zouave & T. Marquenie, An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling, *2017 European Intelligence and Security Informatics Conference*; There are other authors as well writing about Big Data and increased use of algorithms and their benefits (such as Domingos, P. (2015). *The master algorithm: How the quest for the ultimate learning machine will remake our world*. Basic Books; K. Cukier & V. Mayer-Schönberger, The Rise of Big Data: How It's Changing the Way We Think About the World, *Foreign Affairs*, Vol. 92, No. 3 (2013) and specifically for governments: B. Lepri, N. Oliver, E. Letouz, A. Pentland, P. Vinck. Fair, Transparent, and Accountable Algorithmic Decision-making Processes The Premise, the Proposed Solutions, and the Open Challenges. *Philos. Technol*. (2018) 31:611 –627. DOI 10.1007/s13347-017-0279-x.

313 See for example: B. Lepri, N. Oliver, E. Letouz, A. Pentland, P. Vinck. Fair, Transparent, and Accountable Algorithmic Decision-making Processes The Premise, the Proposed Solutions, and the Open Challenges. *Philos. Technol*. (2018) 31:611 –627. DOI 10.1007/s13347-017-0279-x; Shapiro, A. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17(3/4): 456-472. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487.

314 For their position see for example the analysis by Shapiro, A. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17(3/4): 456-472. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487.

to human decision makers and automated, data-driven, decision-making.[315] Research conducted into the COMPAS tool later revealed that the system was in fact not less biased at all, but exacerbated bias against black defendants versus white defendants.[316] So while the tool could have enhanced accuracy in risk assessment and predictions and decreased bias, those aims failed, unforeseen by its law enforcement users, and the tool possibly worsened the situation compared to a scenario with human decision makers. There are many other examples of data-driven or algorithmic decision-making failing to deliver on those promises.[317]

In chapter 2, I defined the concept of risk profiling and I described the practices of risk profiling. Chapter 3 operationalizes these concepts and uses these illustrations to create a bridge to the legal analysis of chapters 4 to 6. The aim of this chapter is to present an overview of all the relevant challenges posed by risk profiling conducted by national law enforcement actors. These challenges are taken from the perspective of individuals and groups impacted by risk profiling in the application of risk profiles, but also include challenges that already arise before the application or use of profiles. Contrary, other perspectives would be for example from the perspective of the law enforcement actors themselves, or the regulator, or supervisory authorities. I approach risk profiling from the perspective of what the challenges are for those who the profiles pertain to, to be able to connect the challenges to the fundamental rights discussions of chapters 4 to 6. The fundamental rights to data protection, non-discrimination, privacy and due process all have some role to play in providing safeguards and protection of the interests of those subjected to risk profiling. This perspective limits the scope of the research by excluding challenges that are purely of a technical, organizational or financial nature and are not relevant for the fundamental rights perspective, such as challenges in budgeting for law enforcement or staff training. Obviously, challenges to fundamental rights of people subjected to the systems can simultaneously also be challenges to law enforcement, such as making sure categorizations are accurate, and use of the tools is non-discriminatory.

The challenges in this chapter are not necessarily an exhaustive overview; new ones can always be added. Rather the analysis reflects on challenges as discussed in bodies of literature concerning (governmental) profiling, automated decision-making and data-driven decision-making, predictive policing, and data-driven sentencing, and

---

315 Practitioner's Guide to COMPAS Core, available at: https://www.equivant.com/wp-content/uploads/Practitioners-Guide-to-COMPAS-Core-040419.pdf.

316 J. Angwin, J. Larson, S. Mattu, L. Kirchner, "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks," ProPublica, 23 May 2016; www.propublica.org/article/machine-bias-risk-assessmentsin-criminal-sentencing.

317 O'neil, C. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Broadway Books, 2016.

groups these challenges into main categories based on commonalities. The challenges discussed need to be seen in the light of the following chapters of this dissertation, which explore how risk profiling in the law enforcement context impacts fundamental rights of those subjected to such processes and to what extent the legal framework mitigates or addresses this impact. Therefore, the challenges discussed in this chapter are limited in scope, being the challenges with the biggest impact on fundamental rights.

The chapter relies on literature studies. Therefore it is important from a methodological point of view to briefly explain that process here. A good start was to look at which challenges are predominantly discussed in literature pertaining to practices similar to risk profiling. Since risk profiling by law enforcement actors is still a relative niche activity, literature pertaining to adjacent practices, such as data-driven policy and decision-making, and literature of components of risk profiling such as data mining, predictive analysis and algorithmic decision-making was used. In addition there is of course plenty of literature on profiling as such, outside of the context of law enforcement or of risk assessment purposes. From the literature studies it became apparent that many challenges are discussed by multiple scholars, but often under slightly different headings or in slightly different contexts. In addition, when discussing different challenges, most authors do not propose a methodology for why they chose to discuss those specific challenges. These points pose difficulties when trying to structure or classify the different discussions. Nonetheless one can distinguish in the literature common themes of bias[318], discrimination (for example in reinforcing stereotypes or exacerbating existing disadvantages)[319], transparency

[318] B. Lepri, N. Oliver, E. Letouz, A. Pentland, P. Vinck. Fair, Transparent, and Accountable Algorithmic Decision-making Processes The Premise, the Proposed Solutions, and the Open Challenges. *Philos. Technol*. (2018) 31:611 –627. DOI 10.1007/s13347-017-0279-x; Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554; Barocas, S., and A.D. Selbst. "Big data's disparate impact." *Calif. L. Rev.* 104 (2016): 671; O'neil, C. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Broadway Books, 2016.

[319] P. Allo, The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020; A. Vedder, "KDD: The challenge to individualism." *Ethics and Information Technology* 1, no. 4 (1999): 275-281; B. Lepri, N. Oliver, E. Letouz, A. Pentland, P. Vinck. Fair, Transparent, and Accountable Algorithmic Decision-making Processes The Premise, the Proposed Solutions, and the Open Challenges. *Philos. Technol*. (2018) 31:611 –627. DOI 10.1007/s13347-017-0279-x; Barocas, S., and A.D. Selbst. "Big data's disparate impact." *Calif. L. Rev*. 104 (2016): 671; Schermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 46.

or information asymmetries[320], privacy[321], de-individualization or effects of non-distributive groups[322] and inaccuracies.[323]

When it comes to literature discussing profiling, the most longstanding and extensive discourse is that on privacy.[324] While obviously there are still concerns over the impact on privacy, it is important to go beyond this privacy-focused discussion.[325] Therefore, this chapter also focuses on other fundamental rights at stake besides privacy and data protection, especially tailoring them to the criminal justice sector.

While the scholars in the debate described above list or discuss several challenges, Zarsky goes further and offers a methodology or structure to selecting the most important challenges. Zarsky proposes a taxonomy for what could be described as the different challenges of algorithmic decision-making.[326] In his taxonomy the main grounds for

---

320 Schermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 46; A. Vedder, "KDD: The challenge to individualism." *Ethics and Information Technology* 1, no. 4 (1999): 275-281; P. Allo, The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020; Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554; B. Lepri, N. Oliver, E. Letouz, A. Pentland, P. Vinck. Fair, Transparent, and Accountable Algorithmic Decision-making Processes The Premise, the Proposed Solutions, and the Open Challenges. *Philos. Technol.* (2018) 31:611 –627. DOI 10.1007/s13347-017-0279-x; Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms." Big Data & Society 3, no. 1 (2016): 2053951715622512.

321 B. Lepri, N. Oliver, E. Letouz, A. Pentland, P. Vinck. Fair, Transparent, and Accountable Algorithmic Decision-making Processes The Premise, the Proposed Solutions, and the Open Challenges. *Philos. Technol*. (2018) 31:611 –627. DOI 10.1007/s13347-017-0279-x; Zarsky, Understanding Discrimination in the Scored Society, *Washington Law Review*, Vol. 89:1375, 2014; Schermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 45.; Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554; A. Vedder, "KDD: The challenge to individualism." *Ethics and Information Technology* 1, no. 4 (1999): 275-281; P. Allo, The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020.

322 Schermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 46; A. Vedder, "KDD: The challenge to individualism." *Ethics and Information Technology* 1, no. 4 (1999): 275-281; P. Allo, The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020.

323 Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554.

324 Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554; Omer Tene and Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239 (2013).

325 Schermer, B. (2011). The limits of privacy in automated profiling and data mining. Computer Law and Security Review, 27, p. 46; A. Vedder, "KDD: The challenge to individualism." Ethics and Information Technology 1, no. 4 (1999): 275-281.

326 Zarsky T (2016) The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision-making. Science, Technology and Human Values 41(1): 118–132.

challenges are opacity and automation. The challenges stemming from opacity occur, for example, because the processes are inherently opaque or because there are laws or rules creating opacity to the outside world. Challenges with automation occur when limited human input presents issues. Zarsky further splits the challenges in those relating to either efficiency, for example having to do with predictions or inaccurate data, and challenges of fairness, such as unfair wealth transfers or a lack of autonomy.[327] The taxonomy that Zarsky proposes is very insightful, demonstrating opacity and automation to be at the root of the problem, but his taxonomy is not tailored to the law enforcement domain. The taxonomy centers heavily on wealth distribution, consumers, and consent, which are aspects that are not relevant for profiling by law enforcement actors. Also, Zarsky's taxonomy can be seen as too shallow, not further specifying the problems in predictive analytics and problems of bias and discrimination discussed in other literature. Nonetheless, Zarsky's taxonomy is useful as a starting point to see at least that opacity and automation are major issues in automated decision-making and each create their own difficulties. In addition, it shows that many issues relate to efficiency, which focus more on the process, and that many other issues relate in some way to fairness, focusing more on the impact of subjecting people to profiling.

Another useful illustration of the process of risk profiling and its challenges can be found in the traditional model of a governance loop.[328] For a process, such as introducing a new profiling system, this governance loop consists of the four stages: collection, processing, utilization and feedback, and learning.[329] A major factor underlying both Zarsky's taxonomy and the feedback loop is the interaction between humans and machines, specifically algorithms. With the rise of Big Data there is a heavy reliance on algorithms to make sense of the information overload. The algorithms sort, mine, parse and configure information.[330] This is combined with a growing willingness to outsource decision-making authority to

---

327 Zarsky T (2016) The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision-making. *Science, Technology and Human Values* 41(1): 118–132; 'Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554' implicitly follow the division into opaqueness and automation in their mapping of the challenges-.

328 Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Wash. L. Rev.*, 89, 1; Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.; T. Zarsky, Transparent Predictions, *University of Illinois Law Review* (2013) 4; Taylor, L., Leenes, R., & van Schendel, S. (2017). *Public sector data ethics: From principles to practice*. Tilburg: Tilburg University.

329 Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554.

330 Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554, p. 2.

machines or AI.[331] Shifting formerly human decision-making to machine decision-making raises questions concerning the relation between the tasks and judgments of humans versus machines and of human decision makers in combination with machines. That is why the shifting relation between humans and machines forms the starting point of most challenges in risk profiling. In a way this also creates opacity, another prominent source of challenges. But opacity can also come from, as described above, law, which is a prominent source of opacity in the law enforcement sector through legislation safeguarding public security and the interest of the criminal investigation.

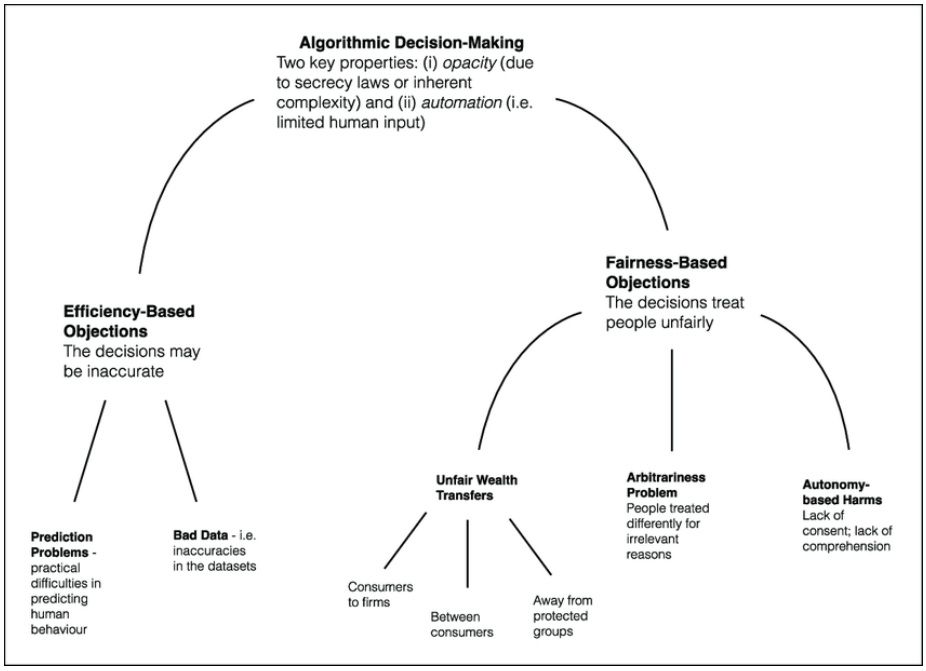

Figure 3. Zarsky's taxonomy.[328]

The challenges in this chapter are presented roughly in order of the steps of the profiling process described in chapter 2, starting with the data or input, moving to the workings of the system, and ending with the use of profiles or the outcomes of the process. This sort of chronological outline allows for a rough grouping of the challenges along those three parts of the profiling process (data collection/input, analysis by the system, outcomes/use) and offers a structure to the discussion. Taking all these insights from

[331] In outlining a research agenda for concerns in governing algorithms, Danaher et al. also state that figuring out how humans are involved in different stages of the process is the key factor in normative questions revolving around AI.

the literature into account, I have grouped the challenges as follows. This chapter will start with an exploration of fairness as a base of many issues. As will be explained in section 3.2, it is not discussed as a challenge of its own, besides the other challenges, but rather as an umbrella challenge that encompasses more specific challenges. Next, bias and errors due to the use of probabilities will be discussed. Within the process of profiling, they pertain more to the start of the risk profiling process. Then opacity will be assessed, which typically involves the obscurity of the middle phase of risk profiling – how the profiling is done; it plays a role in several parts of the risk profiling process, and also has a significant impact on the outcome of the process. Then we move fully to the outcome phase in discussing non-discrimination, privacy, and due process rights. Privacy is discussed mainly in terms of concerns of using non-personal information and group data, as well as autonomy and self-determination concerns; the focus is on those topics as they are key to risk profiling and underexplored compared to for EXAMPLE the collection of personal data. Due process is paramount to the use of risk profiling in the law enforcement context -as displayed in the COMPAS case- since profiling in the law enforcement context deals with people's ability to legally defend themselves and with criminal investigations and trials. In the conclusion of this chapter the challenges will be put into perspective, demonstrating how they relate to one another and how we can view them within the risk profiling process.

3.2. Fairness

One of the concepts that comes to the fore most often in discussions on elements of AI, risk profiling, such as automated decision-making, the use of algorithms, and risk assessment, is fairness.[332] Questions are raised whether these new technologies and

[332] See for example: X. Ferrer, T. v. Nuenen, J. M. Such, M. Coté and N. Criado, "Bias and Discrimination in AI: A Cross-Disciplinary Perspective," in *IEEE Technology and Society Magazine*, vol. 40, no. 2, pp. 72-80, June 2021, doi: 10.1109/MTS.2021.3056293; Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567; Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719895805; Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, 45(5), 494–511. https://doi.org/10.1177/0967010614544204; Žliobaitė, I. Measuring discrimination in algorithmic decision-making. *Data Min Knowl Disc* 31, 1060–1089 (2017). https://doi.org/10.1007/s10618-017-0506-1; R. Binns, Fairness in Machine Learning: Lessons from Political Philosophy, Proceedings of Machine Learning Research 81:1-11, 2018, Conference on Fairness, Accountability, and Transparency 2018; Laurens Naudts, 'How Machine Learning Generates Unfair Inequalities and How Data Protection Instruments May Help in Mitigating Them', in: *Ronald Leenes and others (eds) in, Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2019) ch 3.

tools themselves are fair and whether it is fair to use technologies or automation versus purely human decision-making. However, fairness remains a vague term. Everyone can imagine to some extent what is meant with fair, but authors who use the term fairness usually do not explain what they exactly see as fair. Rather this meaning of fairness can only be derived from the context when authors mention fairness in connection with other terms such as non-discriminatory, bias-free, equal in distribution and so on. This section aims to shed some more light on the meaning of fairness, in the context of the use of risk profiling in the law enforcement domain. Since fairness is such an generic concept, it makes little sense to view it as a challenge in itself besides other challenges. More so, fairness is an underlying issue or concern that ties in to many of the challenges discussed in this chapter.

In the discourse on machine learning, researchers pay increasing attention to fairness in machine learning and consequential decision-making. Fairness is mentioned together with discrimination and bias, framing fairness as a concept in relation to the goal of equal treatment. Binns, for example, discusses systems that reach unfair outcomes, and connects unfairness to systematic bias in the system, reflection or exacerbation of existing discrimination, stating that systems reach unfair outcomes because of these bias and discrimination issues.[333] Also Wachter et al., in their seminal work on AI, automation and non-discrimination law, seem to equate fairness with non-discrimination.[334]

Due to automated systems possibly producing unfair outcomes, a research paradigm of discrimination-aware data mining and fair machine learning has emerged, which attempts to detect and mitigate unfairness.[335] The fair machine-learning community develops machine-learning based systems focused on social and legal outcomes such as fairness, justice, and due process, by using computer science concepts to define notions of fairness and discrimination and to produce fairness-aware learning

---

333 R. Binns, Fairness in Machine Learning: Lessons from Political Philosophy, Proceedings of Machine Learning Research 81:1-11, 2018, Conference on Fairness, Accountability, and Transparency 2018.

334 S. Wachter, B. Mittelstadt, and C. Russell, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI (March 3, 2020). Available at SSRN: https://ssrn.com/abstract=3547922 or http://dx.doi.org/10.2139/ssrn.3547922. For more on their examination of the principle of non-discrimination, see chapter 5.

335 R. Binns, Fairness in Machine Learning: Lessons from Political Philosophy, Proceedings of Machine Learning Research 81:1-11, 2018, Conference on Fairness, Accountability, and Transparency 2018; A. Selbst et al., 2019. Fairness and Abstraction in Sociotechnical Systems. In FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19), January 29–31, 2019, Atlanta, GA, USA. ACM, New York, NY, USA. https://doi.org/10.1145/3287560.3287598.

algorithms.[336] This orientation of the machine learning community heavily correlates fairness to non-discrimination, but also to justice and due process. While it is generally seen as an admirable goal to produce fair algorithms or deliver fair machine learning, some scholars question the ability of technological components such as algorithms and machine learning to create a fair situation, especially taking into account the societal context that decision-making systems operate in.[337] This seems reasonable from a social scientist perspective: whether a risk profiling system is fair cannot be judged simply by, for example, the fairness of a code or input data, but needs to be assessed based on the system as a whole, including its use. Therefore, it is useful to look at the use of the term fairness outside of this machine learning paradigm and also look at the meaning of fairness in social sciences.

In the legal paradigm, the term fairness plays a role in different fields of law, for example in data protection law, competition law and consumer law. Graef et al. propose that fairness can be seen as an overarching principle in all of these three fields of law pertaining to the protection of choice.[338] In the legal discipline the term fairness can be correlated to non-discrimination, but also to open terms such as 'just' and 'reasonable', meaning that fairness can have a different interpretation in different legal regimes.[339] In consumer law, for example, fairness makes for a substantive standard, under the Unfair Terms Directive and the Unfair Commercial Practices Directive, against which the legality of contracts and practices is tested. Fairness in consumer protection focuses mainly on the decision-making capacity of consumers.[340] In competition law the role of fairness is less clear, fairness here can be seen as an inherent objective or an outcome of competition enforcement.[341] The concept of fairness under data protection is the most interesting of the three fields of law mentioned above, given the scope of this dissertation.

---

336 A. Selbst et al., 2019. Fairness and Abstraction in Sociotechnical Systems. In FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19), January 29–31, 2019, Atlanta, GA, USA. ACM, New York, NY, USA. https://doi.org/10.1145/3287560.3287598.

337 A. Selbst et al., 2019. Fairness and Abstraction in Sociotechnical Systems. In FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19), January 29–31, 2019, Atlanta, GA, USA. ACM, New York, NY, USA. https://doi.org/10.1145/3287560.3287598, p. 59.

338 I. Graef, D. Clifford and P. Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, 2018, Vol. 8, No. 3, p. 203.

339 I. Graef, D. Clifford and P. Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, 2018, Vol. 8, No. 3, p. 203.

340 I. Graef, D. Clifford and P. Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, 2018, Vol. 8, No. 3, p. 204.

341 I. Graef, D. Clifford and P. Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, 2018, Vol. 8, No. 3, p. 205.

In data protection law we can distinguish between procedural fairness and fair balancing.[342] Procedural fairness has to do with transparency, timeliness and burden of care in terms of obligations. Fair balancing focuses on proportionality and necessity.[343] Similar to the scholarship of computer scientists, the concept of fairness is seen as a key concept under data protection legislation but at the same time the exact role of fairness remains elusive.[344] Clifford and Ausloos published an extensive paper on the role of fairness in the data protection framework, discussing fairness as "*an overarching objective aligned with the purpose of the framework as a whole, thus targeting the re-balancing of the asymmetric data subject–controller relationship*."[345] In their description of the role of fairness within data protection over the years, Clifford and Ausloos outline that fairness originated from the collection of data, specifically the aim that this should happen with the knowledge or consent of the data subject, thus centering on the overlap between fairness and transparency.[346] Also for later data protection instruments using the fairness principle, Clifford and Ausloos link fairness to transparency focusing on consent, information rights and information asymmetries.[347]

Since consent is not relevant for the law enforcement context, as will be explained in chapter 4, the question arises how fairness can be viewed in that sector if not in terms on choice. Where fairness under the GDPR -the instrument that applies to data protection in the private sector- is focused on which information is provided to data subjects about the collection of their data and fair processing in other regards, fairness in the law enforcement context, such as under the LED, is arguably more about information asymmetries with regard to checks and balances and power abuse. The question in the law enforcement context is not so much whether it is fair to collect or process data without providing the data subject with information, but more so whether it is fair to use certain data for a certain purpose, or whether it is fair to

342 I. Graef, D. Clifford and P. Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, 2018, Vol. 8, No. 3, p. 203; D. Clifford & J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), pp. 130–187, doi:10.1093/yel/yey004.

343 I. Graef, D. Clifford and P. Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, 2018, Vol. 8, No. 3, p. 203; D. Clifford & J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), pp. 130–187, doi:10.1093/yel/yey004.

344 D. Clifford & J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), pp. 130–187, doi:10.1093/yel/yey004.

345 D. Clifford & J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), pp. 130–187, doi:10.1093/yel/yey004.

346 D. Clifford & J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), p. 139.

347 D. Clifford & J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), pp. 130–187, doi:10.1093/yel/yey004.

offer or not offer safeguards accompanying the collection and use of data. This idea of fairness is reflected well in Bygrave's description of the concept of fairness. Bygrave describes fairness as taking into account interests and reasonable expectations of data subjects so that the collection and further processing of personal data is carried out in a manner that in context does not intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity.[348] This concept of fairness requires balancing and proportionality in processing of data in the situation at hand but also in the way in which information systems are designed and structured.[349] Bygrave's explanation of fairness highlights that reasonableness is important: law enforcement actors need to process data in a proportional manner and to an extent that is required by necessity. Balance is provided by safeguards accompanying law enforcement powers that secure a fair balancing between interests such as due process or non-discrimination for a suspect but also security and safety for others. In that sense fairness is an interest that underlies all use of power, and as Bygrave justly remarks, is not just about individual data processing but equally about information systems and processes themselves. This discussion demonstrates that fairness remains elusive. I would conclude that it at least pertains to a form of equal treatment, or non-discrimination or objectivity on the one hand, and to procedural justice and safeguards pertaining to (a)symmetries between those using the system and those subjected to the system on the other hand.

Following the discussion on the concept of fairness, the next question is how fairness is relevant to risk profiling. Going back to Zarsky's taxonomy of issues with algorithmic decision-making, a discussion point is how fairness relates to efficiency in algorithmic decision-making and profiling. More specifically, whether efficiency and fairness should be seen as a dichotomy or not.[350] One of the main proposed advantages of the use of techniques such as risk profiling is efficiency, as information can be distilled, categorized and compared quickly and in large quantities. When one keeps in mind the goals of risk profiling systems, such as efficiency, accuracy and objectivity, it could be assumed that at least accuracy and objectivity go hand in hand with fairness. However, this might not always be the reality. Several authors discuss a compromise

348 Bygrave, L.A, "Core principles of data protection" (2001) 7(9) *Privacy Law and Policy Reporter* 169.

349 Bygrave, L.A, "Core principles of data protection" (2001) 7(9) *Privacy Law and Policy Reporter* 169.

350 Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554, p. 18.

between accuracy and fairness in law enforcement.[351] Think for example of predictive policing, in which the system directs police patrols to areas that are labelled as highest risk, which can be seen as efficient. However, arguably, it would be fairer to send officers to other areas with less information about the risk level available, to gain more knowledge about such areas that are not a priority (yet) and to equally distribute patrols.[352] Some propose that fairness-aware algorithms take into account that outcomes do not disproportionately impact members of a protected class or already disadvantaged societal groups, but in doing so can compromise predictive accuracy by aiming to shelter certain categories of data.[353] Another possible conflict concerning fairness is a dichotomy between different targets of fairness. There can for example be tensions in aiming to achieve both group fairness and individual fairness, where group fairness focuses more on members of different protected groups and individual fairness provides that people who are 'similar' with respect to the classification task receive similar outcomes.[354] This means that when discussing fairness of risk profiling, a starting question should be: for whom are we discussing fairness? Should a system be fair to groups or between groups, should it be fair at the individual level, or should we strive for as much fairness as possible on all accounts? De Hert and Lammerant classify those impacted by profiles into three groups: 1) individuals or groups whose data are used to create the profile; 2) individuals or groups to whom the profile is applied; and 3) individuals or groups who are subject to a decision based on the profile.[355] This distinction makes clear that those whose data is used to create the profile and those to whom the profile is applied do not always have to overlap; I think this distinction made by De Hert and Lammerant illustrates that when discussing fairness of profiling,

---

351 Friedler, S. A., C. Scheidegger, S. Venkatasubramanian, S. Choudhary, E. P. Hamilton, and Derek Roth. 2018. A Comparative Study of Fairness-Enhancing Interventions in Machine Learning. FAT*19 Proceedings of the Conference on Fairness, Accountability and Transparency, 329-338. Atlanta, GA. January 29-31, 2018. http://arxiv.org/abs/1802.04422; Z. Muhammad Bilal, I. Valera, M. Gomez Rodriguez, and K. P. Gummadi. 2017. Fairness Constraints: Mechanisms for Fair Classification, v5. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Fort Lauderdale, FL. http://arxiv.org/abs/1507.05259; Shapiro, A. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17(3/4): 456-472. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487.

352 Shapiro, A. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17(3/4): 456-472. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487.

353 Shapiro, A. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17(3/4): 456-472. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487.

354 Binns, R. (2020, January). On the apparent conflict between individual and group fairness. In Proceedings of the 2020 conference on fairness, accountability, and transparency (pp. 514-524).

355 De Hert P., & H. Lammerant, 'Predictive profiling and its legal limits: effectiveness gone forever?', in: B. van der Sloot, D. Broeders & E. Schrijvers (eds.), *Exploring the Boundaries of Big Data*, The Hague: WRR 2016, p. 147.

it should be made clear in the specific context of the discussion which of these groups are the intended subject of that fairness.

It is clear that fairness is a point of concern in systems such as risk profiling. The question is, however, how fairness can be achieved or how to identify when exactly fairness becomes an issue. As seen above, fairness is not clear-cut and can conflict with other values or even dimensions of fairness itself. Whether viewed from a legal perspective such as in data protection legislation, or whether viewed from a machine learning perspective, it is also clear that fairness cannot be seen as a separate goal or requirement in itself;[356] it is too closely intertwined with other, more specific values and concerns. For the rest of this chapter, fairness will therefore be used as an overarching principle and an underlying value.

3.3 Bias in data

Two terms that are often used together in the context of AI or automation are bias and discrimination. While the two can go hand in hand, bias and discrimination are not the same. The difference is mainly in actions and legal protection. While bias implies that a prejudice exists to one outcome over the other, this does not mean necessarily that unjust treatment will follow, or that this prejudice is acted upon. Discrimination explicitly requires an action such as unfair or unequal treatment, whether intentionally or not. Moreover, bias covers more types of prejudice than are traditionally understood under discrimination in the legal sense; for example, an algorithm could be biased towards favoring people who drive a red car over people who drive a blue car. Discrimination is mostly used to refer to unjust treatment based on grounds mentioned in law such as sex, race, language, religion, political opinion, or national origin. A system can be biased towards a certain outcome instead of towards people, in a way that does not directly require differential treatment, such as an automated sentencing system being biased towards stricter sentencing, compared to non-automated sentencing, for all individuals and groups subjected to the system equally.

Data are the fuel or ingredients for risk profiling. However, data are not always as factual as they might appear. A point of concern that is often put forward in discourse

[356] D. Clifford & J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), p. 159.

on automation, Big Data, profiling, and predictive policing, is that of bias in data.[357] Bias in this context could be described as an inclination or prejudice that does not (completely) reflect an objective state of affairs but that plays a role through choices made by humans in the process, usually not consciously. Bias could for example be present in the training data, in the collected data for analysis, in selecting the input data and in inferring new data.[358] Since data are usually the start of the process and only one of the components, these choices echo throughout the process and the outcomes. In addition, bias is not only an issue in the data itself, but also in the rules, training input, hypotheses or assumptions introduced by the human designing the algorithm, thus affecting the entire process and manifesting itself in a machine learning system itself.[359] Choices are made in all aspects of a process. However, in this section I focus mostly on the data itself, as it is the starting point of the process and it would be repetitive to describe the same issue for choices later in the process.

Risk profiling relies to a large extent on policing strategies. Predictive policing applications suffer from their own bias, as there are all kinds of restraints to crime data, as will be explained in this section: data can be limited, incomplete, inaccurate, or biased due to discriminatory policing practices that reinforce disparate treatments for

---

357 For example: P. Vogiatzoglou, Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity, *European Journal of Law and Technology*, Vol 10, Issue 1, 2019; Friedman, B and Nissenbaum, H (1996) 'Bias in Computer Systems', *ACM Transactions on Information Systems* 14(3), p. 330-347; Kitchin, R (2013) 'Big Data and human geography: Opportunities, challenges and risks', *Dialogues in Human Geography*, 3(3), p. 262-267; Mittelstadt, BD, Allo, P, Taddeo, M, Wachter, S and Floridi, L (2016) 'The ethics of algorithms: Mapping the debate', *Big Data Society*, July-December, p. 1-21.

358 See for example Bennet Moses, L and Chan, J (2014) 'Using Big Data For Legal and Law Enforcement Decisions: Testing The New Tools', *University of New South Wales Law Journal* 37(2), p. 648; van Brakel, R (2016) Pre-Emptive Big Data Surveillance and its (Dis)Empowering consequences: The case of Predictive Policing in: *van der Sloot, B, Broeders, D and Schrijvers, E (ed) Exploring the Boundaries of Big Data* (Amsterdam University Press).

359 P. Vogiatzoglou, Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity, *European Journal of Law and Technology*, Vol 10, Issue 1, 2019; L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

already marginalized communities.[360] An important point to keep in mind concerning the use of any law enforcement data is that these data are limited. Law enforcement data can be influenced by underreporting of crimes or by a focus of law enforcement actors on certain crimes or groups over others; in that sense crime data are not real time data of actual crime, they simply reflect the rate of crime that was caught or reported and recorded.[361] Looking for example at crime rate measurements, this type of data requires the actual uncovering of crime taking place, proper classification, and recording, making official crime data the end result of many processes.[362] The data are limited due to what individuals choose to report and what law enforcement officers record. This gap between actual crime and the recorded crime is not random but rather systemic and differing per type of crime and victim.[363] This means for example that victims who do not report crimes as regularly as other groups are not included in the data and can be marginalized and ignored by law enforcement, and that recorded data can sometimes be categorized inaccurately or inconsistently.[364] Whether an act constitutes a crime, how the crime is classified, what threshold there is for recording it, and so forth, are all to a certain extent up to human discretion, which causes big variations in the data.[365]

---

360 Shapiro, A. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17(3/4): 456-472. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487; see for example also: Brayne, S., A. Rosenblat, and D. Boyd. "Predictive Policing". Data & Civil Rights: a new era of policing and justice. October 27, 2015. https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf; Ensign, D., S.A. Friedler, S. Neville, C. Scheidegger, and S. Venkatasubramanian. 2017. Runaway Feedback Loops in Predictive Policing. Paper prepared for the first conference on Fairness, Accountability, and Transparency in Machine Learning, New York University, New York, February 2018. http://arxiv.org/abs/1706.09847; Jefferson, BJ. 2017. Digitize and Punish: Computerized Crime Mapping and Racialized Carceral Power in Chicago. Environment and Planning D: Society and Space 35 (5): 775–96; Lum, K., and William, I. 2016. To Predict and Serve? *Significance* 13 (5): 14–19.

361 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366

362 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, Vol. 26:287

363 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

364 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

365 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

Not only is crime data the result of reporting and processing, the act of policing itself also influences the data.[366] The police generate the data they rely upon, for example through the observing of specific crime, acting upon those crimes, collected, categorizing and recording the data related to it, while there are certainly also crimes that will go unnoticed or are not properly classified, distorting the data.[367] Racial bias is an often discussed type of bias when it comes to policing, but is not the only bias. [368] Policing is in a way a social (classification) process: police officers take action or refuse to act (for example by choosing not to investigate a report due to lack in evidence), thus every decision in policing is also a decision about whether crime data are generated.[369] This effect is especially visible in predictive policing that targets locations. Based on predictive policing algorithms, officers are sent to a specific area. The increased presence of police in that area might increase the recording of crimes there. This in turn can for example create the illusion or assumption that actual crime in that area is increasing, while it is rather the recording of that crime that increases. Or it can perpetuate a bias in the model by assuming there is crime in that area and then increasingly record crime there. Facts can become self-perpetuating: what might seem to be an objective process can become a means of perpetuating historic discrimination or bias.[370] To give a practical example: the American predictive location-based policing software, PredPol, relies heavily on historical crime data, such as previous arrests.[371] If a significant number of previous arrests in a location were (partly) racially motivated, the prediction builds on this and as the increased police presence in an area will lead to more arrests and thus crime records, more biased data will be fed back to the algorithm. When those new data are used for predictions, those predictions are therefore not bias-free but bias-reinforcing.[372]

---

366 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695; Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California law review*, 671-732.

367 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, Vol. 26:287; see also L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695; Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California law review*, 671-732.

368 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

369 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

370 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

371 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366

372 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366

Aside from predictions, another instance where bias in data is especially problematic is in the stage of training algorithms and models. Training of algorithms requires a translation in the data from the criminal justice perspective to the computer science perspective, because computing systems require a formalised machine-readable task. For this task, performance metrics are required, as well as design choices, such as pertaining to the type of training experience, the target function to be learned, and a representation for this target function.[373] There can also be bias in the distribution of training data and future data, as there is an assumption that the distribution of training examples is identical to the distribution of test samples collected later; this might hold true from a theoretical perspective, but need not be valid in practical reality.[374] Again, like other issues of bias, the problem is in the assumptions and choices made by humans,[375] which becomes problematic when bias in these assumptions and choices is hidden in automated systems.

A clear example of bias in practice, specifically in predictions, can be found in the controversy surrounding the COMPAS software. COMPAS uses 137 data points. Race is not directly one of the data points or factors used in the risk prediction,[376] but an extensive study into the system in 2016 conducted by ProPublica demonstrated that nonetheless there can be racial disparities in the predictions.[377] Apparently, COMPAS scores favor white defendants over black defendants, as the impact of errors in COMPAS affected black and white defendants differently by erroneously predicting the recidivism rate for black defendants disproportionately higher than for white defendants.[378] This conclusion, that COMPAS favors white defendants over black defendants, naturally caused much uproar in the USA scholarly debates. Some scholars posed a perspective countering the ProPublica research. Kleinberg et al. in their paper describe how later analyses conducted by others raised methodological objections to the report and that despite COMPAS's errors, its estimates of the probability of

373 Hildebrandt, Mireille. "Data-driven prediction of judgment. Law's new mode of existence?." *Draft Chapter for OUP Collected Courses Volume EUI 2019 Summerschool* (2019).

374 Hildebrandt, M. "Data-driven prediction of judgment. Law's new mode of existence?." *Draft Chapter for OUP Collected Courses Volume EUI 2019 Summerschool* (2019).

375 Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

376 For an explanation of how COMPAS works, please refer back to chapter 2, section 2.5.2.3.

377 J. Angwin, J. Larson, S. Mattu, L. Kirchner, "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks," ProPublica, 23 May 2016; www.propublica.org/article/machine-bias-risk-assessmentsin-criminal-sentencing.

378 J. Dressel and H. Farid, The accuracy, fairness, and limits of predicting recidivism, *Science Advances* 2018;4: eaao5580 17 January 2018; J. Angwin, J. Larson, S. Mattu, L. Kirchner, "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks," ProPublica, 23 May 2016; www.propublica.org/article/machine-bias-risk-assessmentsin-criminal-sentencing.

recidivism are equally well calibrated to the true outcomes for both black and white defendants.[379] Flores et al. published a very critical response to the ProPublica report proposing that bias can also originate from the justice system itself (including economic factors, policing patterns, prosecutorial behaviour, and judicial biases), and that risk assessment tools informed by objective data can help reduce institutional racial bias from its current level.[380] Of course this discussion pertains to more risk assessment software, not just to COMPAS. For example, a different study showed that while COMPAS makes use of 137 data points, the same accuracy was achieved with relying on non-experts to conduct the assessment, using only 7 features and using a simple standard linear predictor.[381]

Such empirical studies raise awareness of the (non)reliability of automated risk assessment systems in criminal justice in general. I argue that it is problematic to assume, regardless of the actual numbers of COMPAS, that a risk assessment tool in itself is more objective or less biased than human decision makers and law enforcement actors, given the issues with bias discussed above. Flores et al. seem to assume that if the criminal justice system itself is biased, automation can make it more objective. However, it seems more likely that the opposite would be true and the large-scale automated system will exacerbate current issues, since it cannot break free from the bias in data and choices underlying the system. In any case it is dangerous to assume that substituting current practices with algorithmic techniques creates empirical neutrality and infallibility.[382] Algorithms that have as a basis biased data or are produced by biased institutions still function on that bias[383], making it difficult in practice to reduce that bias through automation.

There have been scholarly discussions about whether or not the use of sensitive types of data leads to bias or discrimination. The use of sensitive information can be indirect or hidden. A perfect example of this is masking: with the help of data mining, trivial

---

379 Kleinberg, J., Mullainathan, S., & Raghavan, M. (2016). Inherent trade-offs in the fair determination of risk scores. arXiv preprint arXiv:1609.05807.

380 A.W. Flores; K. Bechtel; C. T. Lowenkamp, "False Positives, False Negatives, and False Analyses: A Rejoinder to Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks," *Federal Probation* 80, no. 2 (September 2016): 38-46

381 J. Dressel and H. Farid, The accuracy, fairness, and limits of predicting recidivism, *Science Advances* 2018;4: eaao5580 17 January 2018.

382 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366

383 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366

information may be linked to sensitive information.[384] It can therefore be questioned whether the exclusion of sensitive information is useful to prevent discrimination.[385] Calders and Žliobaitė explain that if one excludes the sensitive attribute from training data, this does not help if other attributes, such as zip code, are correlated with the sensitive attribute.[386] If one is to also remove those correlated attributes, objective, useful, information about the label is lost as well[387] and the predictive accuracy of a system becomes lower.[388]

Bias can lead to discrimination in various unintended ways. Data and analysis can be based on assumptions baked into the process through the way data are collected or because the data reflect biases that persist in society at large.[389] As discussed above, this problem in law enforcement risk profiling has for the majority to do with the limitations and prejudice of law enforcement data. Nevertheless, another way in which bias can lead to discrimination is through labelling of examples and rules that the algorithm is coded on, or design rules such as attributes in the training data[390], or even technical bugs that can lead to more false results for certain groups.[391] This second group of bias has more to do with the technical components of risk profiling systems.

---

384 Custers B.H.M. (2004), *The Power of Knowledge: Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Tilburg: Wolf Legal Publishers, ISBN: 90-5850-085-3, p. 57.

385 Calders T., & Žliobaitė, I. "Why unbiased computational processes can lead to discriminative decision procedures." In: *Discrimination and privacy in the information society*, pp. 43-57. Springer, Berlin, Heidelberg, 2013.

386 Calders T., & Žliobaitė, I. "Why unbiased computational processes can lead to discriminative decision procedures." In: *Discrimination and privacy in the information society*, pp. 43-57. Springer, Berlin, Heidelberg, 2013.

387 Calders T., & Žliobaitė, I. "Why unbiased computational processes can lead to discriminative decision procedures." In: *Discrimination and privacy in the information society*, pp. 43-57. Springer, Berlin, Heidelberg, 2013.

388 Calders T., & Verwer, S. "Three naive Bayes approaches for discrimination-free classification." *Data Mining and Knowledge Discovery* 21, no. 2 (2010): 277-292.

389 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. in 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125; Barocas, S. & Selbst, A. "Big data's disparate impact." *California Law Review* 104 (2016): 671, p. 671.

390 Van Brakel, B., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. in 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125; L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

391 Van Brakel, B., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125.

Some scholars propose that there is a responsibility for programmers in this respect to design systems that actively try to avoid bias and ultimately discrimination.[392] While I agree with the latter, to the extent that there should be attention in system design for countering bias, this only works for the system design; the limitations in the data still apply and affect the process.

3.4 Probabilistic systems: the use of statistics, group profiles and predictive strategies

Profiles rely inherently on possibilities, as was explained in chapter 2. In itself, a profile is a representation or image of a person through data. Abstracting from an individual is necessary for profiling to be efficient: the activity of profiling cannot do without making some generalizations, assumptions, and relying on chance and correlations. There are multiple aspects of the profiling process that feed into the probabilistic nature and these come with challenges of error and accuracy. Section 3.4.1 describes the challenges of generalizing from the individual to group or aggregated level, section 3.4.2 explains the challenges of predictive aspects of risk profiling.

3.4.1. Correlations and non-distributive profiles

One aspect of profiling that creates assumptions and reliance on probabilities is the focus on correlations. Arguably, the emergence and interpretations of correlations are at the heart of profiling.[393] Most of the profiles are probabilistic, describing the chance that a certain correlation will occur.[394] While profiling facilitates finding correlations easily and profiling is fed useful information via correlations, that does not mean the reliance on correlations is without its problems. A starting point for this discussion is the significance of correlations, or rather, their lack of meaning: a correlation does not mean anything until it is interpreted; correlations are in no way causal connections.[395] Profiling, in contrast to some other analysis processes, does not start from a hypothesis

---

392 Van Brakel, B., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125.

393 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

394 M. Hildebrandt, Defining Profiling: A New Type of Knowledge?. In: *Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth*, Springer 2008, p. 21-22.

395 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

that is then rigorously tested, but generates correlations without necessarily even being interested in causality or reasons.[396]

In section 3.2 I discussed the fairness-efficiency trade-off; in the reliance on probabilities there is a possible accuracy-efficiency trade-off. While it might be efficient to rely on correlations without researching a reasoning behind or causal link between the correlations, it can come at the cost of accuracy. Individuals are grouped together based on a certain correlation, and if the individuals within that group also tend to display a certain other correlation, it can be added to their assumed preference or behaviour while it is not necessarily true that the individual displays both of those correlations. To make it more concrete, if someone's way of typing is being profiled, they can be placed in a group with people who type in a similar way. Consequently, if a lot of people who type this way tend to have a bad credit status, they can be correlated to those with a bad credit status and treated as such. The problem with correlations is that there is not necessarily a meaningful connection: is it logical that your typing behaviour has anything to do with your credit status? No, it is probably not a logical or meaningful connection, so if it is used it will likely lead to inaccurate decisions or measures. In contrast to correlations, causal relations do provide insight into the connectivity between different data points: causal relations explain the 'why' behind a connection. In the legal field, the emphasis is on causal relations rather than correlations. The current focus on correlations due to more data driven processes puts a strain on the reliability of the process.

The example of correlating typing behaviour to other behaviour is not just a matter of correlations, it is also a problem that arises due to the use of non-distributive profiling. In his seminal work on non-distributive profiles, Vedder explains the crucial differences between distributive and non-distributive profiles: distributive profiles assign properties to an individual in such a way that these properties are actually manifested by all the individual members of a group; non-distributive profiles are instead framed in terms of probabilities that certain properties are manifested by members of a group, based on statistical characteristics of the group as a whole. As a consequence, the properties in non-distributive profiles apply to individuals only as likelihoods, whereas the individuals in reality might not actually exhibit these properties.[397]

---

396 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

397 Vedder, A. (1999). KDD: The challenge to individualism. *Ethics and Information Technology*, 1(4), 275-281.

In most cases the individuals included under a profile do not share all the attributes or characteristics of the group profile; they are non-distributive.[398] This means that there is always an inherent risk of errors in the use of profiles, as it might include people erroneously within a profile or might miss certain individuals, leaving them out of scope, the first category being false positives, the second false negatives.[399] In case of false positives, people would be incorrectly classified according to a profile. This in turn could have consequences for decisions taken to the disadvantage of these persons, for instance, they could be erroneously subjected to police powers. In the case of a false negative, we encounter another problem of law enforcement, namely overlooking someone who should be a suspect or miscalculating the risk of recidivism. Especially in the context of terrorism threats, risk profiles aim at minimizing false negatives, as the societal consequences are a lot graver when allowing for a false negative than a false positive.[400]

In terms of accuracy, distributive profiles are more reliable than non-distributive ones. However, in terms of risk profiling, distributive profiles are less interesting as they provide for less new knowledge and possibilities for predictions and classification. Non-distributive profiles are obtained through an inferential process extending beyond what is already known about each individual.[401] As a consequence mistakes are more likely, such as false selection or exclusion.[402] However, mistakes are also difficult to detect, and usually additional data are necessary to trace back why certain individuals are placed in a certain group or are ascribed certain characteristics.[403] In the risk profiling process it should thus be made clear whether risk factors ascribed to people are based on distributive or non-distributive assumptions.

3.4.2. Predictive analytics

A big part of risk profiling is predictive analytics, in the law enforcement context referred to as predictive policing, which is mainly deployed for area-based predictions

---

398 M. Hildebrandt, Defining Profiling: A New Type of Knowledge?. In: *Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth*, Springer 2008, p. 21.

399 M. Hildebrandt, E.J. Koops, The Challenges of Ambient Law and Legal Protection in the Profiling Era, (2010) *Modern Law Review* 73(3) 428-460.

400 M. Leese, The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue* 2014, Vol. 45(5) 494–511.

401 P. Allo, The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020.

402 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

403 P. Allo, The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020.

and increasingly for individualized risk assessments.[404] Predictive policing makes use of data analysis and criminological theories incorporated in predictive models, allowing these models to approximate who will commit crimes and where they will commit them.[405] It is important to keep in mind that predictive policing is, despite the name, not about crime predictions but about implementing a prediction-led policing process, which consists of data collection, analysis, police operations, criminal response, and back to data collection.[406] This means ultimately that predictive policing is more of a process involving actions that are based on approximations of future behaviour, to be distinguished from simply predicting future actions; there can be an underlying assumption to predictive policing that it is actually possible to predict crime[407], and that forecasting tools will be accurate and police can use them to effectively reduce crime.[408] This optimism is often based on a mythological and unrealistic view of actual technological capabilities and practices.[409] Therefore, it is important to assess the flaws in predictive policing and discuss its challenges as a counter voice to the techno optimism surrounding it.[410]

It is important to distinguish between descriptive and predictive data mining.[411] When discussing risk profiling and especially its predictive aspects, the type of data mining that is mostly used is predictive mining for the purposes of classification. The classes for the profiles are based on input fields that contain different characteristics or attributes associated with the different classes.[412] When an individual shares these

---

404 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

405 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

406 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

407 van Brakel, R. and De Hert, P., 2011. Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies. *Journal of police studies*, 20 (3), 163–192.

408 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

409 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

410 See the work of Bennet Moses & Chan, who have a similar aim: L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

411 For a more elaboration on the difference between descriptive and predictive data mining, please refer back to chapter 2, section 2.3.2.

412 Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 46.

attributes with people that are in a class, it is likely that this individual also belongs in that class. The more attributes shared with the class, the more likely it is that this individual indeed belongs in this class, but it remains a likelihood.[413] This type of classification is relatively accurate when it concerns 'either/or' values, but becomes increasingly inaccurate, if not impossible, if a multitude of factors apply, such as classifying whether or not someone will grow up to be a criminal.[414] An extra hurdle is that in many cases various factors that determine the class will not be present in the data set.[415] The omission of relevant variables for the predictive model, which might only become apparent afterwards, can teach an algorithm to classify based on unwarranted generalizations, while more granularity would provide more accurate outcomes.[416] For example, an algorithm can learn on the basis of a general attribute such as 'young and male' to determine dangerous driving while another variable, such as 'aggressive', would be more accurate.[417]

Besides the technique used in data analysis -descriptive versus predictive mining-, problems are caused by the data itself used in predictive analysis. Predictions rely, perhaps surprisingly, often on historic data and aggregated or group data. In most location-based predictive policing applications, in the USA but also in Europe, they are built around an off-the-shelf tool or tool adapted to law enforcement that analyses historical crime data, social media data, and weather data to predict where and when what crime will take place.[418] Taking the PredPol program as an example again, PredPol relies on historical crime data together with near-repeat theory.[419] Near-repeat theory explains that certain crimes re-occur in close temporal and spatial windows compared to when and where they previously occurred.[420] Because the near-repeat theory is so

413 Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 46.

414 Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 46.

415 Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, 27, p. 46.

416 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

417 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

418 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

419 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366

420 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366

dependent on up-to-date temporal information, the input data has to be updated regularly to produce accurate predictions.[421] This type of predictive policing works best for burglaries and property-related crimes such as car theft;[422] this also holds for example for the Dutch predictive policing program CAS[423] which is mainly effective for predicting burglaries.[424] There are also programs that work slightly differently, such as HunchLab. HunchLab was developed by a private company in Philadelphia and does not only use historic crime data but also population density; census data; the locations of bars, churches, schools, and transportation hubs; schedules for home games; and moon phases.[425] In addition, HunchLab incorporates different theories and modeling techniques, such as risk terrain modeling.[426] On the one hand it might seem like some of the data points processed by HunchLab are farfetched in their relation to crime, creating a risk of inaccuracy. On the other hand, it can be argued that it is dangerous to solely rely on historic crime data, like PredPol does. Relying on historic crime patterns assumes that these continue in the future; that assumption holds up better for some types of crime, such as for burglaries, than for other crimes.[427] Another point to consider in predictions, is the effect of inaccuracy due to feedback loops or self-fulfilling prophecies.[428] As this point was already discussed in section 3.3, I will not repeat myself here. It does show that it is difficult to disentangle issues, as one problem can lead to another, such as police biasing their own policing data which leads to errors in predictions.

An additional aspect that should be mentioned is that some predictive policing applications originate from different types of applications. For example, PredPol

---

421 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366

422 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

423 For more information about CAS please refer back to chapter 2, section 2.5.1.

424 TNO, 'Rule of law and investigation', available at: https://www.tno.nl/en/tno-insights/articles/how-big-data-is-reducing-burglaries-in-amsterdam/.

425 M. Chammah, Policing the future: In the aftermath of Michael Brown's death, St. Louis cops embrace crime-predicting software, 3 February 2016, The Verge. Available at: https://www.theverge.com/2016/2/3/10895804/st-louis-police-hunchlab-predictive-policing-marshall-project.

426 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

427 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

428 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

uses an earthquake prediction model.[429] The model works with the presumption that the crime to be predicted operates as a self-excited point process,[430] the same as earthquake aftershocks.[431] Naturally, the reliability can be questioned of predictive models or algorithms developed for a completely different context. Sometimes predictive law enforcement applications also make use of data from other sectors and parties. For example, law enforcement applications can rely on commercial data brokers and data gleaned from social media. The use of data gathered by other actors for different purposes than law enforcement carries risks of producing non-contextual and inaccurate results.[432] While there can be problems with law enforcement data, as discussed in section 3.3, data from other sectors cannot be used without checking them for suitability in the predictive policing context. For example, maybe different labels or categorizations are required for a new context.

The challenges of predictive policing discussed above concentrate mostly on location-based policing. However, there are also specific concerns to be discussed for predictive analysis on the individual level; a good example here is the practice of predicting re-offending. There are four different scenarios possible: the system classifies an offender as at risk of re-offending and the system is right (true-positive); the system classifies an offender as at risk of re-offending and the system is wrong (false-positive); the system classifies an offender as not at risk of re-offending and the system is right (true-negative); the system classifies an offender as not at risk of re-offending and the system is wrong (false-negative). Because systems are not always a 100% accurate in their predictions, there is always a risk of false negatives and false positives. This is highly problematic as the stakes are very high: if someone is given a higher sentence due to a miscalculation in the risk of re-offending, that is a grave violation of their rights. On the other hand, it can be argued if an individual is falsely perceived as non-risk or low risk, they will not be prevented from re-offending. A study in the USA found that most algorithmic approaches to predicting recidivism are not accurate: a

---

429 Mohler, G.O., et al., 2011. Self-exciting point process modeling of crime. *Journal of the American statistical association*, 106 (493), 100–108. doi: 10.1198/jasa.2011.ap09546.

430 Self-exciting point processes can be defined as processes with random sequences of events where the occurrence of an event increases the likelihood that subsequent events occur nearby in time and space, see: Fox, E. W. (2015). Estimation and Inference for Self-Exciting Point Processes with Applications to Social Networks and Earthquake Seismology. *UCLA*. ProQuest ID: Fox_ucla_0031D_13456. Merritt ID: ark:/13030/m5md16wm. Available at https://escholarship.org/uc/item/5cm7g4jp.

431 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

432 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

review of nine different algorithms found that eight of the nine failed to make accurate predictions, including COMPAS.[433] Another analysis found only moderate levels of predictive accuracy across all nine algorithmic approaches and concluded that these techniques should not be the sole basis for decision-making.[434]

There will always be false positives or negatives whether a system is automatized or based on human reasoning. However, in training and designing an algorithmic system, the question is what the consequences are of the various possible errors. For example, on the one hand one can have the risk of a crime of violence not being prevented because of a false negative. The consequence can be large, for instance severe physical harm or even death. On the other hand, in the case of a false positive for a violent crime, the consequence is that someone is unjustly deprived of their liberty, which is also serious. The consequences of different errors are asymmetrical: some will find the violation of the victim a more severe consequence, others the violation of the freedoms of the defendant.[435] Because the consequences are asymmetrical, the severity that is attached to the consequences of different errors needs to be taken into account in the system design. In the USA for example, a risk assessment algorithm was chosen to be programmed in such a way that the cost of a crime that results in the loss of life was scored to be twenty times higher than the cost of having to withdraw a (wrongful) decision to grant probation.[436] I would argue that thus the value attached to the different consequences is not easy to determine from an ethical point of view, to guide this decision the consequences have to be reflected upon using the underlying principles and values of the criminal justice system. This exercise can have a different outcome per jurisdiction or system.

---

433 K. A. Geraghty, J. Woodhams, The predictive validity of risk assessment tools for female offenders: A systematic review. *Aggress. Violent Behav*. 21, 25 (2015); M. Yang, S. C. Wong, J. Coid, The efficacy of violence prediction: A meta-analytic comparison of nine risk assessment tools. *Psychol. Bull*. 136, 740–767 (2010); Julia Dressel and Hany Farid, The accuracy, fairness, and limits of predicting recidivism, *Science Advances* 2018;4: eaao5580 17 January 2018.

434 K. A. Geraghty, J. Woodhams, The predictive validity of risk assessment tools for female offenders: A systematic review. *Aggress. Violent Behav*. 21, 25 (2015); M. Yang, S. C. Wong, J. Coid, The efficacy of violence prediction: A meta-analytic comparison of nine risk assessment tools. *Psychol. Bull*. 136, 740–767 (2010); Julia Dressel and Hany Farid, The accuracy, fairness, and limits of predicting recidivism, *Science Advances* 2018;4: eaao5580 17 January 2018.

435 J. Bijlsma, F. Bex & G. Meynen, Artificiële intelligentie en risicotaxatie: Drie kernvragen voor strafrechtjuristen. *Nederlands Juristenblad* 2019, issue 44, p. 2778- 3319; R. Berk, *Machine learning risk assessments in criminal justice settings*, Springer 2019, p. 32-36.

436 J. Bijlsma, F. Bex & G. Meynen, Artificiële intelligentie en risicotaxatie: Drie kernvragen voor strafrechtjuristen. *Nederlands Juristenblad* 2019, issue 44, p. 3316.

3.5 Opacity of risk profiling systems

Opacity is an issue that is linked to other challenges, since it may exacerbate issues of bias, discrimination, incorrect profiles or application, by hiding these undesirable effects or aspects intentionally or unintentionally. Opacity is also connected to challenges surrounding privacy and due process as it hinders enforcement of these rights. Therefore, the opaqueness of the risk profiling process cannot be seen separately from the other challenges. However, since it is mentioned so often in literature as a challenge of automated justice systems, risk assessment, and profiling in general, a brief exploration is warranted. I will therefore examine how and why the lack of transparency occurs and why this can be problematic.

Burrell, in her work on opacity in machine learning, suggests we can differentiate between different types of opacity. Burrell proposes there are three types of opacity related to algorithms; the first type is intentional corporate or institutional opacity; the second is a temporary opacity of the current time in which we live, in which reading code is not a skill everyone has; the third type is opacity that stems from the mismatch between mathematical optimization necessary for machine learning and the demands of human reasoning and styles of semantic interpretation.[437] This distinction by Burrell demonstrates two different sides of opacity, which require different analysis and solutions. The first type of opacity is primarily organizational. In the case of law enforcement risk profiling this relates to the need for law enforcement actors to shield some of their practices to protect investigative interests. Transparency is limited in this scenario by law and organizational limits; this type will be discussed in section 3.5.2. The second and third type of opacity have to do with automation and interactions between humans and machines and the understandability of that: the use of machines forms a complexity that can cause opacity. This machine complexity as a problem of opacity will be discussed in section 3.5.1.

3.5.1 Machine complexity and opacity

An important aspect of risk profiling is the automation of the process, increasing the involvement of data mining, algorithms and AI in general. As a consequence of this increased automation, discussions take place on the interaction between humans and machines; opacity is at the heart of concerns about algorithms.[438] Where analytical or decisional processes were less automated before, the opacity in those processes came

---

437 Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

438 Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

from not having insight into human reasoning or decision-making. Now the situation is different in the sense that there can be a disconnect between the process occurring in the machine and how humans view a process. Some parts of the automated process might be too complicated to offer transparency, or too complicated to offer any form of meaningful transparency. Algorithms are an almost mystical component in this regard; humans put data in and receive an output. A large part of the opacity concerns stems from the fact that the one who receives the output rarely has a concrete sense of how or why a classification was reached from the input, in addition sometimes not even the input is known or clear.[439]

As Burrell states in the second type of opacity, code writing and reading is a specialist skill,[440] limiting insight into the process to a limited circle of people. This raises questions as to whom transparency should be addressed. Do we view it as a problem that processes become too opaque for lay-people? The same challenge applies to the tension that Burrell mentions between characteristics of machine learning and the demands of human-scale reasoning and styles of semantic interpretation.[441] To what extent machine processes should be interpretable for humans and for which humans is not a question that can be answered here in this chapter, but does illustrate the complexity of the challenge of opacity.

It can be tempting to accept that machine opacity comes unavoidably with automation for scale and efficiency, but opacity is problematic for various reasons, especially when it concerns an application used by actors in law enforcement tasks. For example, transparency has an inherent value for governmental actors in that it allows for informed participation by the public. Transparency also has an indirect value, serving as a check on corruption or systemic problems that become apparent through public scrutiny.[442] Democratic participation is obviously difficult when it comes to covert processes of law enforcement, but it does play a role in law making for such processes and determining the safeguards. Transparency is inherently important throughout the chain of actors in a process: police need to be able to understand what they are doing with a risk profiling system to use it legally, ethically and efficiently; judges and actors such as district-attorneys or judge-commissioners need to be able to follow the process

---

439 Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

440 Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

441 Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

442 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

to give permissions; defendants need to be able to understand the process and activities they are being subjected to. Not only is transparency thus inherently important for a functioning system, it also aims to mitigate problems, which is reflected in its indirect value. This is important because complicated algorithms and the use of machine learning have the potential to exacerbate problems in automated systems. Profiling using machine learning has several more complexities that require transparency to expose potentially problematic aspects; for example, machine learning can create less predictable and more complex inferences that can conceal discriminatory treatment, or machine learning systems can be black-box systems hiding either input, internal logic or output, or turning those factors incomprehensible.[443] This is largely an issue of opacity since issues such as bias or discrimination need to become visible first before people are able to start addressing them.

An interesting question is if there are differences in opacity. Danaher et al. explain that one of the most important developments in the designing of algorithms over the years is a move from 'top-down' algorithms (in which programmers exhaustively define the ruleset for the algorithm) to 'bottom up' machine-learning algorithms (in which the algorithm is given a learning rule and trained on large datasets in order to develop its own rules).[444] Bottom-up algorithms are seen as more opaque, or involving more transparency issues, than the top-down algorithms.[445] Some contend that the more complex an algorithm or automated system is, the more opaque and inscrutable it becomes.[446] Some also contend that the more complex systems are, the higher the reliability or accuracy of the outcomes;[447] for example, Hildebrandt contends that with neural networks high accuracy comes with a lack of interpretability.[448] The neural network operates as a black box, hiding potentially relevant features, their

---

443 S. Wachter, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review* 34 (2018) 436–449, p. 443.

444 Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. Big data & society, 4(2), 2053951717726554.

445 Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554.

446 For example, for some of these arguments, see J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512; Justin Jouvenal, The New Way Police Are Surveilling You: Calculating Your Threat 'Score,' Washington Post (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac.

447 For example, for some of these arguments, see J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

448 Hildebrandt, M. "Data-driven prediction of judgment. Law's new mode of existence?." *Draft Chapter for OUP Collected Courses Volume EUI 2019 Summerschool* (2019).

interrelations and weight.[449] Applying this to risk profiling, one can think of an instrument like COMPAS, but then in an even more complicated form, where it is not clear which factors are relevant in the risk assessment, nor how they are related or ranked and weighed. In the law enforcement context it remains important to maintain insight into the working of this process for law enforcement actors as they need to be able to explain it to judges or other actors providing checks and balances.

An important term in the context of transparency is that of explanation, as explanations can be seen as an information tool offering transparency. The question is what this means in the context of risk profiling. Hildebrandt distinguishes between explanations and justifications: where an explanation does not have much legal meaning, judges will need a justification for the model's predictions.[450] An explanation of how the outcome was achieved does not have the same legal meaning as a justification.[451] In a sense that is true, but it can also be argued that an explanation and justification go hand in hand: one needs an explanation first to draft a justification. One has to keep in mind though that a justification can mean different things. In her work, Hildebrandt uses an example of a justification of a system decision in terms of verifying a causal link between specified input features and the system's output.[452] This is a justification made from a more technical perspective to ascertain that the outcome of a decision is correct in terms of the data pointing that way. This is not the type of justification of an outcome usually referred to from a legal perspective; the data may point a certain way, but legal requirements have to be fulfilled such as a causal link between actions, the presence of guilt, requirements for liability, and so forth. Therefore, the question remains what we require from transparency from a legal perspective and what counts as a justification and what is viewed as an acceptable explanation.

3.5.2. Legal and organizational opacity

As can be derived from Burrell, not all opacity in complex systems stems from machine complexity. There are also intentional limitations to transparency that cause opacity. This is the first type of opacity Burrell mentions, of self-protection and concealment.[453] There is an obvious component to this when discussing profiling practices by law

449 Hildebrandt, M. "Data-driven prediction of judgment. Law's new mode of existence?." *Draft Chapter for OUP Collected Courses Volume EUI 2019 Summerschool* (2019).

450 Hildebrandt, M. "Data-driven prediction of judgment. Law's new mode of existence?." *Draft Chapter for OUP Collected Courses Volume EUI 2019 Summerschool* (2019).

451 Hildebrandt, M. "Data-driven prediction of judgment. Law's new mode of existence?." *Draft Chapter for OUP Collected Courses Volume EUI 2019 Summerschool* (2019).

452 Hildebrandt, M. "Data-driven prediction of judgment. Law's new mode of existence?." *Draft Chapter for OUP Collected Courses Volume EUI 2019 Summerschool* (2019).

453 J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1 (2016): 2053951715622512.

enforcement: if the entire process is transparent there is a possible risk of criminals trying to game the system to avoid detection or to hinder the criminal investigation. The law legitimizes covert operations by law enforcement and in that sense establishes organizational or legal limits to transparency. However, the difficult question, which cannot be answered here, is to what extent law enforcement can rely on this argument to prevent transparency.

There is a more troublesome part relating to organizational opacity, though. Risk profiling applications, or the algorithms for those applications, are usually developed by private companies.[454] The law enforcement sector either buys these applications from companies and for example finetunes them further to their own needs or they work together with a private company for this application. The involvement of private companies in law enforcement activities brings with it a type of opacity of its own. This becomes most apparent in predictive policing algorithms where transparency is widely lacking.[455] Companies such as Intrado, the company behind Beware, claim the right to shield the code powering their algorithms as trade secrets.[456] From the perspective of the private companies, revealing how an algorithm works might expose valuable trade secret information to competitors.[457] I agree that there might be some reasonableness to these claims but it is problematic if police officers, judges, and to some extent the public, do not have access to how the predictions are made, creating a gap in legitimacy of the factors used.[458] This opacity also has consequences further down the chain as it is impossible to ascertain whether searches or arrests were made legally, and the accuracy of decisions and the methodology of law enforcement cannot be put under scrutiny.[459] In the USA, the justification of trade secrecy has been applied by judges to reject requests from defendants to get access to the algorithm that was used in the decision-making in their conviction and by police to deny access requests to their algorithms for predictive policing.[460] In that sense the problem is not so much the companies themselves but rather

454 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

455 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366.

456 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366.

457 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

458 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366.

459 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366.

460 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

the construct of law enforcement working with private companies, instead of investing in in-house technical expertise, and the terms under which they acquire the software. However, if it is not possible to avoid the involvement of private companies, we should question, as some scholars propose, whether these companies should be permitted to invoke trade secrets to keep information from defendants and judges, from police itself, and from the public.[461] Limitations could be posed to the rights of private companies if they choose to get involved in law enforcement practices.[462]

3.6 Discrimination

Profiling as a practice empowers its users to re-establish inequalities.[463] Profiling allows for selection, which is neither good nor bad, but nor is it neutral.[464] Thus profiling impacts the lives of those that are selected and accordingly calls for justification.[465] This necessity for justifying selection becomes obvious in risk profiling through issues of discrimination. Risk profiling programs select specific individuals or groups for measures such as surveillance or detention and thus have a high impact on society. It can be argued that selection on some criteria is necessary for reasons of efficiency and proportionality, but at the same time such selection can have serious impact and requires objective justification. Predictions such as in which areas crimes will occur will likely produce more arrests in those areas by directing police patrols there and in turn generates more historical crime data for those areas and increases the likelihood of further patrols. Thus for those who live in those areas, these hot spots may well become as much part of their personal information as other demographic information.[466] Another illustration of risk profiling being used to target specific groups is in the social sorting aspect of it: people are sorted into categories assigning worth or risk, based on the assumption of a certain idea of what is the norm, non-confirmation of the norm being seen as suspicious.[467] This idea of non-confirmation being suspicious has a discriminatory effect, as can be seen

---

461 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

462 These discussions will be further explored in chapter 5 & 6.

463 Lessig, L. (1999a) *Code and other laws of cyberspace* (New York, Basic Books), p. 155.

464 Kranzberg, M. (1986) Technology and History: 'Kranzberg's Laws', *Technology and Culture*, 27, pp. 544-560.

465 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

466 K. Crawford & J. Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, vol. 55, issue 1, *Boston College Law Review* 2014.

467 Lyon, D. "Sorting for Suspects." *Arena Magazine* 70 (2004): 26-28; Van Brakel & De Hert, Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies* 2011-3, no. 20, Maklu, ISBN 978-90-466-0412-0, p. 176.

in certain stop and search practices by police.[468] Risk profiling is not a passive process of collecting and analyzing data, but shapes society by the choices made in the risk profiling policy. This is prone to (unintentional) discrimination, stigmatization, and inclusion and exclusion, and raises questions on such impacts. For example, if the risk profiling algorithm identifies a correlation between feature X and probability of offending, in what circumstances is it just or unjust to treat a person with feature X differently from others? Or, in the case tools that focus on location, such as CAS, in what circumstances is it just or unjust to increase surveillance of certain neighborhoods?[469] Thus, it comes down to questions of under which circumstances it is justified to target people. Traditionally, these concerns with discrimination focus on race and ethnicity, but predictive tools will create new groupings of targeted individuals or places that may not be associated with any historical category of discrimination, further complicating matters.[470]

The United Nations Special rapporteur on extreme poverty and human rights published a report in October 2019 on the digital welfare state. Under the concept of digital welfare state he describes the following developments: "(…) *new forms of governance are emerging which rely significantly on the processing of vast quantities of digital data from all available sources, use predictive analytics to foresee risk, automate decision-making, and remove discretion from human decision-makers*."[471] These are very reminiscent of risk profiling, albeit describing a broader field of practices by public actors than the law enforcement sector. The Special rapporteur mentions challenges of risk scoring and classification such as enforcing individual rights when groups are targeted, a lack of transparency surrounding the process but also risk classification reinforcing or exacerbating existing inequalities and discrimination.[472] The Special rapporteur made a separate analysis of the Dutch SyRI risk profiling system, in view of the court case against the use of SyRI,

---

468 Van Brakel R., & De Hert, P., Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies* 2011-3, no. 20, Maklu, ISBN 978-90-466-0412-0, p. 176.

469 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695; Zarsky, T.Z., 2013. Transparent predictions. *University of Illinois law review*, 2013 (4), 1503–1569.

470 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695; Zarsky, T.Z., 2013. Transparent predictions. *University of Illinois law review*, 2013 (4), 1503–1569.

471 Report of the Special rapporteur on extreme poverty and human rights, 11 October 2019, A/74/48037, P. 3. Available at: < https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx>

472 Report of the Special rapporteur on extreme poverty and human rights, 11 October 2019, A/74/48037, P. 9. Available at: < https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx>

and submitted his analysis to the court in an amicus brief.[473] According to the Special Rapporteur, such a system requires assurances that particular groups are not being unfairly singled out, and SyRI can have a hugely negative impact on the rights of poor individuals without according them due process.[474] This is not a problem solely of SyRI: many risk profiling systems will bear the risk of targeting minorities and the poor within societies. In the case of SyRI, over-targeting of groups based on nationality or socio-economic status can put individuals from such groups disproportionally on the police radar, or has the inherent risk of putting someone on the police radar based on a sensitive factor such as nationality; as a system risk-based system such as SyRI is used to narrow down against whom to start a criminal investigation (into fraud). Therefore, safeguards are required that ensure that such systems are not deployed to intentionally or unintentionally target disadvantaged groups, exacerbating existing challenges. For risk profiling systems used in later stages of criminal investigation or in sentencing and parole decision, the consequences are potentially even more serious, as will be discussed later in this section.

In essence profiling is a practice of simplifying reality to cope with a data overload, it is a form of prototyping, enabling law enforcement to make decisions. Hildebrandt explains prototyping as making decisions based on a knowledge-construct that filters our perceptions and expectations, and as being a psychological process but also an epistemological process to prevent being flooded by meaningless information.[475] The problem is that while prototyping is appealing as efficient, it is also close to stigmatization.[476] Risk profiling inherently, due to its nature of categorizing people and prototyping, can lead towards stigmatization. Stigmatization can be described as a certain negative attitude or belief towards or about people; when that stigma is acted upon discriminating behaviour takes place.

Some types of risk profiling are more prone to discrimination than other types, at least where it concerns direct discrimination. The risk of algorithmic discrimination is higher with predictive identification systems such as Intrado Beware, as it concerns

473 Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/HA ZA 18/388), available at: <https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf >.

474 Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/HA ZA 18/388), available at: <https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf >.

475 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

476 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

individuals instead of locations or large-scale profiling of populations or groups.[477] For risk profiling applied to individuals or used to identify individuals, the consequences are also potentially more serious.[478] That does not mean that discrimination does not occur in location based systems. Predictive mapping can lead to ethnic profiling, based on bias as described in section 3.3: if arrest rates are for example a factor in predicting in which areas most crime occurs and to deploy police surveillance accordingly, and if arrest rates are disproportionately higher in particular population groups as a result of ethnic profiling, the policing can lead to even more ethnic profiling.[479] For the Dutch predictive mapping system CAS, research has shown already that ethnic profiling is a significant problem.[480]

As stated before, risk profiling is a tool of efficiency and proportionality in policing. Through this function we can also see the other side of the coin; automated tools could also be used to reduce discrimination. According to Bennett Moses and Chan, there are tools that can reduce the potentially discriminatory impact of algorithmic prediction; however, that can only be done via a positive discrimination that may in turn reduce predictive accuracy.[481] Therefore, they do not argue in favor of or against deploying anti-discrimination techniques, rather they emphasize that the use or non-use of such techniques is a controversial choice, and that as a result, it would be unwise to assume that predictive policing tools are inherently neutral.[482] While much discussion is already taking place on the discriminatory effects of profiling, there is not much research yet on the use of automated systems to reduce discrimination; as seen in the COMPAS tool, the use of automation to enhance objectivity can backfire, but it is not

---

477 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125.

478 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125.

479 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125.

480 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 125; van der Leun, J. P., & van der Woude, M. A. (2011). Ethnic profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profiling and a changing social and political context. *Policing and society*, 21(4), 444-455.

481 See their discussion on potential tools: L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, p. 812.

482 L. Bennett Moses & J. Chan, Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, p. 812.

unthinkable that in the future tools are developed that truly create anti-discriminatory effects in previously biased or discriminating systems.

A related discussion is how to view discrimination that is deemed justifiable from a point of view of accuracy; should that be prohibited and under which conditions? Schauer argues that we might want to prohibit statistically justifiable discrimination, when three conditions are met: when such categories are more commonly the basis for inappropriate generalization than for appropriate generalization, when the use of that generalization is unfairly selective, and when the use of that generalization in particular circumstances would be stigmatizing or produce excessive separation.[483] The underlying question is how to apply these criteria in practice that Schauer proposes; these could be standards used in assessments by courts in cases of illegal discrimination in policing. At the same time there are ethical arguments about justice that can be put forward to criticize the idea of allowing discrimination that would be based on statistics or other data. Even if statistics are accurate it can be ethically problematic to reduce an individual's agency to an amalgamation of demographic probabilities and correlations. [484] Barrett illustrates this argument with the following example: "(…) *it would be empirically accurate to state that one in six black men has been incarcerated as of 2001, and that one in three will be incarcerated over the course of his life if current trends continue. It would be immoral to incorporate that demographic probability into the prediction of an individual's likelihood to commit a crime in real time*".[485] Since the possible justification for discrimination in policing is a legal discussion, I will elaborate on this discussion in chapter 5 on non-discrimination law.

3.7 Privacy

While the right to privacy and the right to data protection are two different fundamental rights, in this section I discuss privacy and data protection concerns together, since the specific concerns relating to risk profiling overlap and would cause repetition in discussing them separately. When it comes to concerns of profiling, the heading of 'privacy concerns' is broader than 'data protection concerns', as privacy concerns go beyond personal data and also include dimensions such as decisional

[483] Schauer, F., 2003. *Profiles, probabilities and stereotypes*. Cambridge, MA: Harvard University Press.

[484] L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366

[485] L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366

privacy.[486] Therefore, for completeness sake, the category is defined by the boundaries of the right to privacy rather than the right to data protection to cover the issues that relate to privacy, with a specific focus on informational privacy, which is where the right to data protection comes in.

The discourse on privacy and profiling already predates developments of machine learning and AI. There are extensive debates in legal literature concerning the impact of profiling practices on privacy and the capabilities of the right to privacy to deal with issues of profiling, surveillance, data mining and so forth.[487] Therefore I focus on the privacy challenges that are particular to risk profiling. While many of the previous discussions in this chapter focus on consequences of risk profiling, one concern to discuss is also the use of risk profiling itself, or rather the classification by law enforcement actors of people in itself. This fundamental aspect plays a role under the right to privacy.

I split issues of privacy largely in two parts. Risk profiling challenges the right to privacy because profiling is a process that uses large-scale data and data typical for risk profiling, such as group data or aggregated data. These points are discussed in section 3.7.1. There are also specific issues that connect to privacy from the aspects of risk profiling that focus more on predictions, steering individuals' behaviour or preventing their behaviour from taking place. These issues relate more to the autonomy part of the concept of privacy and deal with pre-emption and chilling effects, as well as confronting people with predictions about them. The latter group of issues is discussed in section 3.7.2.

3.7.1. Use of (non)personal information

In relation to the first cluster of privacy issues, I would argue there are three main issues. The first is the large scale of the data collection. Risk profiling requires big volumes and variety of data to be able to find interesting patterns and correlations. As discussed throughout this chapter, law enforcement risk profiling can also require

---

[486] For a clear overview of how privacy and data protection concerns are sperate but can overlap, see: E.J. Koops , B.C. Newell , T. Timan , I. Skorvanek, T. Chokrevski & M. Galic, 'A Typology of Privacy' (2017) 38 *U Pa J Int'l L* 483, p. 484.

[487] For example, but obviously there are many more: Hildebrandt, M., and S. Gutwirth. *Profiling the European citizen*. Dordrecht: Springer, 2008; Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554; Schermer, B.W. "The limits of privacy in automated profiling and data mining." *Computer Law & Security Review* 27, no. 1 (2011): 45-52; O. Tene and J. Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239 (2013); Wachter, Sandra. "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR." *Computer law & security review* 34, no. 3 (2018): 436-449.

all types of data beyond crime data and criminal history of individuals, such as data about someone's social network, past employment, social media data, and so forth. This ubiquitous nature of data collection raises concerns about protecting the right to privacy, as so much information is being revealed.[488] In the context of law enforcement profiling, some refer to a transparency paradox, as in citizens become increasingly transparent to governmental actors while simultaneously practices of governmental actors become increasingly opaque to citizens due to scale and technology.[489] This paradox shifts the power balance between governments and citizens, as safeguarded through the right to privacy, towards governments.[490]

The second related issue is the use of non-personal data and how increasingly information can be derived from this, such as group data or statistical data. On the one hand this issue relates to the use of group data, as discussed below; on the other hand with this I refer to the use of personal data previously not thought to contain privacy sensitive information, but in the end revealing actually sensitive personal data. The use of profiling can have a further impact on privacy as it infers and exposes new information. Gutwirth and De Hert provide a clear illustration of what they refer to as the 'correlatable human'.[491] Individuals leave a large amount of processable and correlatable electronic traces, which combined with pervasive and powerful datamining increases the correlatable potential.[492] With this focus on correlations and patterns comes a new privacy concern: correlations create new meaning, and seemingly insignificant personal data can turn out to be highly significant.[493] This raises questions for legislators and courts how to protect individuals against privacy infringements caused by generating information in an unseen way or ways that are not covered by existing protections in data protection legislation and privacy safeguards.

---

488 Broeders, Schrijvers, Hirsch Ballin, WRR-Policy Brief: Big Data and Security Policies: Serving Security, Protecting Freedom, The Hague 2017, https://www.wrr.nl/publicaties/policy-briefs/2017/01/31/big-data-and-security-policies-serving-security-protecting-freedom, p. 75.

489 Richards, N.M. en H.J. King (2013) 'Three paradoxes of Big Data', *Stanford Law Review Online* 41, available at: http://ssrn.com/abstract=2325537.

490 Richards, N.M. en H.J. King (2013) 'Three paradoxes of Big Data', *Stanford Law Review Online* 41, available at: http://ssrn.com/abstract=2325537; See also: Broeders, Schrijvers, Hirsch Ballin, WRR-Policy Brief: Big Data and Security Policies: Serving Security, Protecting Freedom, The Hague 2017, https://www.wrr.nl/publicaties/policy-briefs/2017/01/31/big-data-and-security-policies-serving-security-protecting-freedom, p. 75.

491 Gutwirth, S., and P. De Hert. "Regulating profiling in a democratic constitutional state." *In: Profiling the European citizen*, pp. 271-302. Springer, Dordrecht, 2008.

492 Gutwirth, S., and P. De Hert. "Regulating profiling in a democratic constitutional state." *In: Profiling the European citizen*, pp. 271-302. Springer, Dordrecht, 2008; Note that their publication is already from 2008, nonetheless the argument remains valid and relevant.

493 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

Crawford and Schultz describe the same issues for the USA legal framework.[494] In their research on predictive analytics, Crawford and Schultz explain that we cannot know in advance exactly when a learning algorithm will predict personal identifiable information about an individual and thus we cannot know where and when to assemble privacy protections around that data.[495] Similar privacy concerns apply to the use of statistical or anonymized data in profiling; it has been proven over the years that it is in fact not that difficult to identify individuals in such datasets and derive information about them.[496]

The third privacy issue in data collection and analysis is the focus on the use of group data as well as the unclear role of group privacy; this concern can be unpacked into multiple sub-concerns.

As it has been already discussed many times in this dissertation, the practice of profiling is dependent on abstractions and assumptions; aggregated data are used to inform categorizations and predictions; data about groups is used to compare individuals and learn more about individuals. In contrast, rights to protect information or data, such as the right to privacy and right to data protection, are still centering on individuals and information pertaining to them.[497] Taylor et al. explain that especially with the introduction of big data analysis, the individual is no longer central in the analytical process.[498] The appeal in data-driven profiling is in gathering large amounts of data often about undefined groups, where data is analyzed based on correlations and group profiles, resulting in informing general policy.[499] Van der Sloot describes big data as

---

494 K. Crawford & J. Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, vol. 55, issue 1, *Boston College Law Review* 2014.

495 K. Crawford & J. Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, vol. 55, issue 1, *Boston College Law Review* 2014.

496 Tene, O. en J. Polonetsky (2012) 'Privacy in the age of Big Data: A time for big decisions', *Stanford Law Review Online* 64, p. 65; for an extensive analysis of this issue, see my previous research in: B. van der Sloot, S. van Schendel & C.A.F. López, WODC/TILT 2022: The influence of (technical) developments on de the concept of personal data in relation to the GDPR, available at: http://hdl.handle.net/20.500.12832/3229.

497 Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer; For further research on this, in Dutch, see: B. van der Sloot & S. van Schendel, De modernisering van het Nederlands procesrecht in het licht van big data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving. WODC/Tilburg Univeristy, 2019, Tilburg.

498 Introduction: a new perspective on privacy, L. Taylor, L. Floridi and B. van der Sloot. In: Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer p. 13.

499 Introduction: a new perspective on privacy, L. Taylor, L. Floridi and B. van der Sloot. In: Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer p. 13.

gathering massive amounts of data without a pre-established goal or purpose, about an undefined number of people, followed by processing on the group or aggregate level using statistical correlations.[500] The data are not gathered with a specific person or group or aim in mind – the value becomes apparent later after analysis.[501] Van der Sloot gives the following example to illustrate this: *"It may appear that the data string – Muslim + vacation to Yemen + visit to website X – leads to an increased risk of a person being a terrorist."*[502] Taylor et al. contend that policies and decisions can be based on profiles and patterns and as such affect groups, and therefore suggest a focus on the interest of the group.[503] Taylor et al. further assert that the activity of forming groups in itself can already infringe privacy if the profiling is used for a goal that is not meant to respect the privacy of the group.[504]

Already in 1999, Vedder noted a similar shift towards interests of groups for data mining.[505] Not only do groups and their interests come to the fore more, but Vedder also explains the paradox between the data that profiles rely on and the impact that profiles have: the data used and the profiles themselves are not always considered personal data, at the same time the use of profiles can have a big impact on the persons with whose data they are constructed or on the persons to whom a profile is applied; in that sense the profiles, while not qualifying as personal data when it comes to legal protection, are used *as if they were* personal data while in fact they are not.[506]

This does not just impact groups, but according to Vedder also indirectly impacts individuals, as people are judged and treated more and more as members of a group rather than as individuals with their own characteristics and merits.[507] This argument

---

500 B. van der Sloot, Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under Article 8 ECHR. *In: Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies*. Dordrecht: Springer, p. 267-268.

501 B. van der Sloot, Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under Article 8 ECHR. In: *Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies*. Dordrecht: Springer, p. 267-268

502 B. van der Sloot, Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under Article 8 ECHR. In: *Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies*. Dordrecht: Springer, p. 267-268

503 Introduction: a new perspective on privacy L. Taylor, L. Floridi and B. van der Sloot. In: Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer p. 15.

504 Introduction: a new perspective on privacy L. Taylor, L. Floridi and B. van der Sloot. In: Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer p. 17.

505 A. Vedder, "KDD: The challenge to individualism." *Ethics and Information Technology* 1, no. 4 (1999): 275-281.

506 A. Vedder, "KDD: The challenge to individualism." *Ethics and Information Technology* 1, no. 4 (1999), p. 277.

507 A. Vedder, "KDD: The challenge to individualism." *Ethics and Information Technology* 1, no. 4 (1999), p. 277.

ties into the concerns of Taylor et al. about the importance of someone being placed in a group or grouped in a certain category.[508]

The legal framework of data protection and its adequacy in regulating group profiling will be discussed in chapter 4 of this dissertation. Nonetheless it is important to keep in mind here that risk profiling poses challenges to the regulatory scope of data protection and the safeguards awarded by the right to privacy, especially because focusing on the individual and the concept of personal data are put under strain.

3.7.2. Pre-emption, chilling effects and confrontation

3.7.2.1 Prevention & pre-emption

In the simplest sense, predictive aspects of risk profiling impact privacy in terms of collecting massive amounts of data intended to infer information and provide estimates or probabilities. Much becomes known about a person's characteristics, behaviour, and patterns in their behaviour. However, the practice of risk profiling goes further than collecting and analyzing information: knowledge is made actionable and acted upon. Individuals can be prevented from taking certain actions by using law enforcement powers against them: someone can be surveilled or detained; or, hypothetically, someone could be stopped before they break a window to commit a burglary, or stopped from throwing the first punch in a fight.[509] We then move from privacy issues of protecting information about oneself or self-determination to privacy aspects of autonomy and free will. Pre-emptive profiling can involve the systematic or targeted collection and processing of data, used to make predictions about future harm on the basis of profiles, with the main goal of intervening before actual harm is done.[510] Law enforcement actors have an interest in intervening with measures before actual crime takes place, especially in preventing crimes such as terrorist crimes.[511] Predictive algorithms use a preemptive temporality, making future uncertainties actionable in the present.[512] Pre-emptive policing presents a tension with the idea of

---

508 Where Taylor et al. explored the concept of group privacy, Vedder introduced the notion of categorical privacy.

509 Andrejevic, M., To Preempt a Thief, *International Journal of Communication* 11(2017), p. 883.

510 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 118.

511 Van Brakel, R. & De Hert, P., Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies* 2011-3, no. 20, Maklu, ISBN 978-90-466-0412-0, p. 175.

512 Sheehey, B. Algorithmic paranoia: the temporal governmentality of predictive policing. *Ethics Inf Technol* 21, 49–58 (2019). https://doi.org/10.1007/s10676-018-9489-x.

an individual's autonomy as actions are taken based on behaviour that is yet to take place, or a risk yet to materialize. In addition, it is difficult to say for certain or prove that intervention on the part of law enforcement actually prevented crime. Of course, law enforcement actors themselves will argue this is the case and present numbers about prevention of crime through police action.[513]

Andrejevic argues that pre-emption in the predictive policing sense remains a short-term, almost instantaneous practice.[514] For example, stopping a burglary or a fight from taking place is not about transforming conditions that contribute to theft or fighting, it is simply being in the right place at the right time to stop an imminent act before it takes place.[515] These are examples where the police show up to a high risk situation, such as a hotspot for burglaries or a hotspot for violence in bars. I would argue that location based pre-emptive profiling therefore does not necessarily impact privacy. But there is a different situation for systems such as SSL in Chicago or COMPAS where there is space to reflect on why some factors contribute to crime and plan strategies on addressing those, trying to steer individuals on a different path, which interferes with their autonomy. This is not necessarily a new activity for the law enforcement domain, preventing individuals in a vulnerable situation from committing crimes or previous offenders from re-offending. The situation changes to more unfamiliar territory though, when data allows for predictions that go even more into the future or depend on more uncertain correlations. The predictive analytics in risk profiling ask for safeguards to accurately guide this process and prevent privacy infringements.

3.7.2.2 Chilling effects of mass-scale data collection

The data-driven nature of risk profiling processes requires a large volume of data, and various types of data are collected to find interesting correlations that can prove to be relevant for a risk profile. This large-scale, opaque data collection raises questions concerning the proportionality of these processes with regard to the right to privacy. People feel this as a shift towards collecting everyone's data; as a result, this pre-emptive policing, in combination with all other surveillance technologies that are around, can have a cumulative surveillance effect.[516]

---

513 For example the law enforcement statement about PredPol, in: Wolpert, S. (2015, October 7). Predictive policing substantially reduces crime in Los Angeles during months-long test. UCLA Newsroom. Retrieved from http://newsroom.ucla.edu/releases/predictive-policing-substantially-reduces-crime-in-losangeles-during-months-long-test

514 Andrejevic, M., To Preempt a Thief, *International Journal of Communication* 11(2017), p. 883.

515 Andrejevic, M., To Preempt a Thief, *International Journal of Communication* 11(2017), p. 883.

516 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 127.

It is no question that the prevention of crime is a legitimate aim for law enforcement.[517] It is less clear, however, to what extent large-scale data collection is allowed for this aim, or more specifically, which safeguards are necessary to prevent abuse of these powers. One can think of examples such as COMPAS, where the risk profiling is quite overt; in instances of decision, suspects or convicts know that COMPAS is used to assist in these decisions, the process itself is opaque but overt. One can also think of examples such as the Dutch system of SyRI, which is a more covert system; it is not clear to those profiled that they are being profiled by this system or decisions about them are made using this system. Comparisons can be drawn between large-scale covert risk profiling such as SyRI and practices such as mass surveillance by intelligence agencies or large-scale surveillance and analyses by law enforcement agencies. The ECtHR has not decided on any cases of risk profiling with regard to the right to privacy, but it has ruled in many instances of surveillance and large-scale data collection[518], instances of large-scale data retention[519], and in instances of data processing by public actors with aspects reminiscent of risk profiling.[520] These cases also deal with aspects of collecting data about those who are not (yet) suspects and with blanket collection and storage and the (absence of) appropriate safeguards. This body of case law also shows the possibility of a chilling effect of such data collection by law enforcement. After the Snowden revelations[521], about the mass surveillance conducted by NSA, the risk of chilling effects became apparent.[522] The use of large-scale surveillance, combined with the fear that some in society have for governmental large-scale data collection, such as for national security, can have chilling

---

517 See for example the scope of the Law Enforcement Directive and article 8 of the European Convention on Human Rights.

518 Think for example of: ECtHR, *Klass and Others v. Germany* (Application no. 5029/71) 6 September 1978, ECtHR *Roman Zakharov v. Russia* 4 (Application no. 47143/06) December 2015, ECtHR *Szabó and Vissy v. Hungary* (Application no. 37138/14) 12 January 2016.

519 CJEU, C-293/12 and C-594/12, *Digital Rights Ireland*, 8 April 2014.

520 ECtHR, *Rotaru v Romania* (Application no. 28341/95) 4 May 2000; ECtHR, *S. and Marper v. United Kingdom* (Applications nos. 30562/04 and 30566/04) 4 December 2008; ECtHR, *Khelili v. Switzerland* (application no. 16188/07) 18 October 2011.

521 See for more information about this: Kosta, E., Surveilling Masses and Unveiling Human Rights - Uneasy Choices for the Strasbourg Court, Tilburg Law School Research Paper No. 2018-10, Available at SSRN: https://ssrn.com/abstract=3167723; Bauman, Bigo, Esteves, Guild, Jabri, Lyon, and Walker. "After Snowden: Rethinking the impact of surveillance." *International political sociology* 8, no. 2 (2014): 121-144.

522 Broeders, Schrijvers, Hirsch Ballin, WRR-Policy Brief: Big Data and Security Policies: Serving Security, Protecting Freedom, The Hague 2017, https://www.wrr.nl/publicaties/policy-briefs/2017/01/31/big-data-and-security-policies-serving-security-protecting-freedom;Walt, S.M. (2013) 'The real threat behind the nsa surveillance programs', available at: http://foreignpolicy.com/2013/06/10/the-real-threat-behind-the-nsasurveillance-programs/.

effects and distrust in police.[523] The risk of a chilling effect goes beyond the practices of intelligence agencies. The CJEU, in the judgment criticizing data retention and annulling the Data Retention Directive, also points toward the feeling of surveillance that people can experience through large-scale data collection by law enforcement actors: "(…) *the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*".[524]

Despite the 'if you have nothing to hide, you have nothing to fear'[525] rhetoric propagated by some law enforcement agencies, it is undeniable that a constant electronic surveillance by law enforcement actors or other public actors, and in combination with private actors, creates a negative social effect.[526] If the public is aware of large-scale profiling by law enforcement agencies it can have a deterrent effect[527] on behaviour of individuals or of people in specifically targeted groups. It is only a small step from deterring people from certain criminal behaviour to chilling effects more broadly. It can be argued that a main point of risk based policing is to deter; the aim is to prevent risky behaviour from taking place, but the question is where to draw the line between deterring criminal behaviour and between general chilling effects pre-empting non-criminal behaviour. An additional problem is that such intensive data collection or surveillance tends to be aimed at certain high-impact crimes, which are more likely to be committed by people in specific socio-economic groups that are already disadvantaged in society, and people who commit high impact crimes are more likely to have criminal records and be put under intense surveillance.[528] This creates a circle of more data collection, surveillance and profiling targeted at certain groups in society, affecting their privacy more than other socio-economic groups in society.

---

523 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 127.

524 CJEU, C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, para. 37.

525 For an extensive analysis of this argument see: Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44, 745.

526 Hirsch Ballin,, Broeders, Schrijvers, van der Sloot, van Brakel, de Hoog. "Big Data in een vrije en veilige samenleving", WRR: Amsterdam University Press, Den Haag/Amsterdam 2016 p. 92.

527 For more on the deterrent effect of large-scale surveillance see: R. Clarke, Introduction to Dataveillance and Information Privacy, and Definitions of Terms (1997, revised 2016), <http://www.rogerclarke.com/DV/Intro.html>.

528 Van Brakel, R., Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press., Available at http://dx.doi.org/10.2139/ssrn.2772469, p. 127.

3.7.2.3 Confrontation with predictions and knowledge

One way in which information can have an impact is if it becomes known to the person concerned.[529] Most of the privacy discourse seems to focus on what happens if information becomes known to others, such as the police or other decision-makers, or to the public. There are not many authors exploring the other side of the coin: what happens when someone is confronted with information about themselves that is new or unknown to them, especially if it is information they might have preferred not to know? There is research being done on this topic by scholars such as Van der Sloot now: Van der Sloot frames large-scale data collection and predictive analysis in terms of having an impact on one's identity when confronted with such information.[530] This information can have an impact on one's self-development or autonomy. Confrontation with certain information can enable individuals to take measures, but it can also impact their sense of self in an existential way, forcing a person to reconstruct their identity.[531] A general example of knowledge that can be revealed is a diagnosis of a chronic disease. In the law enforcement sector one could think of examples of someone being notified that they statistically have a high chance of being a victim of a violent crime, so that might cause someone to be extremely cautious in their social life, or examples of young adults being told they are on a path to be likely offenders of crime later in life and engaged accordingly by school counselors or youth counselors, creating for example feelings of distrust or defeat. Another example of confrontation with knowledge from profiles comes from the Chicago SSL system[532]: "(…) *the Chicago PD uniquely combines the SSL with a Custom's Notification program to notify and warn subjects on the list with high risk scores that they have been flagged and will face increased legal penalties if they engage in criminal activity*."[533] Knowledge about possible future behaviour or about classification is also significant from a perspective of self-fulfilling prophecies. As someone is flagged as a potential criminal, this information might influence their behaviour accordingly.

---

529 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

530 B. van der Sloot (2021) The right to be let alone by oneself: narrative and identity in a data-driven environment, *Law, Innovation and Technology*, 13:1, 223-255, DOI: 10.1080/17579961.2021.1898315

531 Hudson, B. (2005) Secrets of Self: Punishment and the Right to Privacy, in: E. *Claes & A. Duff (Eds) Privacy and the Criminal Law* (Antwerp Oxford, Intersentia).

532 For more information about SSL please refer back to chapter 2.

533 B. Sheehey, Algorithmic paranoia: the temporal governmentality of predictive policing, *Ethics and Information Technology* (2019) 21:49–58. https://doi.org/10.1007/s10676-018-9489-x.

3.8 Due process

Due process can be described as an obstacle course,[534] more specifically an obstacle course of procedural rules which safeguard against injustice while facilitating the pursuit of truth.[535] Characteristics of due process are for example a reasonable suspicion for a criminal investigation and sufficient evidence for a criminal charge.[536] The core of receiving due process is receiving a fair trial, however there is more to due process than just the trial. While due process is a term frequently used in USA law and literature and is not a right in itself under EU law. Nevertheless, the right to a fair trial under EU law encompasses several aspects of due process, along with the right to an effective remedy, which sees to standing. In this section, the term due process is used to refer to the procedural right to a fair trial together with the right to an effective remedy.

As explained earlier, risk profiling falls within law enforcement practices that are very data driven and focused on preemption and prevention. This shift away from the traditional law enforcement practices and criminal justice paradigm, non-surprisingly, puts strain on the traditional safeguards for those law enforcement activities, which are enshrined in due process. Not only that, but there also needs to be a balance struck between the identification or prevention of risk and protection of the rights of those subjected to risk profiling. This tension between interests of the public and of the suspect or defendant are age-old questions of public policy[537] and are addressed through due process. The fair trial offers an interesting 'ideal type' or 'good practice' for the testing of knowledge claims (by the state) and emphasizes the importance of the combination of the interrelated principles of an independent and impartial judge, a public hearing, equality of arms, presumption of innocence, adversarial proceedings and the principle of immediacy, for lay-people being able to contest expert knowledge claims.[538] Therefore, it is important to explore the challenges to due process in this last section. Here, multiple challenges from the other sections come together: due process is about redress for discrimination, errors, privacy infringements but also dependent on fairness and transparency.

---

534 H. Packer, *The Limits of the Criminal Sanction*, Stanford University Press 1968, p. 163.

535 Marks, Bowling and Keenan, Automatic Justice? Technology, Crime and Social Control (October 19, 2015). In: *R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology*, OUP, Forthcoming.

536 Marks, Bowling and Keenan, Automatic Justice? Technology, Crime and Social Control (October 19, 2015). In: *R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology*, OUP, Forthcoming.

537 A. L. Washington, "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

538 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

When discussing challenges of risk profiling to due process, we can distinguish between four different groups of challenges discussed in the literature. The first group of challenges pertains to effective remedy and standing; the second group of challenges pertains to a fair trial with regard to neutrality and fairness; the third group of challenges pertains to transparency for a fair trial and equality of arms; and the fourth group of challenges pertains to the presumption of innocence.

3.8.1. Effective remedy

There are many possible causes why people want to seek redress in the context of risk profiling, for example: people can suspect that the collection of data for the creation of a risk profile is a violation of their right to privacy; the application of a profile to an individual can create a detailed overview of that person's life, causing them to seek redress; people can have the feeling that a risk profiling tool is biased, causing errors in decision-making or causing discriminatory treatment; or a risk profiling process can be opaque, raising the question whether rights of criminal suspects and defendants are respected. Besides all these possible fundamental rights violations, harm from risk profiling can also occur in other ways; for example, the sheer collection of data can have a chilling effect on people or feelings of distrust or unease towards law enforcement, or the classification and ranking of people can be perceived as a violation of their dignity or as stigmatizing. For these reasons, those experiencing harm might want to seek redress. However, there are several factors to law enforcement risk profiling that pose challenges to exercising an effective remedy.

An increasing problem is that many due process safeguards are tied to the trial stage, while with risk profiling, many issues might not make it to trial as an individual might not be tried in the end; in the traditional investigatory model the focus is on the trial, nowadays the focus is more on the pre-trial investigation.[539] It can be that risk profiling is being deployed against people without them being aware of this. When risk profiling is used in decision-making on the individual level, such as is the case with COMPAS, the suspect or defendant will be aware that a risk profiling instrument is used. However, in most other scenarios, this will not be apparent. If people are not aware of possible infringements, in terms of privacy or discrimination for example, they will not seek redress. A different problem is that when people are aware of possible infringements of their human rights due to risk profiling, it will be difficult to make use of an effective remedy. Risk profiling often targets groups, for example in location based predictive policing, or relies on data about groups or aggregated data. However, standing for most procedures (national courts, the CJEU, the ECtHR) requires an

[539] Koops, E. J. (2009). Technology and the crime society: rethinking legal protection. *Law, Innovation and Technology*, 1(1), 93-124, p. 118.

individual interest, granting individuals an effective remedy, but not groups.[540] At the same time, the interest that is at stake can be difficult to individualize. This creates a gap in due process.

There are legal developments that acknowledge this problem. Traditionally, the ECtHR in principle rejects complaints that are *in abstracto* (regarding a law or policy as such)[541], complaints *a-priori* (before a privacy violation takes place)[542], and class actions or *actio popularis*[543]. Nowadays, however, the Court is being less strict on these criteria and more inclined to allow in abstracto claims and claims by groups such as civil rights organizations, in exceptional cases such as cases concerning mass surveillance.[544] A similar development can be seen in data protection legislation, where the new instruments, the GDPR and LED, introduce rights of representation of data subjects. Article 55 of the LED, which is most applicable to law enforcement risk profiling, entails:

> *"Member States shall, in accordance with Member State procedural law, provide for the data subject to have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54[545] on his or her behalf".*[546]

---

[540] For more on this, in Dutch, see: B. van der Sloot & S. van Schendel, 'De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving', WODC 2019.

[541] ECtHR, *Lawlor v. UK*, application no. 12763/87, 14 July 1988.

[542] ECtHR, *Tauira and others v. France,* application no. 28204/95, 04 December 1995.

[543] ECtHR, *Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxemburg*, application no. 29121/95, 29 June 1999.

[544] B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities', In: *S. Gutwirth, R. Leenes & P. De Hert (eds.), 'Data Protection on the Move*', Springer, Dordrecht, 2016.

[545] The right to lodge a complaint with a supervisory authority, the right to an effective judicial remedy against a supervisory authority and the right to an effective judicial remedy against a controller or processor.

[546] Similarly, recital 87 of the LED explains: "Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body which aims to protect the rights and interests of data subjects in relation to the protection of their personal data and is constituted according to Member State law to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy. The right of representation of data subjects should be without prejudice to Member State procedural law which may require mandatory representation of data subjects by a lawyer, as defined in Council Directive 77/249/EEC (10), before national courts".

Developments such as including a right to representation for data protection infringements and opportunities for group representation with the ECtHR at least lower a part of the threshold for those impacted by risk profiling to seek redress when violations of their rights occur. Obviously, this still requires that people are aware of possible violations and that there is an organization willing and suited to help.

De Hert and Lammerant distinguish between three ways in which individuals or groups can be impacted by profiling: there are individuals or groups whose data are used to create the profile; there are individuals or groups to whom the profile is applied; and there are individuals or groups who are subject to a decision based on the profile.[547] Those who are subjected to a decision, generally speaking, have the most opportunities for redress. Those to whom the profile is applied might not be aware of this or have no opportunities to seek a remedy against the use of a profile as such. The individuals or groups whose data are used have an even more difficult road to seeking redress. A central problem to seek an effective remedy is harm. Where is the harm in one's data being used to construct profiles? What is the harm in being categorized, ranked or labelled? In general privacy harms are already difficult to grasp or prove, even more so when the harm is possibly not on the individual level.[548] Overall, it can be difficult to have access to an effective remedy in case of errors in categorization or ranking, or in case of discrimination or privacy violations in the use of risk profiles, depending on whether those issues become transparent or not and depending on the (clear existence) of harm.

3.8.2. Fair trial: neutrality & fairness

The right to fair trial, as the name implies, requires fairness of procedure. Many aspects of the risk profiling process raise questions pertaining to what is fair in terms of procedure: think of aspects such as replacing human decision makers with automated systems; influencing decision makers with data and automated decision-making; relying on categorization, scores, and predictions of behaviour. In exercising the right to fair trial there are two types of procedural issues: the first is that, as explained in the previous section, the criminal investigation might not result in a trial; secondly, possible issues with risk profiling are sometimes not assessed by the trial judge because they are deemed to have been corrected earlier. Most risk profiling systems

---

547 De Hert, P., & Lammerant, H., 'Predictive profiling and its legal limits: effectiveness gone forever?', in: B. van der Sloot, D. Broeders & E. Schrijvers (eds.), *Exploring the Boundaries of Big Data*, The Hague: WRR 2016, p. 147.

548 For more on this, in Dutch, see: van der Sloot, Bart. "B. van der Sloot & S. van Schendel, 'De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving', WODC 2019." (2019).

assist in decision-making or policy making.[549] At first sight it could be assumed that risk profiling systems are therefore a mere aid and do not heavily impact the fairness of procedures as such. For example, a tool such as COMPAS or OxRec merely provides an advice for parole and sentencing decisions. However, further research in the assistance by automated systems demonstrates that it is not that simple. Data tends to be surrounded by an 'aura of infallibility', deterring attempts to understand the process by which results are reached.[550] With the use of automated systems comes automation bias. Barrett presents a clear definition of automation bias: "*Automation bias stands for the proposition that individuals tend to rely on the judgments of automated decisions as superior to their own, even when they have reason to believe the technology is flawed*".[551]

Automation bias creates serious problems if not taken seriously. Compared to the bias in data discussed earlier in section 3.3, the problem here is more the perceived neutrality of using an automated system and the authority connected to such a system. This raises the question if we can really speak of systems *assisting* human decision makers. Rather, the situation becomes one where human decision makers have to present convincing grounds to diverge from the system analysis, or where so much authority is assigned to risk profiling systems that it is virtually impossible to contest them. Judges might treat the outcomes of a system that law enforcement used as a given and neutral, or police might rely on technology in the field despite mitigating circumstances that might have swayed their judgment otherwise.[552] To be able to contest a system such as a risk profiling system, the basic assumption that an algorithmically-derived assessment is objectively true, distant, and fixed, needs to be challenged or overcome first. Risk analysis is not objective but rather actively constructed and subject to a variety of subjective influences.[553] This subjectivity needs to be able to be challenged.[554]

---

549 See for example: van der Sloot, B. (2017). Where is the Harm in a Privacy Violations? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(4).

550 Eckes C, *EU Counter-Terrorist Policies and Fundamental Rights: The Case of Individual Sanctions* (OUP 2009); Marks, Bowling and Keenan, Automatic Justice? Technology, Crime and Social Control (October 19, 2015). In: *R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology*, OUP, Forthcoming.

551 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366.

552 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366.

553 A. L. Washington, "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

554 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017):327-366.

Automation bias is very difficult to tackle, as we have seen in the case of Loomis vs Wisconsin[555] challenging the COMPAS system. The court provided a procedural safeguard to alert judges in future cases to the dangers of such automated assessments, basically an advice attached to the Pre-Sentence Investigation (PSI) report[556] saying that judges should be alert to the dangers of systems[557] such as COMPAS. However, judges might not receive the tools to make an informed objective analysis of the quality and neutrality of the data, nor receive enough information or have enough expertise to assess the analysis conducted by the system. If systems are so complicated that only the programmers who developed them might understand them, how can we expect judges to make their own objective analysis about them? And if the workings of these systems are so secretive, how can we use expert witnesses, such as programmers, to offer explanations? After reviewing the Loomis case, Washington observed that the court in that case ignored the computational procedures that processed the data within the algorithm.[558] If courts only look at the data itself and the use of the outcome of the system, we miss an important step in assessing the process.

3.8.3. Fair trial: transparency & equality of arms

The principle of equality of arms is part of the right to fair trial. Equality of arms centers on giving both parties, prosecution and defense, equal opportunity to present their case. A necessary requirement for equality of arms is that both parties have access to the necessary information. This requires a certain level of transparency. In the law enforcement context, this is an especially difficult point, as explained in section 3.5. What information should be provided to the defense and to judges to guarantee a fair trial? How do we overcome the barriers posed by exceptions for law enforcement actors

---

555 Loomis v. Wisconsin, docket no. 16-6387, available at: http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/. Last accessed 28 March 2020.

556 The Wisconsin circuit court ordered a PSI report on the defendant in Loomis, which included a risk assessment generated by the COMPAS algorithm. See: A.L. Washington, "How to argue with an algorithm: Lessons from the COMPAS-ProPublica debate." *Colo. Tech. LJ* 17 (2018): 131.

557 Any PSI containing a COMPAS risk assessment must inform the sentencing court about the following cautions regarding a COMPAS risk assessment's accuracy: (1) the proprietary nature of COMPAS has been invoked to prevent disclosure of information relating to how factors are weighed or how risk scores are to be determined; (2) risk assessment compares defendants to a national sample, but no cross-validation study for a Wisconsin population has yet been completed; (3) some studies of COMPAS risk assessment scores have raised questions about whether they disproportionately classify minority offenders as having a higher risk of recidivism; and (4) risk assessment tools must be constantly monitored and re-normed for accuracy due to changing populations and subpopulations. See: A.L. Washington, "How to argue with an algorithm: Lessons from the COMPAS-ProPublica debate." *Colo. Tech. LJ* 17 (2018): 131.

558 A.L. Washington, "How to argue with an algorithm: Lessons from the COMPAS-ProPublica debate." *Colo. Tech. LJ* 17 (2018): 131.

to provide information and by private companies developing the risk profiling systems hiding behind their trade secrets?

In the case of Loomis vs Wisconsin[559], errors in the data used by the system were a threshold requirement for disputing the risk assessment score.[560] The data quality alone, however, is not sufficient to dispute the assessment because it says nothing about the manner of processing and analysis of the data.[561] Therefore, information about the data that goes into the system is rather meaningless in itself. The risk profiling systems combine data sources, weigh variables, establish ranks and categories.[562] The score or outcome is not directly apparent by looking at the data. The algorithm balances the relative importance of each data point to create weighted outcomes, the design requirements of the algorithm specify what the weighted value of each data point is.[563] For the case of COMPAS evaluations, without any indication of how the responses were evaluated, it is not possible to challenge the predictive score by just reviewing the question responses.[564] Thus, it matters which information is provided to achieve true equality of arms. As automated decision-making and profiling become more prominent and more complicated, this requires a regulatory response to further clarify and set minimum requirements for which information is to be provided. In the field of data protection legislation for example, we see provisions such as in the GDPR about providing information concerning the logic of the algorithm.[565] The provisions in the LED differ from the GDPR, leaving it up to national criminal procedural law to regulate such aspects.

Ultimately, an important question for the use of profiles is what defendants are able to contest in their defense: is it allowed to contest the decision based on the profile? The profile itself? The assumptions underlying the profile? If the remedy is only targeted at the decision, is it really effective? Someone might fit the profile that law enforcement created, but they might want to contest the validity of the knowledge construct that

---

559 Loomis v. Wisconsin, docket no. 16-6387, available at: http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/. Last accessed 28 March 2020.

560 A. L. Washington, "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

561 A. L. Washington, "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

562 A. L. Washington, "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

563 A. L. Washington, "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

564 A. L. Washington, "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

565 See chapter 4, section 4.3.4, for an extensive discussion on this topic.

lies at the basis of their profile (for example that the profile is a false positive) and/or they may want to question the relevance of categorizing people on the basis of the factors used.[566]

3.8.4. Fair trial: presumption of innocence

Risk profiling systems that are not aimed at decision-making in individual cases tend to have a large scale, think for example of the Dutch SyRI system. As the net is cast more and more widely to collect as much information as possible for building profiles and to detect or predict possible crimes, questions arise of who exactly is being surveilled or profiled. To give an example: most citizens are subjected to data-mining techniques, so even a very small false positive rate (1%) will result in a large number of innocent people being flagged as suspicious.[567] Marks et al. explain the critique on large-scale practices form the point of view of the presumption of innocence:

> *"A common criticism of mass surveillance and data retention is that it makes 'all citizens suspects' and this is frequently deemed to be objectionable in and of itself. A system of crime control has emerged that operates in parallel to the traditional criminal justice system. The parallel system treats all citizens as suspicious and its surveillance is not predicated on individualized suspicion but is ubiquitous".*[568]

I think such claims can be nuanced and disentangled. Taking the example of the Dutch implementation of this principle, the presumption of innocence assures multiple aspects: first, that a suspect cannot be faced with the burden of proving their own innocence; second, before a conviction, the suspect has to be subject to measures that are irreparable as less as possible; third, during pre-trial custody the suspect cannot be treated as if convicted and measures taken before conviction cannot have the aim of punishment; and fourth, the judge has to be impartial and unprejudiced.[569] The descriptions above from literature in which individuals are claimed to be unjustifiably labelled suspects thus misinterpret the presumption of innocence: first, the use of surveillance is not the same as labelling someone a criminal suspect, and generally speaking investigatory powers of police are meant to detect or find suspects. Second, if individuals are actually considered suspects, the presumption of innocence ensures

---

566 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

567 Solove D, 'Data Mining and the Security–Liberty Debate' (2008) 75 *University of Chicago Law Review* 343.

568 Marks, Amber, Ben Bowling, and Colman Keenan. "Automatic justice? Technology, crime and social control." *The Oxford Handbook of the Law and Regulation of Technology*, OUP, Forthcoming (2015).

569 See Corstens, G. J. M., & Borgers, M. J. (2014). *Het Nederlands strafprocesrecht* (8th edition). Kluwer, p. 45-47.

they have rights not to be treated 'as guilty', or as convicted. Using surveillance or gathering data on a large scale is not the same as treating someone as if convicted before a conviction and is thus not in itself a violation of the presumption of innocence. Another question is whether the burden of proof, which is put upon the public prosecutor during the trial and evidence collection leading up to the trial to prove a suspect should be convicted, is altered in any way in risk profiling, which would have an impact on the presumption of innocence. Some scholars propose that automatic systems reverse the burden of proof and are subject to errors that have to be substantiated.[570] Similarly, scholars propose that in large-scale data collection, a shift in the burden of proof occurs, as there is no crime to start with and hence individuals are surveilled before they, if ever, commit any crime.[571] Again, such claims have to be nuanced. The collection of data cannot be equated with shifting the burden on defendants to prove they are not guilty of a crime: the data can be collected as evidence to build an argument that a suspect is guilty, but it is still up to the prosecution to substantiate this position during a criminal trial. The fact that there is simply more data out there does not mean that it is then up to the suspect to disprove their own guilt.

In the court case contesting the SyRI program, the claimants also raised concerns of such large-scale systems eroding the presumption of innocence.[572] In essence, the complaint was that systems such as these assume that the people being profiled in them are suspects. The court did not go into this question, but rather viewed the large-scale data collection from the perspective of the right to privacy and proportionality within that right.[573]

For tools that predict recidivism risk, such as COMPAS or OxRec, it can be argued that individuals are then not judged on what they have already done but rather on what is likely that they will do in the future, based on inferences or correlations drawn by algorithms that suggest they may behave in certain ways.[574] Some authors speak of guilty prediction and a prevailing climate of suspicion.[575] Again, such statements can be nuanced. Certainly, there is a tension between predicting risk in future behaviour and the idea of criminal law as a tool to punish for (culpable) behaviour, that is, behaviour that already took place. At the same time such tools for probation and sentencing have

---

570 McGarry J, 'Named, Shamed, and Defamed by the Police' (2011) 5 *Policing* 219.

571 P. Vogiatzoglou, Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity, *European Journal of Law and Technology*, Vol 10, Issue 1, 2019.

572 Subpoena: https://pilpnjcm.nl/wp-content/uploads/2019/08/EN-Subpoena-SyRI.pdf

573 District court The Hague, 5 February 2020, ECLI:NL:RBDHA:2020:865.

574 P. Vogiatzoglou, Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity, *European Journal of Law and Technology*, Vol 10, Issue 1, 2019.

575 Wigan M and R Clarke, 'Big Data's Big Unintended Consequences' (2013) 46 *Computer* 46.

been used already before the introduction of risk profiling; they are subject to rules for judges to take these assessments into account in determining an appropriate sentence, as the risk of recidivism is at the same time an unavoidable part of determining an appropriate sentence, for example from the perspective of protecting (future) victims. I would thus argue that the problem is not the use of risk profiling as such here, but rather the regulation of the process and safeguards, for example when it comes to transparency and contestability, and non-discrimination. In addition, again, this is not really a question of presumption of innocence: the use of a recidivism risk tool does not convict someone of a crime not yet committed, rather it further details a sentence for a crime already committed, when found guilty.

3.9 Conclusions

This chapter assessed the various ways in which the use of risk profiling by law enforcement actors challenges the fundamental rights protection offered to those subjected to or impacted by the risk profiling process. For the challenges the argument can be made that they come to the fore in all stages of the risk profiling process. However, it is interesting to see which part of the risk profiling process creates the most challenges and where in the chain of events these concerns should be tackled. This is a difficult exercise, as there may be differences in the point in the process in which a challenge is created, the point where it causes an effect, and the point where it should be addressed.

Overall, questions arise whether the use of such systems in itself is fair and whether the systems provide fair outcomes or are used in a fair way. Fairness remains under-defined; although it is used by many scholars in a similar way, it cannot be delineated precisely. However, the concepts of fairness explored in this chapter generally point in one direction: this fairness concern mainly sees to a possible disparate impact or discriminatory effect of risk profiling systems; but it can also be linked to a perspective of due process in asking whether it is fair for humans to be judged by an automated system versus a human decision maker. Equality and a just treatment are therefore at its core; this is also reflected in legislation where fairness is used as a standard or requirement, such as in data protection legislation. The fairness concerns thus originate already at the start of the process, although the effects are felt mostly in the phase of applying the profile, and they should be addressed already in system design as well as again in the application phase.

Scholars from various disciplines explain the bias concerns of algorithmic or data driven systems. The issue of bias is that it prejudices the way in which data are

collected and selected or the way in which they are analyzed. As a consequence risk profiling can have errors in the process, because of underlying false assumptions, for example that the data are completely representative for the situation at hand. Another possible consequence is that the bias leads to an unequal treatment or application of the profiles, because the system is designed (unintentionally) to over-target certain groups or individuals or because incomplete data points that way. Bias therefore originates already in the data collection, while the effects are mostly noticeable in the data analysis and in the application. The redress has to already take place in the phase of data collection and design; I assume for the application phase that the focus will be on non-discriminatory treatment rather than bias.

Risk profiling systems work with a degree of probability. In order to efficiently make use of large volumes of data, assumptions are made about the patterns in data and approximations are made to evaluate individuals and groups. Relying on probabilities to scale up and perform predictive analysis carries an inherent chance that errors are made. It is often not even known how accurate risk profiling systems are, or research shows such tools are only moderately accurate.[576] If risk profiling systems are not fully accurate, the system will create false positives and negatives. As a consequence policing can fall short in that people who should be profiled as high risk slip through the nets of the system and, contrary to the preventative purpose of risk profiling, commit crime or re-offend. Another consequence is that some are treated unfairly and are profiled unjustly as high risk or are simply placed in a wrong category, which can cause a violation of human rights. The concerns surrounding the probabilities used in risk profiling thus arise in the phase of analysis and the consequences are felt in the application of the profiles. The easiest way to mitigate problems might be in the analysis phase, to achieve a correct outcome while the input data might be correct.

When algorithms are involved, questions of transparency come to the fore. In simple systems that revolve around analysis and decision-making conducted by humans we also see opacity in that decisional factors or reasoning by human decision-makers should be able to be questioned. When it concerns more complicated systems that rely on technology such as extensive data mining and algorithms, there can be some friction between what humans understand of the automated system: either the system is too complicated for non-technical experts involved in the risk profiling process to understand, turning it opaque, or it can even be too complex to fully grasp for more

576 K. A. Geraghty, J. Woodhams, The predictive validity of risk assessment tools for female offenders: A systematic review. *Aggress. Violent Behav*. 21, 25 (2015); M. Yang, S. C. Wong, J. Coid, The efficacy of violence prediction: A meta-analytic comparison of nine risk assessment tools. *Psychol. Bull*. 136, 740–767 (2010); J. Dressel and H. Farid, The accuracy, fairness, and limits of predicting recidivism, *Science Advances* 2018;4: eaao5580 17 January 2018.

technical experts. This machine complexity can obscure problematic aspects such as bias, discriminating use of the system or errors in the analysis or application. The use of risk profiling systems by law enforcement actors is also inherently opaque, as holds for most law enforcement practices. Law enforcement actors can make claims that a certain level of opacity is required to safeguard the effectiveness of their practices or protect the investigation. There is an underlying fear that transparency will lead to suspects gaming the system and abusing knowledge of law enforcement algorithms and assessment methods. Opacity is an issue that plays throughout the process, although in a lot of cases the sources of the data are relatively transparent. The concerns originate in the analysis and mainly pertain to that phase.

Risk profiling systems have the likelihood to discriminate against certain individuals or groups. The system can be biased through its data or design and then applied in such a way that groups are over-targeted by law enforcement actors and indirectly discriminated against by the system. Predictive systems specifically run the risk of working with biased data or assumptions that create a self-fulfilling prophecy towards certain individuals or groups in society, stigmatizing them further or discriminating against them. While discrimination can originate from for example bias in the data, discrimination itself takes place in the application or use of the profiles when the bias results in an unequal treatment. Perhaps discrimination, because of its component of unequal treatment, is addressed best in the phase of application or treatment.

Naturally, all systems that collect and process large amounts of data cause friction with the right to privacy. Risk profiling systems reveal a lot of information about individuals or groups. Risk profiling often makes use of aggregated data or non-personal data or uses data not directly concerning a specific individual to still make predictions or evaluations regarding their behaviour. This blurs the boundary of the traditional distinction between personal and non-personal data and raises new questions pertaining to the more traditional privacy paradigm. Risk profiling also creates privacy challenges in terms of whose privacy to protect: while traditional privacy protection is focused on the individual, risk profiling relies on the forming of groups and generalizations and profiles are used to form public policy and can become public knowledge. Individuals are also treated as a member of a group. Therefore, risk profiling impacts both the privacy of individuals directly and indirectly as well as the privacy of groups. In addition to these concerns of the collection and use of information pertaining to individuals and groups, there are concerns pertaining to autonomy. Large-scale data collection can have chilling effects. Risk profiling can also be used to preempt behaviour. Individuals can even be confronted with information about their possible future actions limiting autonomy and creating self-fulfilling

prophecies, or simply confronting them with inferred information that is new to them. Privacy concerns of risk profiling originate sometimes in the collection of data itself, sometimes in the analysis of data that reveals information, but in the more predictive aspects more so in the application, such as through pre-emptive measures. The effects are thus also felt in different stages, but mostly in the collection of data (which feeds into the data analysis) and the application. The mitigation of possible issues depends on the one hand on proportionality and safeguards in data collection, but also on privacy preserving measures in the analysis, and safeguards for the autonomy of individuals in the application.

Risk profiling is a proactive or preemptive practice rather than a reactive practice. This shift away from the traditional law enforcement practices and criminal justice paradigm puts strain on the traditional safeguards for those law enforcement activities, which are enshrined in due process. More specifically, risk profiling challenges effective remedies and the right to fair trial. An increasing problem is that many due process safeguards are tied to the trial stage, while with risk profiling, many issues might not make it to trial. It can be that risk profiling is being deployed against people without them being aware of this, or that those impacted simply have no remedy available. The use of automated system outcomes from the investigation or in the trial can impact the neutrality or fairness of the trial, for example through automation bias. Risk profiling also raises fair trial concerns in terms of equality of arms if the defendant does not have access to the necessary information about the risk profile; the opacity puts a strain on due process. Due process concerns arise when risk profiles are applied and the effects are felt then; safeguards therefore also pertain to the application phase.

The placement of the concerns above along the risk profiling process can be viewed in the two tables below.

Table 2. Origin of the challenges along the stages of risk profiling

Challenge / Stage	Data collection/system design	Data analysis	Application
Fairness	X		
Bias	X		
Probabilistic systems		X	
Opacity		X	
Discrimination	X		
Privacy	X	X	X
Due process			X

Table 3:.Effect or impact of the challenges along the stages of risk profiling

Challenge / Stage	Data collection/system design	Data analysis	Application
Fairness			X
Bias		X	X
Probabilistic systems			X
Opacity		X	
Discrimination			X
Privacy	X		X
Due process			X

As shown in table 2, most challenges originate already in the phase of the design of the system and the data collection; some in the data analysis. The division between the origin of problems being placed in data collection and system design, or data analysis, or application, is admittedly over-simplified and to an extent also dependent on the situation at hand. Nonetheless, the point of the table is merely to illustrate in simple means that while problematic consequences of risk profiling are mostly experienced in the stage of application of the profile, as illustrated in table 3, that is not to say that the challenges originate there. The assumption that the challenge are mostly notably later on in the risk profiling process is a result of the fact that this is the point in time where those subjected to profiling are made aware of or confronted by possible problems. Because the profiling process is a process where different steps are so heavily influenced by each other, issues early on in the process will reverberate throughout.

This chapter presented the challenges of risk profiling that the later chapters rely on as well. In chapters 4 to 6 the regulatory frameworks of data protection law, non-discrimination law and criminal procedural law are discussed. The concluding chapter brings together this analysis of the challenges of risk profiling and the regulatory framework, by explaining how the challenges are addressed by the different laws, or how they are left unaddressed.

Chapter 4

Data protection regulation of law enforcement risk profiling

4.1 Introduction

One of the legal frameworks to explore for the regulation of risk profiling is that of data protection, which regulates the resource of profiling, namely data. Data protection legislation forms a complicated framework in itself with legislation on the level of primary EU law and of CoE law, but also contains secondary EU instruments, CoE recommendations, and national legislation. Data protection legislation covers many steps of the profiling process, such as the collection of data for the creation of the profiles, but also, to some extent, the conditions under which data can be analyzed or used -data protection can for example be used to ensure fair treatment in application of the profiles-.[578] More importantly, data protection legislation contains specific provisions regulating profiling and automated decision-making and related rights for individuals.

Data protection legislation has developed over the last four decades on a European level, first in the context of the CoE and later at the level of the EU.[579] Data protection can be seen as a legal framework aiming to protect rights, freedoms and interests of individuals whose personal data are collected, processed, and disseminated.[580] Data protection aims to protect values of fairness. Scholars such as Bygrave and Tzanou for example argue that the objective of data protection legislation is to ensure fairness in the processing of data and to some extent in the outcomes of the processing.[581] The objective of fairness is safeguarded through the main principles found in data protection legislation, whether it concerns CoE or EU legislation, such as purpose limitation, data quality, data security, transparency of processing and accountability.[582]

Data protection and privacy are often mentioned together in the context of profiling. While the right to data protection certainly has components that safeguard

---

578 Koops, E.J., Some Reflections on Profiling, Power Shifts, and Protection Paradigms (June 2008). *Profiling the European Citizen*, Hildebrandt & Gutwirth, eds., Springer, 2008, Available at SSRN: https://ssrn.com/abstract=1350584.

579 Hustinx, P., "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", available at: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en.

580 Gutwirth, S., and P. De Hert. "Regulating profiling in a democratic constitutional state." In: *Profiling the European citizen*, pp. 271-302. Springer, Dordrecht, 2008.

581 L.A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International: The Hague/London/New York 2002) 2; M. Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

582 M. Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

informational privacy or informational autonomy,[583] data protection also bears other core characteristics that are relevant for the context of profiling.

The processing of personal data is an asymmetrical process.[584] In most cases, the data subject has less power over the collection and analysis of data and requires information or transparency safeguards to compensate for the knowledge imbalance over the process, compared to the data processor or controller. Data protection aims to address this asymmetry through values of transparency, foreseeability, accountability, and participation of the data subject.[585] In addition to protecting informational privacy and addressing asymmetries, data protection aims to protect a broader interest, that of non-discrimination. The value of non-discrimination is important for all data processing but especially for those processes that are prone to discriminatory effects such as profiling.[586] There is thus a strong correlation between the right to data protection and the right to non-discrimination.

In this day and age, we have become very dependent on large-scale and multi-purpose processing. It seems practically impossible to solely focus on limiting data collection. [587] Therefore it is important that in addition to setting conditions and requirements for data collection, data protection offers tools for addressing wrongs.[588] In their seminal work distinguishing between privacy and data protection, De Hert and Gutwirth describe the role of data protection in a democratic society as a transparency tool promoting procedural justice while privacy is assigned a role of opacity in stopping power.[589] According to the De Hert and Gutwirth, data protection instruments do not aim to prohibit public authorities from collecting or processing data but rather channel their power, promote meaningful public accountability and provide data subjects with

---

583 See the work of Tzanou in discussing the overlap between privacy and data protection and how data protection forms a right in its own: Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

584 Tzanou, M., Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

585 Tzanou, M., Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

586 Tzanou, M., Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

587 E.J. Koops, The trouble with European data protection law, *International Data Privacy Law*, Volume 4, Issue 4, November 2014, available at: https://doi.org/10.1093/idpl/ipu023, p. 253.

588 Koops, E.J., Some Reflections on Profiling, Power Shifts, and Protection Paradigms (June 2008). *Profiling the European Citizen*, Hildebrandt & Gutwirth, eds., Springer, 2008, Available at SSRN: https://ssrn.com/abstract=1350584.

589 Gutwirth, S., and P. De Hert. "Regulating profiling in a democratic constitutional state." In: *Profiling the European citizen*. Springer, Dordrecht, 2008.

opportunities to contest practices.[590] Together with criminal procedural law, De Hert and Gutwirth see data protection as a form of procedural justice rather than substantive justice.[591] Especially with complex profiling, the consequences of the creation or the use of a profile are not always foreseeable, so it is difficult to prevent all possible negative consequences of profiling. Rather, tools are important that can correct errors, allow objection to profiling in a certain context, inform people about profiling, and so forth. Data protection legislation offers a framework of provisions that lay down the conditions for profiling and creates legal grounds to conduct profiling.

In the law enforcement context those provisions are further detailed per Member State in national legislation. In the criminal justice sector, the information asymmetry that data protection legislation aims to address is an inherent aspect of the law enforcement context especially when a data subject is a criminal suspect. Therefore it is important to review all aspects of data protection legislation together: general data protection principles that propagate values such as fairness and non-discrimination, provisions specific to profiling, but also data subject rights such as information rights that are paramount in safeguarding fundamental rights in such an inherently opaque sector.

An important factor for data protection legislation to be applicable, whether it is CoE or EU law, is that the data that are being processed are *personal data*. In that sense, the concept of personal data is key for data protection legislation. One question when it comes to risk profiling is whether all the processing concerns personal data. The reason that it can be questioned whether all parts of the profiling process are always regulated by data protection law is because personal data concern identified or identifiable individuals.[592] Profiling is a process that has parts that are not solely about data of individuals, for example, statistical or group data play a crucial role in creating profiles.[593] Or for example, a group profile can be created, and until that profile is

---

590 Gutwirth, S., and P. De Hert. "Regulating profiling in a democratic constitutional state." In: *Profiling the European citizen*. Springer, Dordrecht, 2008, p. 282.

591 Gutwirth, S., and P. De Hert. "Regulating profiling in a democratic constitutional state." In: *Profiling the European citizen*, p. 282. Springer, Dordrecht, 2008; See also Gutwirth, Serge and De Hert, Paul (2007). "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power." In: *Erik Claes, Antony Duff, and Serge Gutwirth., eds., Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia. pp. 61-104.

592 Article 2(a) Convention 108+; Article 3(1) LED.

593 A. Vedder, Why data protection and transparency are not enough when facing social problems of machine learning in a big data context. *In: E. Bayamlioglu et al. (eds), Being profiled: Cogitas, ergo sum. 10 Years of Profiling the European Citizen*. Amsterdam University Press, 2018, Available at SSRN: https://ssrn.com/abstract=3407853; Schreurs, W., Hildebrandt, M., Kindt, E., Vanfleteren, M. (2008). Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In: *Hildebrandt, M., Gutwirth, S. (eds) Profiling the European Citizen*. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-6914-7_13.

applied to a specific individual, it remains unclear what the status of the group profile is in terms of personal data.[594] For this chapter, in order to analyze data protection legislation, I assume most of the profiling process to be included in the scope of data protection legislation for two reasons: first, the concept of personal data itself is very broad, and if not identified already, individuals are often indirectly identifiable in data. This is an argument that has already been extensively discussed by others and by myself in other works.[595] For example, a lot of aggregated data can still contain identifiable information, while only large-scale statistical data is likely to be outside of the scope of personal data.[596] Second, as soon as group profiles are applied to the individual, data protection legislation becomes applicable.[597] Thus the only grey zone to discuss here is the application of profiles to groups instead of individuals, which I will discuss in section 4.3.3.

This chapter aims to answer the following question:

> *How is risk profiling by national law enforcement actors regulated under European data protection legislation, and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?*

In answering this research question chapter 4 presents one part of the puzzle of regulatory analysis of this dissertation, where chapter 5 and chapter 6 take the same approach for the legal frameworks of non-discrimination law and criminal procedural law. Chapter 4 also connects to chapter 3, which outlined the challenges caused by the use of risk profiling, and to the overarching analysis of the concluding chapter 7,

---

[594] A. Vedder, Why data protection and transparency are not enough when facing social problems of machine learning in a big data context. In: *E. Bayamlioglu et al. (eds), Being profiled: Cogitas, ergo sum. 10 Years of Profiling the European Citizen*. Amsterdam University Press, 2018, Available at SSRN: https://ssrn.com/abstract=3407853; Schreurs, W., Hildebrandt, M., Kindt, E., Vanfleteren, M. (2008). Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In: *Hildebrandt, M., Gutwirth, S. (eds) Profiling the European Citizen*. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-6914-7_13.

[595] See for example: Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40-81. https://doi.org/10.1080/17579961.2018.1452176; Sloot, B., Schendel, S. V., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. WODC/TILT. Available at: https://repository.wodc.nl/handle/20.500.12832/3229.

[596] Sloot, B., Schendel, S. V., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. WODC/TILT. Available at: https://repository.wodc.nl/handle/20.500.12832/3229, p. 100-112.

[597] See articles 11 LED and 22 GDPR for example; See also Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), 162-176.

which reflects on the adequacy of the current legal framework when data protection legislation, non-discrimination law and criminal procedural law are put together.

Chapter 4 starts with an analysis of CoE data protection legislation and its application to profiling in section 4.2. Section 4.3 follows with an analysis of EU data protection legislation, starting with a brief discussion of the history and background on the current instruments in section 4.3.1. Section 4.3.2 describes the data protection principles that apply to all data processing under the LED and GDPR, including profiling, moving to an analysis in section 4.3.3 of the specific provisions that regulate profiling. Subsequently in section 4.3.4 the relevant data subject rights are discussed to complete the picture. Section 4.4 concludes the chapter, providing the answer to the sub-question.

4.2 The CoE landscape

4.2.1 Convention 108+ and profiling

In 1981 the CoE adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[598], the Convention 108. As article 8 of the ECHR safeguards the protection of the private life, the Convention 108 lays down more specific safeguards for the protection of personal data. The scope of this convention covers both processing of personal data in the private and public sector, including the sector of law enforcement.[599] In contrast to the data protection legislation of the EU, there is no separate framework under the CoE jurisdiction for actors operating in the area of freedom, security and justice. In fact, until the introduction of the LED in the EU, the Convention 108 was leading for regulating security-related personal data processing.[600] The CoE's legislation on data protection has inspired data protection legislation elsewhere, such as that of the EU.[601] The CoE and EU data protection legislation can be seen as mutually supporting.[602] The CoE data protection legislation together with jurisprudence from the ECtHR on article 8 ECHR have had an enormous

---

598 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, No. 108.

599 Article 3 paragraph 1 of Convention 108.

600 P. De Hert & V. Papakonstantinou, Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review* 40 (2021), p. 4.

601 Convention 108+ Explanatory Memorandum, available at: https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo.

602 Bygrave, L.A., The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review*, October 2020, https://doi.org/10.1016/j.clsr.2020.105460.

impact on EU legislative developments in the data protection area, especially with regard to the DPD.[603] In addition, it is clear that CoE efforts inform much of the GDPR backbone and have been an important benchmark for EU data protection rules in the area of freedom and justice.[604] In 2018, the Convention 108 was updated to Convention 108+, to modernize it and to align the Convention better with the GDPR which then entered into force.[605] With the modernization, the aim was to include innovations such as accountability, transparent processing and also a new provision on automated decision-making. Convention 108+ includes additional safeguards such as the right not to be subject to automated decision-making without having his or her views taken into consideration and the right to obtain knowledge of the logic underlying the processing, as well as the right to object.[606]

Since the Convention 108 and EU legislation on data protection are so related, it is not necessary to analyze both on the regulation of profiling into detail. As the GDPR and LED have created much more debate and contain more detailed regulation than Convention 108, the focus in this chapter is on the EU instruments. Nonetheless it is important to at least briefly explain the regulation of profiling under CoE jurisdiction.

One of the criticisms expressed on the 1981 version of the Convention 108 text is that it was very limited in regulating the collection of data.[607] Only article 5 of the Convention 108 applied to the collection of data in that data had to be collected fairly and lawfully, and collected data should be adequate, relevant, not excessive and accurate.[608] Convention 108+ amends this by including collection of data in its definition of data processing, making all principles that apply to automated processing applicable to the full process of profiling, from collection of the data to applying the profiles or

---

603 Bygrave, L.A., The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review*, October 2020, https://doi.org/10.1016/j.clsr.2020.105460; See also G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

604 Bygrave, L.A., The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review*, October 2020, https://doi.org/10.1016/j.clsr.2020.105460.

605 Kierkegaard et al., 30 years on – The review of the Council of Europe Data Protection Convention 108, *Computer Law & Security Review* 27 (2011) 223-231. J. Ukrow, "Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention 108," *European Data Protection Law Review* (EDPL) 4, no. 2 (2018): 239-247.

606 Council of Europe, 'Modernisation of the Data Protection "Convention 108", available at: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.

607 Kierkegaard et al., 30 years on - The review of the Council of Europe Data Protection Convention 108, *Computer Law & Security Review* 27 (2011) 223-231.

608 Kierkegaard et al., 30 years on - The review of the Council of Europe Data Protection Convention 108, *Computer Law & Security Review* 27 (2011) 223-231.

making use of automated decisions. Another major change to article 5 is the inclusion of the principle of proportionality, laid down in paragraph 1. Previously the collection of the data had to be proportionate but the Convention did not place emphasis on the proportionality of the processing itself.[609] In the context of profiling, where large-scale data collection and processing takes place, pertaining to a potentially large group of individuals, proportionality is an important requirement.

Compared to the original Convention 108, Convention 108+ adds a few new data subjects rights in article 9. Article 9 paragraph 1 of Convention 108+ lays down restrictions for automated decision-making. Under (a), individuals have the right not to be subjected to automated decision-making without taking the views of the data subject into consideration, when it constitutes a decision with a significant effect. The explanatory report to Convention 108+ states that it is essential for individuals to be able to challenge automated decision-making by putting forward their arguments in a meaningful way.[610] Specifically the data subject should be allowed to substantiate possible inaccuracies of the personal data, the irrelevance of the profile to be applied, or other factors that impact the result of the decision.[611] According to the explanatory report, this is especially the case where data subjects are stigmatized by the application of algorithmic reasoning resulting in the limiting of a right or benefit.[612] The rest of paragraph 1 contains an information right with regard to processing of personal information (under b), an information right pertaining to knowledge underlying the processing (under c), the right to object to processing (under d), the right to rectification or erasure (under e), the right to remedy (under f), and assistance of a data protection authority (under g). The information right concerning knowledge underlying the processing of (c) is especially interesting for profiling when people want to know why they are profiled in a certain way or at least why a certain decision is being made about them. The explanatory report acknowledges this and states that data subjects should be entitled to know especially the consequences of the reasoning underlying the processing and the resulting conclusions,

---

609 C. de Terwangne (2014) The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data, International Review of Law, *Computers & Technology*, 28:2, 118-130, DOI:10.1080/13600869.2013.801588.

610 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

611 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

612 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

in particular in cases of profiling.[613] In this way the data subjects should be informed not just of the outcome of the process such as a yes or no, but more so about the logic underpinning this decision or the reasoning leading to it. According to the explanatory report, having this knowledge contributes to the effective exercise of other safeguards such as the right to object.[614]

Article 9 paragraph 2 determines that the right of paragraph 1 (a) not to be subjected to automated decision-making does not apply if there is a national law providing the legal basis for the decision and creating suitable safeguards. For risk profiling in the law enforcement context, this means that states can create a national law which enables data subjects being subjected to automated decision-making that significantly impacts them without their views being taken into consideration, provided there are suitable safeguards. Obviously, the question is what qualifies as suitable safeguards. As I will discuss later, article 9 of Convention 108+ on data subject rights is very similar to the data subject rights under the LED and GDPR of the EU, and the subsections of article 9 pertaining to automated decision-making are very similar to article 22 of the GDPR, although the GDPR is more detailed. The discussion on article 22 of the GDPR is therefore also relevant to article 9 of Convention 108+ and the discussion on data subject rights under the LED and GDPR will further engage in the question of what suitable safeguards are.

The Convention 108+ has a broad functional scope in that it applies to all data processing in the private and public sector, apart from the household exemption laid down in article 3 (2). In practice this means that all risk profiling will be subject to Convention 108+, but this does not mean that all the rights under article 9 of the Convention 108+ will apply to risk profiling in all fields. Article 11 of the Convention 108+ contains exemptions. For law enforcement purposes exceptions to various parts of Convention 108+, such as article 9, are possible when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society. The explanatory report states that processing of data must always be lawful, fair and transparent and limited to specific purposes.[615] This threshold applies to law enforcement authorities

613 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

614 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

615 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

as well and does not limit them from carrying out covert investigation or surveillance for the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, as long as their exceptions comply with the requirements above. The necessity of exceptions needs to be examined on a case-by-case basis, according to the explanatory report.[616]

4.2.2 The CoE Police Recommendation & profiling

In 1987 the CoE Committee of Ministers adopted the CoE Police Recommendation, which covers the use of personal data in the police sector, when personal data are processed for police purposes. In terms of scope of the recommendation, "police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order. With this document, the Committee of Ministers recommends that the governments of Member States respect a series of principles concerning control and data collection, notification of automated files, storage, use and communication of data for police purposes, and rights of access, rectification and appeal to police files.[617] Although the Convention 108 was already in place and also includes the police sector in its scope, it was deemed necessary to have a policy tool providing guidelines that takes into account the specificities of the law enforcement sector. While a recommendation as a policy tool does not have the 'teeth' that an instrument such as a treaty has, it does have the ability to fill in blank spaces in the discretion left to law enforcement actors in their ability to act under exemptions based on national laws, such as exemptions to Convention 108+ when it comes to data subject rights.

Since its adoption, the CoE Police Recommendation was subsequently evaluated in 1993, 1998 and 2002.[618] The accompanying explanatory memorandum gives further background on the CoE Police Recommendation, along with a practical guide released in 2018.[619]

---

616 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

617 Committee of Ministers explanatory memorandum, to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

618 Council of Europe, 16 February 2018, 'Newly adopted: Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime', available at: https://www.coe.int/en/web/data-protection/-/newly-adopted-practical-guide-on-the-use-of-personal-data-in-the-police-sector-how-to-protect-personal-data-while-combatting-crime-.

619 Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Practical guide on the use of personal data in the police sector.

Principle 2 of the CoE Police Recommendation contains guidance on the collection of data. Paragraph 1 details that:

> *"the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation".*

Interesting to note is the wording of 'a real danger' and 'specific criminal offence', seemingly to limit fishing expeditions or blanket predictive policing. The explanatory memorandum emphasizes indeed that principle 2.1 should be read as putting limitations on expansive police data collection. Principle 2.1 is intended to exclude *"an open-ended, indiscriminate collection of data by the police"*.[620] Furthermore the explanatory memorandum links back to data minimization under the Convention 108+: the Convention 108+ allows for a derogation from data minimization for the suppression of criminal offences, but principle 2.1 of the CoE Police Recommendation fills in that discretionary space by setting boundaries to this exception by limiting the collection of personal data to what is necessary for the prevention of *a real danger* or the *suppression of a specific criminal offence*.[621] Clarifying the term 'real danger' it is explained that this is not a restriction "*to a specific offence or offender but includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities*".[622]

Principle 2 paragraph 2 makes an interesting recommendation related to information rights of data subjects:

> *"Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where*

620 Committee of Ministers explanatory memorandum, to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

621 Committee of Ministers explanatory memorandum, to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

622 Committee of Ministers explanatory memorandum, to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

> *practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced".*

When a data subject is a suspect in a criminal investigation, or someone in the close social environment of the suspect, police will want to limit sharing what information they have on a suspect, meaning that national laws will provide exemptions from data protection information rights in such situations. Therefore, it is important that this document takes this opacity into account and recommends the police to release information as soon as this is possible, to prevent situations of police storing data on individuals without their knowledge, such as secret lists. The explanatory memorandum details two important points on this principle. The first point is the choice for the wording 'where practical': the recommendation is intended to take into account situations such as secret street surveillance where many individuals can be filmed and notifying all these individuals on the storing of such video data, following the principle 2.2, would be practically impossible. The second point is that it was deemed important to add this principle in view of case law of the ECtHR, which has demonstrated that the secret storing of data can be a data protection violation under article 8 ECHR.

Principle 2.3 recommends that technical surveillance or other automated means to collect data should be subject to detailed regulation. Again, here the recommendation follows the case law of the ECtHR. The explanatory memorandum gives the example of *Malone v. the UK*[623] from 1977 on wiretapping, but of course other cases since then have further added meaning to foreseeability and to the level of detail and safeguards required in national legislation.[624]

In addition to principles on the collection of data, the CoE Police Recommendation also contains one provision on the use of data, namely that "*personal data collected and stored by the police for police purposes should be used exclusively for those purposes*".[625] The only comment the explanatory memorandum makes on this is that this principle expresses the notion of finality, in that personal data collected for the prevention and suppression

---

623 ECtHR, *Malone v. the United Kingdom*, (Application no. 8691/79), 2 August 1984.

624 See for example: ECtHR, *Leander v. Sweden*, 1987; ECtHR, *Valenzuela Contreras v. Spain*, 1998; ECtHR, *Weber and Saravia v. Germany* , 2006; ECtHR, *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007; ECtHR, *Roman Zakharov v. Russia* [GC], 2015.

625 Principle 4.

of criminal offences or for the maintenance of public order must subsequently only be used for those purposes.[626]

4.2.3 The CoE Profiling Recommendation

In addition to its Convention 108, the CoE has a recommendation specifically on profiling and data protection.[627] This CoE Profiling Recommendation from 2010, on the protection of individuals with regard to automatic processing of personal data in the context of profiling, lays down internationally agreed minimum privacy standards in the context of profiling to be implemented through national legislation and self-regulation.[628] The main rationales behind the CoE Profiling Recommendation are listed in the preamble. The first one is the concern that profiles attributed to data subjects make it possible to generate new personal data which are not those which the data subject himself has shared with the controller. The second concern is the lack of knowledge on the side of the individual that they are being profiled, the lack of transparency and the lack of accuracy. Therefore, profiling might take place without the knowledge of the individual and the original data might be degraded when they are combined with old or inaccurate data.[629]

In the definitions, the CoE Profiling Recommendation distinguishes between creating and applying a profile. A profile is *"a set of data characterising a category of individuals that is intended to be applied to an individual"*.[630] Applying a profile means "*an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences,*

626 Committee of Ministers explanatory memorandum, to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies), para. 55.

627 Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

628 Council of Europe, Press release , 'Council of Europe adopts recommendation on profiling and data protection', Strasbourg, 25.11.2010. Available at: https://rm.coe.int/168071e498.

629 Savin, A., Profiling in the Present and New EU Data Protection Frameworks (December 1, 2015). In: Nielsen, P.A., Schmidt, P.K., Dyppel Weber, K. (eds.) Erhvervsretlige emne, Juridisk Institut CBS (Djøf 2015) ISBN 978-87-574-3524-5. Available at SSRN: https://ssrn.com/abstract=2697531.

630 Article 1(d), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

behaviours and attitudes".[631] For the scope of the CoE Profiling Recommendation it is important to keep these concepts in mind, especially which activities are acknowledged within the profiling process.

The CoE Profiling Recommendation also sets requirements for profiling, which are conditions regarding the lawfulness, data quality, and the use of sensitive data.[632] Article 3.1 requires that the purpose of the profiling should be specific. One could argue that this requirement is unrealistic, as profiles are increasingly created without a specific purpose in mind or the purpose can become apparent in a later stage.[633] The idea behind profiling can exactly be represented as a shift from knowledge being the result of a tested hypothesis to generating hypotheses, where the patterns and correlations in profiles are the outcome of the analysis and trigger the questions and suppositions.[634] Several scholars share the criticism or skepticism that principles of purpose specification and purpose limitation are not functioning anymore in the modern day and age in their current form.[635] However, this discussion goes beyond the CoE Profiling Recommendation; it is more of a criticism on data protection requirements in general.

The DPD, GDPR and LED have received a lot more attention from legal scholars than the CoE Profiling Recommendation, while there are quite some similarities regarding the regulation of profiling between these instruments. Therefore, the criticism and debate around the profiling provisions of the EU instruments is also relevant for the CoE profiling discussion. An interesting part of the CoE Profiling Recommendation compared to the GDPR and LED, is its detail on the parts of fairness and transparency

631 Article 1(e), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

632 Article 3, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

633 Savin, A., Profiling in the Present and New EU Data Protection Frameworks (December 1, 2015). In: Nielsen, P.A., Schmidt, P.K., Dyppel Weber, K. (eds.) Erhvervsretlige emne, Juridisk Institut CBS (Djøf 2015) ISBN 978-87-574-3524-5. Available at SSRN: https://ssrn.com/abstract=2697531.

634 Ferraris, V., Bosco, F., Cafiero, G., D'Angelo, E., & Suloyeva, Y. (2013). Defining profiling. Available at SSRN 2366564.

635 For example, see the works of Prins and Moerel: Prins, C., & Moerel, L. (2015). On the death of the purpose limitation principle. International Association of Privacy Professionals. Available at: https://privacyassociation.org/news/a/on-the-death-of-purpose-limitation/; Moerel, E.M.L. and Prins, J.E.J., Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016). Available at: http://dx.doi.org/10.2139/ssrn.2784123.

towards data subjects. Article 4 of the CoE Profiling Recommendation, on information rights of the data subjects, stipulates under article 4.1.f. which information is necessary to provide to data subjects from a point of view of fairness:

> *"- the categories of persons or bodies to whom or to which the personal data may be communicated, and the purposes for doing so;*
>
> *- the possibility, where appropriate, for the data subjects to refuse or withdraw consent and the consequences of withdrawal;*
>
> *- the conditions of exercise of the right of access, objection or correction, as well as the right to bring a complaint before the competent authorities;*
>
> *- the persons from whom or bodies from which the personal data are or will be collected;*
>
> *- the compulsory or optional nature of the reply to the questions used for personal data collection and the consequences for the data subjects of not replying;*
>
> *- the duration of storage;*
>
> *- the envisaged effects of the attribution of the profile to the data subject."*

Not only do these requirements demand from data controllers that they grant rights of access, objection and correction where necessary, but controllers also need to provide information concerning the envisaged effects of the attribution of the profile to the data subject. This requirement demands from controllers that they think ahead of what the effects of the use of this profile will be for the person(s) impacted.

4.3 The EU landscape

4.3.1 Moving from the DPD and the Framework Decision to the GDPR and LED

In May 2016 the data protection reform package was adopted, introducing the GDPR and the LED. As of 25 May 2018, the GDPR repealed the 1995 DPD and entered into force. The LED had to be transposed in Member States law by 6 May 2018. The decision was made to keep the AFSJ (the former third pillar) separate, although the EU is gradually involving itself over the years in data protection of personal data in

the police and justice sector.[636] The GDPR was drafted as a replacement instrument for the DPD and the LED was inserted as a new instrument for the AFSJ going beyond the scope of the data protection instruments existing in that sector at that time. The introduction of the LED is a significant change for the AFSJ. Before the introduction of the LED, data protection in this area was left mostly to national legislation, partly standardized by Convention 108 of the CoE, and to some extent regulated by a variety of specialist and sector specific instruments, creating a very fragmented landscape.[637] In addition, it can be argued that Convention 108 is too general to effectively safeguard protection of personal data in the law enforcement domain.[638] The LED repeals the Council FD[639], which was very narrow in scope, only applying to personal data that are or have been transmitted or made available between Member States.[640] Thus, it only applied to cross-border transfers and exchanges of personal data, excluding domestic processing of personal data.[641] In contrast, the LED applies to cross-border processing as well as processing in domestic situations. The LED still leaves discretion to the Member States as implementation of the provisions in national legislation is necessary; however, the introduction of a directive with such a broad scope already creates some harmonization. In addition, it can be argued that the LED raises the general data protection standards in the law enforcement area and it can be seen as an advantage that the LED is enforceable by national courts.[642] Nevertheless, as the regulation of the processing of personal data by national law enforcement agencies has not been completely harmonized so far, a wide margin is left to the criminal law of Member States to lay down requirements and safeguards. For data processing by national law enforcement agencies the LED therefore needs to be seen together with the safeguards and requirements following from Member States' legislation that arranges the competencies of these actors.

---

636 De Hert, Papakonstantinou & Riehle, Data protection in the third pillar: cautious pessimism, in: *Martin, Maik (ed.), Crime, Rights and the EU: cautious pessimism*. Justice, London (2008), p. 122.

637 P. De Hert & V. Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and analsyis', *Computers & Law Magazine of SCL* 2012, vol. 22, issue 6.

638 E. Kosta, F. Coudert, J. Dumortier, Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive, (2007) *International Review of Law Computers & Technology*, volume 21, no. 3, p. 348.

639 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, L 350/60.

640 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, L 350/60, article 1.2 (a).

641 T. Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security Review* 33 (2017) 324-340.

642 T. Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security Review* 33 (2017) 324-340.

The personal and material scope of the LED are defined in article 1 (1). The personal scope requires that a *"competent authority"* carries out the processing. The material scope requires that the *"processing is for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including safeguards against and the prevention of threats to public security"*. However, it can be argued that it is not always clear-cut when the LED applies instead of the GDPR.[643] First, the purpose of the processing could change. Sajfert and Quintel give the example of police officers processing personal data for identification purposes in the area of migration or border control where the crossing of the border could qualify as a criminal offence depending on the circumstances, changing the purpose from identification to prosecution of a criminal offence.[644] Second, there is confusion whether minor offences fall within the scope of the LED, Member States having different legislation determining whether minor offences are criminal offences or not.[645] Third, the lines between national security and law enforcement are blurring, especially in the context of information sharing between national intelligence agencies and law enforcement agencies.[646] To some extent this does not pose problems as some provisions of the GDPR are used as well in the LED. However, some chapters of the instruments differ significantly to accommodate for the nature of law enforcement activities, including the chapters on principles and rights of data subjects.[647] With regard to profiling, provisions on information rights and transparency are crucial and those differ significantly between the instruments.

Some scholars argue that law enforcement actors are given too much leeway, lowering the protection of data subjects compared to the rest of the public sector processing.[648] On the other hand it can also be acknowledged that the law enforcement sector is

643 See for example: Brewczyńska, M. (2022). A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation. *In: E. Kosta, R. Leenes, & I. Kamara (Eds.), Research handbook on EU data protection law* (pp. 91-114). (Research Handbooks in European Law series). Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781800371682.00013; Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), 162-176.

644 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

645 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

646 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019; Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), p. 165.

647 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

648 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

significantly different than the public sector operating under the GDPR, requiring a different instrument for this sector which contains more exemptions.[649] Especially in the context of information rights of data subjects, arguments of protecting the integrity and efficiency of police investigations are raised. If data subjects would be given the same information rights as under the GDPR, secret surveillance and certain evidence gathering would become difficult.[650]

In light of all this, the GDPR and LED will be discussed together in their regulation of profiling, as both instruments make use of the same definition of profiling and have similar provisions on profiling and automated decision-making. Most debates and literature on profiling concern the GDPR as this is the general instrument, so where the LED differs from the GDPR's approach to profiling, this will be discussed. With regard to the LED being a directive, national legislation needs to be taken into account, so provisions from the Dutch implementation of the LED will be discussed below where relevant. Given the scope of the LED, the LED is the relevant instrument of the two when it comes to risk profiling conducted by national law enforcement actors, such as police and the public prosecution. Therefore the LED provisions are discussed first, but the GDPR provisions and literature concerning them are used as well as illustrations, given the lively debate on profiling under the GDPR and given the limitations of the LED having to be seen in connection to national legislation.

The Article 29 Working Party, in its guidelines on automated decision-making and profiling under the GDPR, explained how profiling practices have become present in all sectors of society and how technological developments such as the development of AI have facilitated the creation of profiles and instances of automated decision-making, exposing individuals to risks such as a violation of their fundamental rights and freedoms.[651] Because automated decision-making and profiling can pose significant risks for individuals' rights and freedoms, appropriate safeguards were required. The Article 29 Working party in particular emphasized how automated decision-making and profiling can be opaque and individuals might not be aware they are subjected to these processes or knowledgeable of what these processes entail.[652] In addition, the Article 29 Working Party put forward that profiling can perpetuate stereotypes and

649 D. Alonso Blas, First Pillar and Third Pillar: Need for a Common Approach on Data Protection. In: S. *Gutwirth et al. (eds.), Reinventing Data Protection?* Springer 2009, p. 232.

650 D. Alonso Blas, First Pillar and Third Pillar: Need for a Common Approach on Data Protection. In: *S. Gutwirth et al. (eds.), Reinventing Data Protection?* Springer 2009, p. 232.

651 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017.

652 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017.

social segregation and lock people into a category.[653] The GDPR therefore introduces provisions, such as article 22, to address the risks for fundamental rights, mainly, but not limited to, the right to privacy.[654] According to the 2012 Commission proposal for the GDPR, article 22 builds on article 15 of the DPD and the CoE's Profiling Recommendation, adding modifications and additional safeguards.[655] Much of the same reasoning with regard to risks for fundamental rights and freedoms applies to the introduction of article 11 of the LED. Article 11 of the LED builds on its own predecessor, article 7 of the Council FD. While Article 22 of the GDPR builds on article 15 DPD, as Brkan rightly states, the practical importance of such a provision has much increased.[656] Whether the GDPR and LED are better equipped than their predecessors to safeguard against the risks of automated decision-making and profiling will depend also on other provisions, such as data subjects' rights, as will be discussed below. Following the evolution of article 22 GDPR, the provision originally focused on profiling and developed into a more general provision on automated decision-making.[657] Regarding the provision in question, the original Commission proposal spoke of the data subject's right not to be subject to 'a measure based on profiling'.[658] Originally, the provision thus focused on profiling, not necessarily on automated decision-making in general. This early draft of the provision is more similar to article 15 DPD, which also seemed to focus mostly on automated decision-making linked to profiling.[659] In the draft version of the GDPR provision there was also an obligation to inform the data subject about the existence of automated processing as well as

653 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017.

654 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017.

655 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final - 2012/0011 (COD).

656 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi: 10.1093/ijlit/eay017, p. 95-96.

657 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi: 10.1093/ijlit/eay017, p. 96.

658 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final 2012/0011 (COD), Brussels, 25 January 2012.

659 For more on this point see: Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121, doi: 10.1093/ijlit/eay017, p. 95-96.

concerning the envisaged effects for the data subject.[660] As will be discussed below, in the final version additional information rights were added which covered such obligations. The information obligations were removed from the provision on profiling itself. In the first reading of the Council, the focus on profiling was replaced by a focus on individual automated decision-making, including profiling.[661]

Comparing the LED and GDPR in their regulation of profiling to the CoE landscape, it is clear that there are similarities between the EU and CoE frameworks, but profiling is not viewed and regulated exactly the same. In that regard the Article 29 Working Party emphasized that the GDPR (and LED) concept of profiling was inspired by the CoE Profiling Recommendation, but is actually broader in scope than the latter.[662] The CoE Profiling Recommendation, as discussed in section 2.4, excludes processing that does not include inference, while for the LED and GDPR inference is not an explicit requirement for the specific provisions for profiling to apply.

4.3.2 The data protection principles under the LED & profiling

While article 11 LED and 22 GDPR are leading in determining the regulation of profiling, it is clear that these provisions cannot be viewed in isolation. As explained with regard to the scope of both provisions, there will be instances of profiling not covered by the provisions on automated decision-making, thus the other provisions of the LED or the GDPR are all the more relevant there. The Article 29 Working Party illustrated this importance of the entire instrument for the profiling process:

> *"The GDPR does not just focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals".*[663]

---

660 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final 2012/0011 (COD), Brussels, 25 January 2012; See also Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121, doi: 10.1093/ijlit/eay017, p. 96.

661 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final 2012/0011 (COD), Brussels, 25 January 2012; See also Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121, doi: 10.1093/ijlit/eay017, p. 96.

662 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017, p. 7.

663 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017.

In addition, it should be kept in mind that an important aspect of both the LED and the GDPR is that all the principles and rights and obligations work together, the provision on automated decision-making and profiling cannot be seen as standing alone. The strength of both instruments lies in the general processing principles that are complemented by more detailed provisions such as the provisions on automated decision-making and the various rights of data subjects. As a consequence, almost all of the provisions of the LED have some significance to profiling and automated decision-making, ranging from the data protection principles to data subject rights, to requirements such as data protection impact assessments and data protection by design and by default. As the data protection principles always apply to all personal data processing under the LED, it is good to briefly assess here what their specific value is when it comes to profiling. The Article 29 Working Party also discussed the data protection principles in their application to profiling.[664] While their guidelines concerned profiling under the GDPR, most of the considerations apply to the LED as well.

Article 4 of the LED contains the general processing principles, which are: lawfulness and fairness (paragraph 1), purpose limitation (paragraph 2), data minimization (paragraph 3), accuracy (paragraph 4), storage limitation (paragraph 5), data security (paragraph 6). When it comes to profiling all of these play a specific role.

The principle of lawfulness and fairness plays a role in multiple ways. First of all, lawfulness requires that there is a legal basis for the profiling process. In the case of law enforcement profiling this will be a specific legal basis, for example in national criminal law. Article 8 of the LED determines that processing will only be lawful if it is necessary for the performance of a task carried out by a competent authority for the purposes set out in article 1(1) LED and that it is based on Union or Member State law, the law in question specifying at least the objectives of processing, the personal data to be processed and the purposes of the processing.

The element of fairness is a crucial aspect when it comes to profiling.[665] The specific safeguards and prohibitions for profiling found in article 11 LED can be viewed as an instance of fairness requirements, such as the right to obtain human intervention, the prohibition on the use of special categories of data, and the considerations of the impact of (group) profiles on the individual. Profiling and automated decision-making have particular risks from a fairness perspective, most predominantly in terms of

664 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017, see pages 9-12.

665 See for example: Zarsky, T. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision-making. Science, *Technology, & Human Values*, 41(1), 118-132.

discrimination, as profiling is a practice inherently reliant on classification or scoring and focuses on group characteristics.[666] The Article 29 Working Party gave the example of profiling being unfair or discriminatory in excluding people or denying them access or targeting them in a negative way.[667] Still, fairness should not be equated completely with the principle of non-discrimination: there is non-discrimination law specially equipped to deal with such issues, and data protection law does not have to cover all possibly relevant issues.[668] The principle of fairness and what it means for profiling is further detailed in article 11 LED and further discussed in section 4.3.3.

It is important to realize that in contrast to the GDPR, the LED does not contain the principle of transparency under the heading of lawfulness and fairness.[669] I would argue that for profiling this lack of a transparency principle could be a crucial gap, because traditionally, fairness and transparency have been seen as strongly connected principles in data protection.[670] In order to achieve fairness, some transparency is required so that data subjects can make decisions relating to their personal data:[671] transparency facilitates crucial information to counter power- or information asymmetries.[672] Thus it can be difficult to achieve fairness of processing without providing transparency. This is all the more a difficult issue because profiling tends to be an inherently opaque process. The Article 29 Working Party also underlined the importance of transparency when it comes to profiling in two ways: first of all, they address the fact that often data subjects do not know they are being profiled. An important contributing factor to that is that the profiling process depends on creating 'new' data, derived or inferred about individuals, that has not been provided directly by the data subjects themselves. Secondly, transparency is a problem in understanding the often complex techniques and processes of profiling.[673] Some authors also propose

---

666 See for example: Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Wash. L. Rev.*, 89, 1.

667 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017, p. 10.

668 See also: E.J. Koops, The trouble with European data protection law, *International Data Privacy Law*, Volume 4, Issue 4, November 2014, available at: https://doi.org/10.1093/idpl/ipu023, p. 253.

669 For more on the implications of a missing principle of transparency see: Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework', *Computer Law & Security Review*, Vol 33, No 3, 2017, pp. 324-340.

670 For an elaborate discussion, see: D. Clifford, J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Volume 37, 2018, Pages 130–187, https://doi.org/10.1093/yel/yey004.

671 D. Clifford, J. Ausloos, Data Protection and the Role of Fairness, *Yearbook of European Law*, Volume 37, 2018, available at: https://doi.org/10.1093/yel/yey004, p. 140.

672 Zuiderveen Borgesius, F. (2015). *Improving privacy protection in the area of behavioural targeting*. PhD thesis, Faculty of Law (FdR), Institute for Information Law (IViR). Available at SSRN 2654213, p. 150.

673 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017, p. 9.

that the absence of a transparency principle can conflict with the EctHR case law.[674] To what extent there is still transparency provided for profiling elsewhere under the LED will be discussed in section 4.3.4 on data subject rights.

The purpose limitation principle also plays a crucial role for profiling. One often heard criticism in processes that rely on large volumes of data is that the purpose limitation is thrown out the window, as there is an appeal in collecting as much data as possible and determining its value or use only later.[675] Defining a specific pre-determined purpose can be especially difficult with profiling involving machine learning or other more complex algorithmic structures, as it may be difficult to reconcile dynamic processes with purposes that are specified narrowly in advance.[676] However, at the same time it can be argued that this is an exaggeration, since collecting as much data as possible without any goal is also not efficient from a law enforcement perspective. It can also be pointed out that there are questions on how narrowly defined a purpose should be under the LED: the LED itself does not provide guidance on how to distinguish between different law enforcement purposes. Nor can a processing activity be established solely by the mention of one of the LED purposes; the legality of the purpose also depends on the circumstances under which it is pursued.[677] Obviously this is an ambiguity that transcends profiling but applies to all processing under the LED.

There can be some criticism on the part of purpose compatibility within purpose limitation, looking at paragraph 2 of article 4 LED[678], which states:

---

674 Vogiatzoglou, P., Marquenie, T. 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 33.

675 V. Mayer-Schönberger and Y. Padova 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation' (2016) 17 *The Columbia Science and Technology Law Review* 315, 317; Axel Voss and Yann Padova, 'We need to make big data into an opportunity for Europe' (Euractiv, 25 June 2015) available at: https://www.euractiv.com/section/digital/opinion/we-need-to-make-big-data-into-an-opportunityfor-europe; L. Moerel and C. Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (25 May 2016) 2, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123.

676 C. Kuner, D. Jerker B. Svantesson, F. H. Cate, O. Lynskey, and C. Millard, Machine learning with personal data: is data protection law smart enough to meet the challenge? *International Data Privacy Law*, 2017, Vol. 7, No. 1, p. 1.

677 Vogiatzoglou, Plixavra; Marquenie, Thomas; 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 34.

678 See for example also F. Coudert, "The Directive for data protection in the police and justice sectors: towards better data protection?", April 2016, via: https://www.law.kuleuven.be/citip/blog/the-directive-for-data-protection-in-the-police-and-justice-sectors-towards-better-data-protection/.

> *"Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:*
>
> *(a) the controller is authorized to process such personal data for such a purpose in accordance with Union or Member State law; and*
>
> *(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law."*

Especially the vague formulation of (a) leaves it open to interpretation whether law enforcement actors can then use data collected for an entirely different purpose to construct profiles, if the construction of such profiles simply falls within their mandate under member states' law. At the same time, in the requirement of purpose limitation one can also find a requirement of proportionality,[679] limiting profiling from being a mass, untargeted, practice. Proportionality through purpose limitation binds the data processing to what is suitable, necessary, and proportionate vis-à-vis its stated purposes, just like a measure interfering with the right to personal data has to comply with those requirements.[680] One example where this requirement can be seen clearly is in case law pertaining to data retention, where the CJEU ruled the EU data retention directive to be invalid because of it exceeding what is necessary and violating proportionality.[681] For profiling this is an important limitation: data that is not needed for a specific purpose cannot be collected simply for the reason that it might be used for some interesting unforeseen purpose later. As new correlations pop up, there can be an urge to re-use data for new purposes, but this is thus not allowed without limitation.

When discussing risk profiling in the law enforcement context, it is also important to realize that some data protection principles in the GDPR are regulated differently than those in the LED. As a consequence, for profiling sometimes the data protection principles are applicable in a different way for profiling under the LED compared to profiling under the GDPR. One such difference is in relation to the purpose limitation principle. The purpose limitation principle consists of two components: first, the requirement of purpose specification, to define a purpose in advance to the processing

---

679 See for example: L. Dalla Corte, On proportionality in the data protection jurisprudence of the CJEU, *International Data Privacy Law*, 2022, Vol. 12, No. 4, p. 260.

680 L. Dalla Corte, On proportionality in the data protection jurisprudence of the CJEU, *International Data Privacy Law*, 2022, Vol. 12, No. 4, p. 265.

681 Zuiderveen Borgesius, F. (2015). *Improving privacy protection in the area of behavioural targeting*. PhD thesis, Faculty of Law (FdR), Institute for Information Law (IViR). Available at SSRN 2654213, p. 143.

that is specific enough; second the requirement of purpose compatibility. Under the GDPR the latter is given shape by requiring that further processed of data must be done under a compatible purpose. The LED chooses a different approach in that it does not use the wording of 'further processing', but puts specific rules in place on changing of purpose in article 4(2) LED. The rule specified by the LED here is that 'subsequent processing by the same or another controller is permitted if authorized by law and if necessary and proportionate to the new purpose, as long as the new purpose remains within the scope of the Directive'.[682]

In data protection scholarship there are two different strands of opinion presented on the different rules of the LED and GDPR for repurposing data. On the one hand there are scholars such as Jasserand who criticize the LED for this different approach to purpose limitation in that it would derogate from article 8 CFREU and is lacking adequate data subject safeguards, mainly because the LED does not provide for a compatibility test when personal data are originally collected by private parties before being processed by law enforcement actors.[683] On the other hand there are scholars such as De Hert and Sajfert who argue that the LED does not offer less safeguards than the GDPR when it comes to purpose limitation. Their reasoning is that if personal data are originally collected in the private sector under the GDPR, once they are transmitted to a controller under the LED or used for one legal basis and next for another legal basis, the processing begins at step one again, triggering information rights and obligations.[684] There is perhaps a third view on this dilemma, seeing the arguments proposed by Vogiatzoglou and Marquenie, who argue that whether it is subsequent or further processing can be a matter of semantics, but ultimately compliance with article 8 of the CFREU should be respected and can guide the implementation and application of article 4(2) LED.[685] Thus, this means that it is unclear in practice whether the GDPR is stricter than the LED when it comes to purpose limitation, but perhaps the difference between the two is not as big as it might appear. There are rules for when personal data are processed for a different purpose, which is important for profiling as a minimum protection. How much margin there is for law enforcement actors will

---

682 De Hert, P., & Sajfert, J. (2021). The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680. Available at SSRN 4016491, p. 11.

683 See also: De Hert, P., & Sajfert, J. (2021). The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680. Available at SSRN 4016491, p. 11.

684 De Hert, P., & Sajfert, J. (2021). The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680. Available at SSRN 4016491, p. 11.

685 Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 35.

depend on the national law authorizing the processing and the interpretation of the criteria of "necessary and proportionate to the new purpose" in practice.

The principle of data minimization plays a similar role in the profiling process to that of purpose limitation. According to article 4(1)I LED, data minimization requires that only data are processed that are 'adequate, relevant and not excessive in relation to the purposes for which they are processed'. The wording of 'not excessive' implies that fishing expeditions, where as much data as possible are collected and filtering for necessity happens afterwards, are not allowed. The same could be said for the wording 'relevant'. Some scholars propose that equal to the principle of purpose limitation, the principle of data minimization is difficult to maintain in data-driven forms of profiling, where the focus on limiting of data collection would hinder the use of AI and innovation.[686] At the same time, from a more technical perspective it can be argued that more data is not always more useful. For example, in machine learning, simply using more data and focusing on quantity does not create better analysis or output.[687] However, at the same time the wording 'adequate' in article 4(1)(c) LED could imply that data should also be adequate to the purpose for which they are collected. That could mean an interpretation in a different direction, in that data should also be sufficient to be adequate: some have called this the idea of data *minimummization*, having a threshold of what is required as a minimum in data collection, analysis and storage.[688] I would argue, however, that providing the data that is necessary to complete an analysis is related to the principle of accuracy rather than adequacy, as discussed below.

For data minimization there is also a difference between the LED and GDPR that could be relevant for profiling. Where the GDPR phrases data minimization as 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed',[689] the LED chooses a different phrasing: 'adequate, relevant and not excessive in relation to the purposes for which they are processed'.[690] The key difference is that 'not excessive' in the LED seems less stringent than the necessity criterion of the GDPR. De Hert and Sajfert for example propose that under the GDPR controllers have to demonstrate that the data collected is absolutely necessary, while the LED

686 Finck, M., & Biega, A. J. (2021). Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. *Technology and Regulation*, 2021, p. 44-45.

687 Finck, M., & Biega, A. J. (2021). Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. Technology and Regulation, 2021, p. 45-46.

688 Van der Sloot, B. (2013). From data minimization to data minimummization. In: *Discrimination and Privacy in the Information Society*. Springer, Berlin, Heidelberg, 273-287.

689 Article 5(c) GDPR.

690 Article 4(1)(c) LED.

implies a much easier burden of proof for controllers.[691] De Hert and Sajfert also rightly point out that although the LED requires less precision than the GDPR on this point, this does not mean that law enforcement actors can collect unlimited data, as the LED data minimization principle ensures the same level of protection as under Convention 108+.[692] However, again similarly to the discussion on purpose limitation, the difference between the LED and GDPR on this point might not be so clear-cut or so big in practice; there are even those who argue that the LED data minimization principle should be interpreted in the same way as the GDPR one.[693]

The principle of data accuracy is specifically relevant for risk profiling in two ways. The first aspect is that data have to be accurate and kept up to date (article 4(1)(d) LED). This can be read as pertaining to the data that go into risk profiles, where each data point in itself has to be correct. The second aspect is about the profiles themselves. It can be argued that those also have to be accurate, focusing on the combination of individual data points that together also have to be accurate. This latter aspect is, however, not explicitly present and therefore less clear in article 4 LED. Whether the profile itself, as a combination of data, has to be accurate, depends on the question whether the profile is considered personal data.

The next principle is that of storage limitation, following from article 4(1)(e) LED. Putting a time limit on how long data can be kept in identifiable form also poses a limitation to unbridled growth of databases containing personal data. This provision should be read in connection to article 5 LED, which stipulates that Member State law has to provide for appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data.

---

691 De Hert, P., & Sajfert, J. (2021). The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680. Available at SSRN 4016491, p. 13.

692 "(…)*adequate, relevant and not excessive in relation to the purposes for which they are processed*", article 5(3)(c) Convention 108+; De Hert, P., & Sajfert, J. (2021). The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680. Available at SSRN 4016491, p. 14.

693 Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 36-37. See also: Article 29 Data Protection Working Party, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015, p. 7.

In addition to data protection principles, two other provisions of the LED placed before the specific provision on profiling have specific importance for profiling: article 6 and 7 LED. Article 6 LED requires for Member State law to provide that the controller makes a distinction between different categories of data subjects, such as suspects, offenders, witnesses and victims. Article 7 LED requires member state law to provide a distinction between data based on facts and data based on personal assessments. Both of these provisions are key to the law enforcement sector. Different safeguards and rights will for example apply when dealing with a victim versus a suspect of a crime. A lot of police data is based on reports of officers or witnesses, sometimes creating more of an assessment or hearsay than hard facts, which creates a certain error rate or probability. For that reason it is important that the LED distinguishes between these sources of information. However, it is important to place a critical note at the practical possibility to apply these two provisions in profiling. For article 6 LED, it can be difficult to maintain distinctions between different data subjects when profiling is such a fluid and dynamic process.[694] At an early stage a classification has to be made, which can be erroneous and required to change later on, especially given that also criminal investigations are fluid processes and not static, being based on a constant stream of new information.[695] There are also no guidelines in the LED what the consequences of such categorizations are for data subject rights, or how to deal with the fact that the categories are linked to different time limitations for storage and processing of the data.[696] Similarly, under article 7 LED, it might be difficult to assess what the line is between facts and personal assessment: is the risk profile considered factual or does the assessment using an algorithm constitute a personal assessment? Or more specifically, in which category do inferred data fall, are they fact or opinion? Inferences are not opinions, but at the same time they involve a layer of interpretation of facts, as they are characteristics derived from data analytics and not directly observable as facts.[697] At the same time, the question is what to do with data files that are partly opinion and partly facts. Since article 6 and 7 LED have to be further detailed in national law, this will be further discussed in chapter 6 when discussing Dutch criminal procedural law.

---

694 Leiser, M. and Custers, B., The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, *European Data Protection Law Review* 2019, Vol. 5, nr. 3, p. 376.

695 Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 39-41.

696 Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 39-41.

697 Leiser, M.R. and Custers, B.H.M. (2019) The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, *European Data Protection Law Review* 2019, Vol. 5, nr. 3, p. 377. See also: BHM Custers, 'Effects of Unreliable Group Profiling by Means of Data Mining' in: *G Grieser, Y Tanaka and A Yamamoto (eds), Lecture Notes in Artificial Intelligence*, Proceedings of the 6th International Conference on Discovery Science (DS 2003) Sapporo, Japan vol 2843 (Springer 2003) 290-295.

4.3.3 An exploration of article 11 LED

Profiling is defined under the LED as follows[698]:

> *'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural per'on's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*[699]

The Article 29 Working Party explained that this definition comprises of three elements: automated processing, personal data, and the objective e to evaluate personal aspects about a natural person.[700]

In the LED, profiling is regulated in article 11 on automated decision-making, which reads as follows:

> *Article –1 - Automated individual decision-making*
>
> 1. *Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unleuthorizedsed by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.*
>
> 2. *Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subj'ct's rights and freedoms and legitimate interests are in place.*
>
> 3. *Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.*

---

698 The Article 29 Working Party emphasizes in its Opinion on the Law Enforcement Directive that the concerns regarding profiling from Guidelines on automated decision-making and profiling pertaining to the GDPR are thus also relevant for profiling under the LED.

699 Article 3(4) LED & article 4(4) GDPR

700 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017; For an elaborate discussion of definitions of profiling, see chapter 2.

As explained before, much of the scholarly debate on profiling and automated decision-making has focused on the GDPR rather than the LED. While some of the core characteristics of the LED and GDPR approach to profiling are the same, there are also major differences. For that reason it is crucial to also present the relevant GDPR provision here and reflect on the differences between the two to complement the existing scholarly debates. In the GDPR, profiling is regulated explicitly in article 22 on automated decision-making, which reads:

> *Article 22 – Automated individual decision-making, including profiling*
>
> 1. *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*
>
> 2. *Paragraph 1 shall not apply if the decision:*
>
>   1. *is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
>
>   2. *uthorizedsed by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
>
>   3. *is based on the data subject's explicit consent.*
>
> 3. *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*
>
> 4. *Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

4.3.3.1 The scope

The first question these provisions raise is what type of risk profiling falls within the scope of article 11 LED. Article 11 LED talks about automated individual decision-

making 'including profiling', meaning that automated decision-making can be part of a profiling process. Similarly to profiling under the DPD, the wording does not exclude profiling that does not involve automated decision-making, nor does it exclude automated decision-making that occurs without profiling. The Article 29 Working Party confirmed this, for example in its opinion about the LED:

> *"Although profiling and automated decision-making can be combined activities of the same process, they can also be carried out separately. There may be cases of automated decisions made with (or without) profiling and profiling which may take place without making automated decisions. Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition."*[701]

Comparing the scope of article 15 DPD to that of article 11 LED and article 22 GDPR, the DPD focused on automated decision-making that was part of profiling; in contrast, the formulation of the LED and the GDPR covers a wider spectrum of automated decision-making. However, regardless of the broader formulation, it can be questioned to what extent these new provisions truly cover automated decisions that are not based on profiling. I agree with scholars such as Brkan here that decisions based solely on automated processing are usually based on profiles or profiling. It is difficult to imagine situations where all criteria apply, such as a fully automated process and the processing of personal data, but no profiling would be involved.[702] Vice versa, this does not mean that all profiling will lead to an automated decision: the decision, especially in the law enforcement context, can include a level of involvement of a human decision maker. Thus, one can conclude that at least profiling that results in an automated decision will be covered by these provisions.

The remaining question is then which (other) parts of profiling are covered by the LED and GDPR and by which provisions. While articles 11 LED and article 22 GDPR focus on the automated decision, the preceding part of the profiling process that uses personal data and some level of automation will be covered by other provisions, such as the main principles of data protection, which I discussed in the previous section. The Article 29 Working Party made this scope very clear:

---

701 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

702 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi: 10.1093/ijlit/eay017, p. 97.

> *"The GDPR does not just focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals."*[703]

Sajfert and Quintel argue that different types of profiling might be covered by different regimes, as article 11 LED only deals with decision-making *solely* based on automated means.[704] Following this logic, indeed some parts of profiling will fall under the LED provision on automated decision-making, and some profiling will only be regulated through other provisions such as the general data protection principles, for example fair and lawful processing. This is not surprising, keeping in mind that article 11 LED and article 22 GDPR are meant specifically to counter the harmful effects of purely automated decisions that have a big impact on individuals. In that sense, these articles are an extra safeguard on top of the other principles and rights from both instruments. The key factor is whether there is human involvement or not:[705] the lack of any human involvement in a process needs to be compensated for through extra safeguards.

It is also important to notice what type of provision article 11 LED and article 22 GDPR are, since there is a difference here: article 11 LED is placed in the chapter of 'principles' and is phrased as a prohibition on automated decision-making, while article 22 GDPR is placed in the chapter of data subject 'rights' and is phrased as a right rather than a prohibition. Consequently, data subjects under the GDPR would have to assert their right procedurally.[706] It can be questioned however to what extent the seemingly stringent phrasing of the LED as a prohibition of automated decision-making actually is that much of a prohibition in practice and would be more stringent than the GDPR. First of all, the Article 29 Working Party, in their guidelines on automated decision-making under the GDPR, consistently spoke of the prohibition on automated decision-making and profiling defined in article 22(1),[707] clarifying that article 22 GDPR should be interpreted as a prohibition rather than a right data subjects have to assert themselves.[708] This recommendation to interpret the article 22 GDPR as

---

703 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017, p. 6-8.

704 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

705 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017, p. 8.

706 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

707 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017.

708 More specifically: "This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data", page 19 of the Guidelines.

a prohibition stemmed from the idea that otherwise this provision would offer less protection than its counterpart under the LED. [709] It is a useful consideration given the nature of profiling, which can be opaque, but also considering that profiling and automated decision-making are increasingly frequently used in crucial decisions, and it would pose a risk to data subjects' interests if they constantly have to invoke a right to receive protection.[710] Thus the phrasing of a prohibition can be welcomed from the perspective of protecting data subjects' fundamental rights. However, the prohibition of article 11 LED is subject to numerous limitations, some overlapping with limitations to article 22 GDPR, some being extra limitations on top of those.[711] These limitations, which will be discussed in the continuation of this section, place question marks as to the effectiveness of the prohibition on profiling.

Apart from the presence of automated decision-making, there are specific elements of both article 11 LED and article 22 GDPR that determine the applicability and scope of these and other provisions. One can distinguish five elements here: the requirement of solely automated processing, the requirement of individual decisions, the requirement of (adverse) legal effects or similar effects, the requirement for the legal basis, and the extra requirements connected to special categories of data and discrimination. These five aspects of both provisions are discussed below, step by step. In these steps the limitations of article 11 LED as a prohibition and the possible criticism on this provision will become more clear.

4.3.3.2 Solely automated processing

An important boundary marker for the scope of both article 11 LED and article 22 GDPR is that the decision is based solely on automated processing. The Article 29 Working Party clarified that this refers to the ability to make decisions by technological means without human involvement in the decision-making process.[712] Article 15 DPD used the exact same wording here, so this is nothing new. Nonetheless, as this was a point of

---

709 Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), p. 173.

710 See also Kaminski, Margot E., The Right to Explanation, Explained. U of Colorado Law Legal Studies Research Paper No. 18-24, *Berkeley Technology Law Journal*, Vol. 34, No. 1, 2019, Available at SSRN: https://ssrn.com/abstract=3196985, p. 4; Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), p. 173.

711 Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 50; See also: González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.

712 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

discussion under the DPD, it is still debated in the age of the LED and the GDPR how to interpret this criterion.

Wachter et al. deem the criterion problematic, as it would open up a loophole whereby any form of human involvement in the decision-making process could mean it is no longer automated decision-making and therefore outside the scope of article 22 GDPR or article 11 LED.[713] Wachter et al. interpret the criterion of 'solely' to mean that even some nominal human involvement may be sufficient to escape the requirement. More particularly, they wonder whether the use of automated processing for the preparation of a decision that is acted upon by a human is still a decision based on automated processing, if the human does not interfere, verify, or modify the decision or decision-making rationale.[714] A narrow interpretation of the requirement of 'solely' would then mean that decisions that are predominantly based on an automated process but with nominal human involvement would not receive the protection of the right of access under article 15(1)h GDPR, nor the safeguards against automated decision-making of article 22(3) GDPR.[715] Wachter et al. find further evidence for their narrow reading of the term 'solely' in the fact that the European Parliament proposed amendments to the GDPR text adding that it should constitute decisions solely or 'predominantly' based on automated processing; significantly, this broadening of the scope beyond 'solely' never made it to the final version of the GDPR, which only contains the term 'solely'.[716] However, in contrast to this narrow reading of 'solely' by Wachter et al., Bygrave, as well as Selbst and Powles argue that a different or more relative notion of 'solely' is required for the provision to be meaningful.[717] I agree that a broader understanding of solely is required to attribute meaningful protection to article 11 LED and article 22 GDPR, to distinguish between decisions with human assessment or application and decisions made by computerized systems. If the humans who have to ultimately apply the decision are so biased or steered by the automated system that they do not really make their own decision, intentionally or unintentionally, important safeguards would

---

713 S Wachter, B Mittelstadt, and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *IDPL* 76, p. 92. For this argument Wachter et al. also rely on previous works by Hildebrandt and Bygrave.

714 S Wachter, B Mittelstadt, and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *IDPL* 76, p. 92.

715 S Wachter, B Mittelstadt, and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *IDPL* 76, p. 92.

716 S Wachter, B Mittelstadt, and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *IDPL* 76, p. 92.

717 L.A. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 *Computer Law & Security Review* 17; Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 235.

be disregarded. The Article 29 Working Party seemed to support such a reading where human involvement needs to be more than nominal, as it states in the guidelines on automated decision-making:

> *"The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data."*[718]

With risk profiling systems, currently some systems are not that far advanced and still described as decision-support systems, especially those that have a potentially significant impact, at least as far as is publicly known.[719] Edwards and Veale, for example, think many decisions made with these type of systems, such as algorithmic risk assessment in criminal justice, will not fall within the scope of protection against automated decision-making due to there being human involvement.[720] As an example they take COMPAS, which in their opinion shows problematic bias but is at least nominally advisory.[721] Other similar examples are the UK HART tool, which provides automated recommendations on offenders' rehabilitation prospects[722], or the Dutch tool OxRec,[723] which provides automated risk assessment for recommendations on probation decisions. Bygrave similarly states that when the system functions as decisional support, so when there is a human in the loop, article 22 GDPR is irrelevant. The few court cases on article 22 GDPR and its predecessors have tended to result in findings that the decisional system

---

718 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017, p. 21.

719 See for example chapter 2, section 2.5.

720 Edwards L., and Veale, M., "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1, p. 45.

721 Edwards, L., and Veale, M., "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1, p. 45.

722 Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 50; Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), p. 174.

723 M. de Vries, J. Bijlsma, A.R. Mackor, F. Bex, and G. Meynen. "AI-risicotaxatie: nieuwe kansen en risico's voor statistische voorspellingen van recidive." *Strafblad* 2021, no. 2 (2021): 58-66.

is not fully automated.[724] Therefore, even with a broader reading of "fully automated" that includes nominal but not meaningful human involvement, it can be questioned to what extent in practice risk profiling systems in the law enforcement sector will be seen as fully automated and falling within the scope of article 11 LED. A case by case assessment would be necessary with information about the actual involvement of humans in the loop and to what extent they determine the use of the outcomes of the analysis. In addition, the criterion will depend on national transpositions of article 11 LED.[725] Matters are further complicated by the complex processing situations in reality: Binns and Veale rightfully point out that profiling processes in practice often have multiple stages, potentially both manual and automated, which poses problems for the application of article 11 LED and article 22 GDPR.[726]

4.3.3.3 Individual decisions

The headings of article 11 LED and article 22 GDPR make clear that both provisions apply only to decisions about individuals. The text of the provisions further emphasizes this by mentioning the data subject in singular form. Already the scope of the LED and GDPR of applying only to the processing of personal data and the focus on identifiable natural persons demonstrates that these instruments are tailored to the individual dimension. Over the years, there have been increasingly more discussions about this strong individual dimension of data protection legislation at the expense of attention for the group or collective dimension.[727] This point of criticism on instruments such as the LED becomes painfully clear in connection to profiling. While the protection offered by data protection, such as article 11 LED, focuses on the individual, algorithmic harms in profiling arise from how systems classify groups or compare individuals, creating a mismatch between profiling practices and the legal safeguards. Some scholars argue that this issue with groups versus individuals has been an issue in data protection and

---

724 L.A. Bygrave, Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions. University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2020-35. [Version 1.1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (forthcoming)].

725 Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office, p. 52.

726 Binns, R. and Veale, M., 'Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR', *International Data Privacy Law*, Vol. 11, No. 4, 2021.

727 For the field of data protection, see the works of Alessandro Mantelero, most notably: A. Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, *Computer Law & Security Review*, Volume 32, Issue 2, 2016, pages 238-255, available at: https://doi.org/10.1016/j.clsr.2016.01.014. For a broader discussion see: Taylor, Linnet, Luciano Floridi, and Bart van der Sloot, eds. *Group privacy: New challenges of data technologies*. Vol. 126. Springer, 2016.

privacy legislation for some time[728] and that it remains underexplored in the context of automated decision-making and explanations.[729] The creation of groups and categories of individuals for the purposes of creating or applying profiles means that profiling practices or decision-making can have risks or harmful effects that go beyond the individual or are not even applicable to the individual level. This concern also applies to automated decision-making, where scenarios are possible in which a decision has an effect that goes beyond the individual, which implies that article 11 LED does not apply to the situation or the provision only applies to one individual while the actual scope of the decision is much broader. Collective decisions affecting multiple individuals or groups can for example be based on the shared characteristic of living in a certain area, such as automated decisions taken by the police to increase police surveillance in a certain geographical area, affecting all data subjects living there.[730]

The use of profiles also means that information about categories or groups becomes the most prominent data, sometimes more so than personal data of an individual. As Edwards and Veale explain, profiles can be seen as belonging to a group rather than to an individual.[731] The merit of the use of profiles is not so much the identification of characteristics of individuals but rather the contrast with other individuals in the dataset.[732] Using a simplistic example to illustrate this: an individual who has committed a string of burglaries is more likely to commit another burglary than someone who has a record of traffic violations. In a more interesting and complicated scenario, the knowledge that is interesting, in the case of law enforcement risk profiling, is what makes an individual more likely to commit a certain type of crime compared to others, more so than identifying the individual characteristics of a person. Mittelstadt talks of algorithmically assembled groups, to which data protection (and privacy) legislation would not be attuned, since the focus of legislation is on the individual. In algorithmically assembled groups, individuals are linked through patterns and correlations based on behaviour, preferences and other characteristics using offline identifiers (e.g. age,

728 P. De Hert & V. Papakonstantinou, Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review* 40 (2021); L. Taylor, L. Floridi & B. van der Sloot (eds), *Group Privacy. New challenges of data technologies*, Philosophical Studies series, vol 126, Springer, 2017, p. 238.

729 Edwards L., and Veale, M., "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1, p. 22.

730 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi: 10.1093/ijlit/eay017, p. 100.

731 Edwards L., and Veale, M., "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1, p. 35-36.

732 Edwards L., and Veale, M., "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1, p. 35-36.

ethnicity, geographical location) and new behavioural identity tokens, allowing for predictions and decisions to be taken at a group level.[733] Examples of the latter could be in very generic terms, the decision to patrol a neighborhood or zipcode area based on a risk profile of residents of that area, or the application of a risk profile to a criminal organization resulting in investigative measures against that group. The provisions on profiling under the LED and GDPR are thus limited in scope in that they only protect against automated decision-making about a specific individual.

In addition to this limitation in *ratione personae*, a possible threshold can also be found in the requirement of processing personal data. Decisional systems not involving the processing of personal data but focusing on the aggregate or the group could fall outside of the scope[734], as already briefly mentioned in the introduction to this chapter. Hildebrandt argues that even if a profile itself becomes personal data once it is applied to an individual, this still does not offer protection to the group and group profile in question.[735] Following this line of reasoning, neither article 11 LED nor article 22 GDPR covers a decision impacting only groups, or a collective decision. Edwards and Veale reason that excluding collective automated decisions from the scope of protection creates an imbalance in how individual and collective automated decisions are treated and could open the door to circumvent the prohibition of individual automated decisions by adopting collective decisions. Therefore, they propose to consider a collective or group decision as a bundle of individual decisions.[736] This would however direct the protection to individuals still, focusing on individual harm. So it can be questioned whether such an approach would solve all problems around individual decision-making as the scope of protection. It solves part of the problem, but still does not say anything about how to treat situations where the problem is not so much the (individual) decision, but the underlying group profile itself. Perhaps a

---

733 Mittelstadt, B. From Individual to Group Privacy in Big Data Analytics. *Philos. Technol.* 30, 475–494 (2017). https://doi.org/10.1007/s13347-017-0253-7, p. 476.

734 L.A. Bygrave, Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions. University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2020-35. [Version 1.1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (forthcoming)]; See further e.g. Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer law & security review*, 32(2), 238-255; Mittelstadt, B. (2017). From individual to group privacy in big data analytics. *Philosophy & Technology*, 30(4), 475-494.

735 See M. Hildebrandt, *Smart technologies and the end(s) of law: novel entanglements of law and technology* (Edward Elgar 2015); L. Edwards, Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective, 1 *EUR. DATA PROT. L. REV.* 28, 28–58 (2016).

736 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi: 10.1093/ijlit/eay017, p. 100-101.

scenario where the decision only has an effect on the group and not on the individuals comprising that group is still very much a fictional one. At the same time, that is not to say that the existence of the group profile rather than the decision itself, cannot have a significant effect, for example in terms of fairness or discrimination. Thus, I would argue, based on all of the above arguments, that while article 11 LED and article 22 GDPR are provisions supposedly offering safeguards for profiling, the provisions neglect to acknowledge the inherent nature of profiling, namely the importance of groups and aggregated data.

4.3.3.4 Legal effects or similar effects

Another requirement for article 11 LED or article 22 GDPR to apply is the effect of the decision. The GDPR speaks of 'legal effects' of the decision concerning the data subject or a decision that 'similarly significantly' affects the data subject; the LED follows this wording partially but specifically speaks of an 'adverse' legal effect or a significant effect. The LED does not require the significant effect to be similar to a legal effect, as under the GDPR.[737] Compared to article 15 DPD, Mendoza and Bygrave put forward that the DPD did not draw a link between significant consequences ('significantly affects') and 'legal effects', while article 22 GDPR does draw this link by inserting 'similar' before 'significant consequences'.[738] According to Mendoza and Bygrave this could mean that such consequences must have a non-trivial impact on the 'status of a person relative to other persons', which is what legal effects usually entail.[739] In its Opinion on the LED, the Article 29 Working Party provided the example of a typical adverse legal effect being the application of increased security measures or surveillance by the competent authorities and a significant effect being the case where a passenger is not allowed on board because they are registered on a black list.[740] The addition of the term 'significant' on the one hand opens up the scope beyond adverse legal effects but is also intended to exclude trivial effects: the effect should be substantial enough to influence the individual's situation.[741] In this sense it can be argued that the language of the

---

737 J., Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

738 I. Mendoza and L.A. Bygrave, The Right not to be Subject to Automated Decisions based on Profiling, University of Oslo Faculty of Law Legal Studies Research Paper Series, No. 2017-20, p. 12.

739 I. Mendoza and L.A. Bygrave, The Right not to be Subject to Automated Decisions based on Profiling, University of Oslo Faculty of Law Legal Studies Research Paper Series, No. 2017-20, p. 12.

740 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258, p. 12.

741 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258, p. 12.

LED on the effects is clearer and offers stronger protection to individuals compared to article 22 GDPR.[742]

However, in my opinion, whether there is truly a difference in practice remains to be seen. Brkan argues that based on the Article 29 Working Party guidelines on automated decision-making, 'similarly' in article 22 GDPR refers to the significance of the effect and not to the nature of the effect.[743] Following this reasoning, the similar significant effect should not be linked to the legal dimension but rather take it to mean a non-trivial effect. The same applies to the lack of the term 'adverse' in the GDPR provision: it makes sense to interpret article 22 GDPR to mean an adverse effect as well: a data subject would not require protection against an automated decision if it did not have at least a partially adverse effect. A decision falling under the scope of article 22 GDPR can have both positive and negative aspects for the data subject; it does not need to be entirely adverse for the person, but the more adverse the effects are, the greater the chance they may properly be deemed significant in the sense of this provision.[744] In the end, therefore, article 11 LED and article 22 GDPR can both be interpreted as referring to decisions that significantly affect individuals (legally or otherwise) in a way that is (also) negative for them.

4.3.3.5 Legal basis & exceptions

Both the LED and GDPR provision provide for Member State law to make exceptions. The prohibition of article 11 LED does not apply if such an automated decision is authorized by Union law or a Member State law that provides suitable safeguards for the rights and freedoms of data subjects.[745] It is thus up to Member States to authorize and enable fully automated decision-making in law enforcement matters. This approach can be criticized, as Member States can enact legislation legitimizing the reliance by law enforcement authorities on fully automated decision-making to make systemic and individualized predictions and classifications, severely minimizing the protective character of the prohibition on automated decision-making including profiling.[746] The Article 29 Working Party explained that due to the nature of law enforcement activities,

---

742 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

743 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121, doi: 10.1093/ijlit/eay017, p. 102.

744 I. Mendoza and L.A. Bygrave, The Right not to be Subject to Automated Decisions based on Profiling, University of Oslo Faculty of Law Legal Studies Research Paper Series, No. 2017-20, p. 12.

745 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

746 Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), p. 173.

the LED naturally does not contain the same exceptions as the GDPR.[747] Under the GDPR there are additional exceptions for processing necessary for the performance of or entering into a contract[748] and processing based on the data subject's explicit consent[749]. While there are more varied exceptions under the GDPR to allow automated decision-making than under the LED, the GDPR at the same time provides for a wider array of safeguards for individuals[750], as will be discussed below and in section 4.3.4.

In creating an authorization for such automated decision-making as under article 11 LED, in Member States' legislation appropriate safeguards must be provided, at least the right to obtain human intervention on the part of the controller. The Article 29 Working Party emphasized that although article 11 LED only refers to the right to human intervention and not to a right of data subjects to express their point of view and to contest the decision as is the case under article 22 GDPR, it should be noted that recital 38 of the LED states that processing under article 11 LED should be subject to suitable safeguards. Recital 38 mentions not only the right to obtain human intervention, but also 'in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision'.[751] In this way, it seems that the legislator aimed to close the gap in safeguards and rights between article 22 GDPR and 11 LED. However, Sajfert and Quintel rightly note that including this in a non-binding recital, together with the instrument being a Directive that requires transposition into Member State law, has possibly little effect and cannot be compared to article 15(h) GDPR.[752] It is worrying that the LED in this way leaves it up to Member States whether they allow contestation of automated decision-making, as states may choose not to regulate it and not provide such a procedural right. If Member States do not implement this possibility, data subjects will need to turn to the supervisory authority or court to challenge an automated decision. Brkan proposes that the data subject can attempt to contest the decision when requesting human intervention with the competent authority, but that the authority obviously does not have a distinct obligation to address this contestation.[753]

747 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

748 Article 22 (2)a GDPR.

749 Article 22 (2)b GDPR.

750 Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), p. 173.

751 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

752 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

753 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi: 10.1093/ijlit/eay017, p. 109.

On the importance of human intervention as a minimum safeguard, the Article 29 Working Party stated that human intervention allows the data subject not to be submitted to indecipherable automated decisions that may suffer from errors or bias, and that human intervention allows the data subject to have an exchange with the controller also on contestations the data subject may want to raise.[754] The Article 29 Working Party emphasized that in order for the data subject to benefit from these safeguards, the human intervention has to be 'carried out by someone who has the appropriate authority and capability to change the decision and who will review all the relevant data including the additional elements provided by the data subject'.[755] This is easier said than done: the question to what extent human intervention actually entails a serious measure is difficult to answer in practice. There are various practical factors that can impede serious intervention by a human decision-maker. One is automation bias, through which the human decision maker is already influenced or biased by the decision outcome proposed by the system.[756] This can be a subconscious effect, but the human involved in the process can also consciously choose not to diverge from or modify the decision from the automated analysis because of a fear for accountability on their part.[757] In this way, automation bias and the opacity of profiling systems blur the lines between automated decision-making and systems assisting in decision-making.[758] A second factor is that it remains unclear how a human with limited capacities of data analysis, compared to an automated system, can come to their own conclusion regarding a complex and multifaceted decision. The human decision maker can have an extremely difficult task in reviewing such a decision, no matter how willing they are to do so.[759]

De Hert and Lammerant argue that for profiling there is a duty of care for states in decision-making in administrative law. From that perspective they argue that automation bias can violate this duty of care, as exaggerated trust in computers would run counter to that duty of care. An example of such a duty of care vis-à-vis

---

754 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

755 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

756 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change 41*, no. 3 (2017):327-366. See chapter 3, section 3.8.1. for more on this.

757 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi:10.1093/ijlit/eay017, p. 108.

758 Lammerant, H., & De Hert, P. (2016). Predictive profiling and its legal limits: Effectiveness gone forever. In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, p. 166-167; See also: Citron, D.K. (2008) 'Technological Due Process', *Washington University Law Review* 85: 1249-1313.

759 Brkan, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. doi:10.1093/ijlit/eay017, p. 108.

governmental profiling and automation can be found in the *Commission of the European Communities v Kingdom of Spain* judgment by the CJEU, which concerned a refusal of entry into the Schengen area based on flagging in the SIS system.[760] De Hert and Lammerant point out that the CJEU argued there that a refusal without preliminary verification of whether the person presented an actual danger violated EU law, and thus the decision makers had a duty of care towards their computer-assisted decision-making system.[761] Based on the prominent work on automation and due process by Citron[762], De Hert and Lammerant subsequently give examples of proper safeguards such as including audit trails on rules applied and the data considered, explanations by decision-makers how they relied on computer-generated information, along with training to critically evaluate information and combat automation bias.[763] Here it becomes clear that data subject rights on information and explanation -which will be further discussed in section 4.3.4- have an important role to play when it comes to offering appropriate safeguards for profiling and automated decision-making to counter negative implications of automation.

4.3.3.6 Special categories of data

A last point to consider when discussing the requirements of article 11 LED is the use of special categories of data or sensitive data. In profiling this is especially important to assess in connection to the serious risk of discrimination. Article 22(4) GDPR states that automated decision-making cannot be based on special categories of data, unless there is consent from the data subject as laid out in article 9 (2)(a) GDPR or unless processing is necessary for reasons of substantial public interest following the requirements of article 9(2)(g) GDPR, and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. Article 11(2) LED states that automated decision-making cannot be based on special categories of data unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. In addition, Article 11(3) LED states that profiling that results in discrimination on the basis of special categories of data is prohibited as this is a violation of EU law. The Article 29 Working Party in its opinion on the LED recognized that due to the nature of the data processed there and the risks of discrimination of automated systems, Member States in their implementation legislation must provide strict safeguards for individuals' rights. Furthermore,

---

760 Judgment of the Court (Grand Chamber) of 31 January 2006, *Commission of the European Communities v Kingdom of Spain*, ECLI:EU:C:2006:74.

761 Lammerant, H., & De Hert, P. (2016). Predictive profiling and its legal limits: Effectiveness gone forever. In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, p. 166-167.

762 Citron, D.K. (2008) 'Technological Due Process', *Washington University Law Review* 85: 1249-1313.

763 Lammerant, H., & De Hert, P. (2016). Predictive profiling and its legal limits: Effectiveness gone forever. In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, p. 166-167.

discrimination is unquestionably a decision that significantly affects the data subject, therefore article 11(3) LED was adopted, so that national law is not allowed to authorize profiling that results in discrimination based on processing of sensitive data.[764]

While it may seem that profiling using special categories of data is thus subjected to strict rules, this is not necessarily the case. The processing of special categories of data under article 10 LED is only allowed where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and if it is for example authorized by Union or Member State law. However, this raises the question what the notion 'appropriate safeguards' entails and whether authorization by law is not a potential catch-all basis for the processing of sensitive personal information.[765] Furthermore, for profiling specifically, article 11 LED refers to 'suitable safeguards' when processing special categories of data rather than appropriate safeguards that apply to processing under article 10 LED. Marquenie argues that the threshold for using special categories of data in profiling versus other personal data is not higher.[766] The Article 29 Working Party, in its opinion on the LED, concluded that the term 'strictly necessary' in article 10 LED has to be seen as paying particular attention to the necessity principle with regard to the processing of special categories of data, as well as to foresee precise and solid justifications for such processing.[767] The Article 29 Working Party acknowledged that the processing of special categories of data always entails a risk of discrimination, for example a violation of article 21 of the CFREU or other significant adverse effects to the data subjects' rights and freedoms. Thus the safeguards are only appropriate if they are sufficient to protect the data subjects against those risks.[768] For examples of safeguards reference is made to recital 37 of the LED, which provides the following examples of appropriate safeguards:

> *"(…)the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data".*

---

764 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

765 T. Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security review* 33 (2017), p. 332.

766 T. Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security review* 33 (2017), p. 332.

767 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

768 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

Ultimately this means that Member States have a lot of discretion when it comes to establishing safeguards for processing sensitive data, even if national laws have to comply with fundamental rights protection from the CFREU and instruments such as Convention 108+.[769]

4.3.4 Information rights and explanation mechanisms connected to profiling under the LED & GDPR

As explained in the previous section, a complete perspective on adequate fundamental rights safeguards for profiling can only be achieved when also assessing information rights in relation to profiling. Information rights are a first step in achieving protection of other fundamental rights and data subject rights. For the law enforcement sector it is understandable that those information rights are not as broad as in a non-law enforcement context due to reasons of the interest of the criminal investigation, creating differences between the LED and GDPR in this regard.[770] Nonetheless law enforcement actors are not completely exempted from providing information. For example, following case law of the CJEU such as *Tele2 Sverige*, individuals whose personal data has been accessed by law enforcement authorities should be notified as soon as possible and in any event as soon as the notification no longer prejudices the ongoing investigations. [771] Whether there is such a right to notification actually present in the LED is a topic of debate[772], but it is interesting here to refer back to section 4.2.2 where the CoE Police Recommendation was discussed, which did contain such a recommendation under principle 2.2.

One of the biggest points of discussion regarding article 22 of the GDPR, and perhaps even one of the most heatedly debated points of the GDPR in its totality, is the discussion of explanations of automated decision-making and profiling. The discussion follows articles

---

769 Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), p. 173.

770 C. Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, *Computer Law & Security Review*, Volume 34, Issue 1, 2018, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.08.002, page 162.

771 C. Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, *Computer Law & Security Review*, Volume 34, Issue 1, 2018, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.08.002, page 162.

772 For an extensive analysis, see: C. Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, *Computer Law & Security Review*, Volume 34, Issue 1, 2018, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.08.002, page 162.

13 2(f), 14 2(g), 15 1(h) and article 22 as well as recital 71 of the GDPR.[773] Many scholars have entered in the debate whether, following these provisions, there is a right to explanation or not, whether it is even relevant if these provisions constitute a right or another type of requirement, as well as what information should be provided then to data subjects exactly to meet the requirements of the GDPR.[774]

Most notably, Goodman and Flaxman[775] started the debate by introducing that the GDPR contains a right to explanations, while Wachter et al.[776] take an opposite stance and

---

773 See for example, Goodman and Flaxman, European Union Regulations on Algorithmic Decision-making and a "Right to Explanation", *AI MAGAZINE*, arXiv:1606.08813; Brkan and Bonnet, Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. European *Journal of Risk Regulation*, 11 (2019), pp. 18–50 doi:10.1017/err.2020.10; Bygrave, "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions." Version 1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (Forthcoming); University of Oslo Faculty of Law Research Paper No. 2020-35 (2020).

774 See: E. Bayamlıoglu, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391; Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27; Brkan and Bonnet, Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. *European Journal of Risk Regulation*, 11 (2019), pp. 18–50 doi:10.1017/err.2020.10; Bygrave, "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions." Version 1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (Forthcoming); University of Oslo Faculty of Law Research Paper No. 2020-35 (2020); Edwards and Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1; Edwards and Veale, Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling, *Computer law & security review*, 34 (2018) 398–404; Goodman and Flaxman, European Union Regulations on Algorithmic Decision-making and a "Right to Explanation", *AI MAGAZINE*, arXiv:1606.08813; Kaminski and Malgieri, Multi-layered Explanations from Algorithmic Impact Assessments in the GDPR, ACM, ISBN 978-1-4503-6936-7/20/02, https://doi.org/10.1145/3351095.3372875; Kaminski, "The Right to Explanation, Explained," *Berkeley Technology Law Journal* 34, no. 1 (2019): 189-218.; Malgieri and Comande, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 4; Mendoza and Bygrave. "The right not to be subject to automated decisions based on profiling." In: *EU Internet Law*, pp. 77-98. Springer, Cham, 2017; Roig, Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR), *European Journal of Law and Technology* Vol 8, No 3 (2017); Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4; Veale, Binns and Van Kleek, Some HCI Priorities for GDPR-Compliant Machine Learning. The General Data Protection Regulation: An Opportunity for the CHI Community? (CHI-GDPR 2018), Workshop at ACM CHI'18, 22 April 2018, Montréal, Canada; Wachter, Mittelstadt and Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 2.

775 B. Goodman and S. Flaxman, European Union Regulations on Algorithmic Decision-making and a "Right to Explanation", *AI MAGAZINE*, arXiv:1606.08813.

776 S. Wachter, B. Mittelstadt and L. Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 2.

advocate that the GDPR does not contain a right to explanation, at least not ex post of the reasoning that led to a decision. At the same time, for example, Mendoza and Bygrave, as well as Selbst and Powles and Brkan all put forward various arguments on how a right to explanation can be derived from the GDPR.[777] Scholars such as Edwards and Veale take a middle ground and are critical of the GDPR's approach to transparency and information, especially concerning the possibilities to actually exercise information rights.[778]

For the purpose of this research, the question is not so much whether these provisions constitute such a right under the GDPR or not,[779] but rather to explore which information or explanations regarding profiling processes should be provided to data subjects and especially how information rights differ between the GDPR and the LED. For the protection of data subjects it is more interesting to see the information rights pertaining to profiling being delineated and given meaning than to debate whether there is a right to explanations or not.[780] As was identified in chapter 3, many of the challenges risk profiling poses to the protection of fundamental rights are caused (partially) by opacity, making transparency a crucial topic. Information rights and more specifically explanations are appealing to apply to automated decision-making and profiling since these processes can defy human understanding, creating tensions in protecting data subjects' rights or the ideals behind data protection, such as autonomy, personhood and fairness.[781] There are scholars who heavily criticize the information rights under the GDPR and question whether the transparency offered

---

777 I. Mendoza and L.A. Bygrave. "The right not to be subject to automated decisions based on profiling." In: *EU Internet Law*, pp. 77-98. Springer, Cham, 2017; Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4; Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27.

778 L. Edwards and M. Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1.

779 See for example Goodman and Flaxman, who advocate that such a right can be read into the text of the GDPR, and Selbst and Powles who agree to some extent: Goodman and Flaxman, European Union Regulations on Algorithmic Decision-making and a "Right to Explanation", AI MAGAZINE, arXiv:1606.08813; Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 235; And see Wachter, Mittelstadt and Floridi on the opposite position: Wachter, Mittelstadt and Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 2.

780 See also Brkan and Selbst and Powles who advocate this same point: Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, p. 112; Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4.

781 See for example: A. Selbst and J. Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 233.

through the information rights under the GDPR is what should be strived for and even whether these rights might achieve the opposite and create a transparency fallacy.[782]

4.3.4.1 Recital 71 GDPR and recital 38 LED

Starting with the recitals of the GDPR, recital 71 refers to several rights for data subjects in the course of automated decision-making and profiling. Regardless of the legal basis for the profiling, data subjects should be protected by suitable safeguards, which should include: specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Thus recital 71 does not only refer to the data subjects' rights contained within article 22 GDPR, such as human intervention and for the data subject to express their point of view, but also claims that data subjects should be able to obtain an explanation of the decision as a safeguard. The GDPR does not use this wording of 'an explanation of the decision' anywhere else in the text of the instrument. With the non-binding nature of recitals, the recital does not confer a right itself, but that does not devoid the recital of meaning. In the context of risk profiling, Member State legislation seems the most logical option for establishing a legal basis for profiling. Member States will thus have to assess where suitable safeguards to profiling are required in their national legislation. It seems at least that the European legislator strongly suggests to include explanations in national safeguards, next to other safeguards such as human intervention. Whether it is relevant that the term 'explanations' itself is not used later in articles 13 -15 and 22 GDPR is debatable; requirements for providing explanations can be found in a combination of factors there, as is discussed below. Moreover, recital 71 can be seen as at least supporting the effective exercise of data subject rights under articles 13–15 GDPR and 22 GDPR.[783]

Surprisingly, the LED contains a very similar recital that is often not brought into the 'right to explanations debate' in the literature. Recital 38 LED contains the same sentence: "*In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision*." Brkan and Bonnet mention recital 38 of the LED alongside recital 71 of the GDPR but do not venture further and do not

---

782 For example, L. Edwards and M. Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1.

783 See for example: Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 235; Brkan and Bonnet, Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. *European Journal of Risk Regulation*, 11 (2019), p. 21.

engage in a discussion on the meaning of recital 38 of the LED.[784] Sajfert and Quintel do comment on this LED recital in combination with explanations. However, Sajfert and Quintel propose that a discussion similar to the right to explanation debate as we know under the GDPR is not possible under the LED, meaning that the recital about explanations under the LED would not have much weight. Sajfert and Quintel emphasise the differences between the GDPR and LED, since the recital itself is non-binding, the legal nature of a directive requires national implementation and because of the specific context of the law enforcement area.[785] Sajfert and Quintel therefore attribute the right to explanation solely to article 15(h) GDPR.[786] As explained below, it can be argued that the discussion is and should be broader than article 15(h) GDPR: a debate on explanations is also possible for the LED even though it does not have the same provision as the GDPR does under article 15(h). In addition, the importance of the recital itself should not be forgotten. If the legislator had deemed explanations of automated decisions or of profiling impossible under the LED, it would not have been mentioned specifically in recital 38. In other words, the legislator apparently deems explanations also in this context a suitable safeguard.

4.3.4.2 Articles 13-15 GDPR

Articles 13 and 14 GDPR contain the right to notification for data subjects in scenarios where data are collected from the data subject or from other parties, respectively. Article 15 GDPR contains the right of access for the data subject. Each of these provisions requires the following information necessary to ensure fair and transparent processing in respect of the data subject to be provided (whether through notification to the data subject or by means of an access request by the data subject): information concerning the existence of automated decision-making and profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[787]

Under the LED there is also an article 13 requiring information to be given to the data subject, and article 14 granting the right of access to data. However it does not contain the specific terminology that the GDPR does which sparked the debate on the 'right to explanation'. Notably also the LED provides for exceptions not to grant information to

---

784 M. Brkan and G. Bonnet, Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. *European Journal of Risk Regulation*, 11 (2019), p. 20.

785 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019, p.10.

786 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019, p.10.

787 Article 13(2)(f) GDPR, article 14(2)(g) GDPR and article 15(1)(h) GDPR.

data subjects, most notably for avoiding obstructing of legal inquiries, investigations or procedures, avoiding prejudicing the prevention, detection, investigation or prosecution of criminal offences, and protecting public or national security. That is why in this subsection I focus on the GDPR to demonstrate what information regarding profiling could look like, if similar wording would ever be adopted for the LED or its successor in the future.

In relation to profiling, articles 13-15 GDPR can be broken up into three parts. First of all, the data subject has to be made aware of the existence of profiling to be able to exercise any rights pertaining to the profiling. That is why it is important to receive information of the existence of the profiling from a perspective of transparency and fairness. Beyond the question of what falls under the scope of automated decision-making and profiling, this requirement does not raise many questions.

Second, meaningful information about the logic involved has to be provided, to give the data subject some insight into the decision-making or profiling process. Arguably, this is the most complicated part of information providing in the context of profiling. This wording raises many questions, such as which information counts as meaningful, how to determine what is meaningful to whom, and which parts of the profiling process are covered by the ' logic involved'. Interestingly enough, the GDPR also specifies that this meaningful information should be provided at the least, creating the impression that this is a minimum of information to be provided; Member States are free to create more safeguards in providing information if they wish to do so. This second step of providing meaningful information about the profiling can be seen as cracking the black box of profiling open a little bit, after awareness raising in the first step. Information will have to be provided about, for example, the rationale and the criteria relied upon in reaching the decision.[788] The meaningful information to be provided goes beyond decisional transparency. Decisional transparency does not per se create comprehensibility, and can even be used as a means of obfuscation in complex processes.[789]

When assessing what information would count as meaningful, this involves a subjective assessment that requires a perspective; in other terms, requires determining

---

788 E. Bayamlıoglu, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391, p. 10.

789 Bygrave, L.A. "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions." Version 1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (Forthcoming); University of Oslo Faculty of Law Research Paper No. 2020-35 (2020).

to whom the explanation should be meaningful. It would be the most logical to require that information should be meaningful to the data subject, as the information rights are intended to serve the data subject.[790] Information should then be meaningful to an average person with no specific technical expertise of, for example, automated decision-making, profiling or algorithms. This idea is further supported by the text of the LED and GDPR itself, where both instruments determine with regard to information rights that information should be provided in a concise, intelligible and easily accessible form, using clear and plain language.[791] It is generally agreed that data subjects do not have to be presented with the source code or the mathematical formula of the algorithm itself, which is logical since the average data subject does not have the expertise to count this as meaningful information.[792]

Subsequently, the question is how to determine what is meaningful to the data subject. Selbst and Powles provide an interesting theory on this by distinguishing between two roles that explanations can serve to the data subject: an instrumental and an intrinsic one.[793] In the intrinsic role, explanations focus on the value they create for a person's autonomy or personhood. In the instrumental role, functionality is the focus. Selbst and Powles put forward that a focus on the intrinsic value of explanations would weaken a right to explanations because concepts, such as autonomy, that are not that clearly defined, are being balanced against more concrete concepts such as trade secrecy or fighting crime.[794] Here the debate could enter into the murky waters of the discussions on trade-offs and balancing of rights and interests.[795] I do not

---

790 See for example also: Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121. 113; Bayamlıoglu, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391, p. 10; Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 236.

791 See article 12 LED and article 12 GDPR. Bayamlıoglu also stays close to the text of these provisions and asserts that accessibility and comprehensibility are the primary components of meaningful information, see: Bayamlıoglu, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391, p. 10.

792 M. Kaminski, "The Right to Explanation, Explained," *Berkeley Technology Law Journal* 34, no. 1 (2019): 189-218, p. 211.

793 A. Selbst and J. Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 236.

794 A. Selbst and J. Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 236.

795 See for example: Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press; Van der Sloot, B. (2016). The Practical and Theoretical Problems with 'Balancing'. Delfi, Coty and the Redundancy of the Human Rights Framework. *Maastricht Journal of European and Comparative Law*, 23(3), 439-459.

think that this critique is entirely fair, as explanations also should be seen as a basic respect towards individuals, ensuring that they can understand how they or data about them are viewed, especially in the context of complex and opaque processes performed by actors with more power. An interesting concept to demonstrate this is Bygrave's proposed cognitive sovereignty, which includes the idea that humans deserve the capacity to comprehend their environs and their place therein out of dignity.[796] With the rise of machine profiling and decision-making, this dignity can come under strain due to machine determinism. One could say that explanations express a desire to ensure that humans are able to participate in, shape and retain responsibility for decisions, for example to check for machine errors and undue discrimination.[797] Thus the important intrinsic value gives explanations a weight just as well. Selbst and Powles further put forward that an intrinsic value puts too much emphasis on what the individual requires or desires of such an explanation, which would limit discussing what meaningful explanations should look like.[798] Although explanations have a value of their own, in light of the notion of cognitive sovereignty, I also see the appeal of an instrumental value of explanations that Selbst and Powles put forward. If explanations are viewed in the context that the GDPR places them in, namely as existing through data subjects' rights, it makes sense to see them as a stepping-stone for data subjects to be able to exercise rights effectively, such as the right to contest an automated decision.[799] The functional or instrumental value of explanations also has a broader appeal in the context of profiling in the law enforcement sector, if similar rights would exist under the LED. If explanations can be used by data subjects to efficiently exercise rights, this also enables due process. The information provided about the profiling can be used to exercise criminal procedural rights related to profiling conducted by law enforcement actors. A similar argument can be made for using explanations in making an actionable claim of discrimination.[800] If explanations are viewed as serving both an

---

796 Bygrave, L.A., "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions." Version 1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (Forthcoming); University of Oslo Faculty of Law Research Paper No. 2020-35 (2020).

797 Bygrave, L.A., "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions." Version 1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (Forthcoming); University of Oslo Faculty of Law Research Paper No. 2020-35 (2020).

798 A. Selbst and J. Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 236.

799 For example, see also M. Brkan and G. Bonnet, Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. *European Journal of Risk Regulation*, 11 (2019), p. 21.

800 For more on this see the discussion on non-discrimination law in chapter 5. For more on explanations and discrimination specifically, see for example: Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 236.

intrinsic and instrumental value, this might offer the most protection to data subjects, by granting them a right to information as such that has to be acknowledged when assessing secrecy for law enforcement purposes and by facilitating the use of other important fundamental rights and remedies.

To avoid confusion, it should be noted that there are also scholars who see a functional approach to explanations of decisions, but view 'functional' as demanding that the algorithm or system is simple enough to offer functional information about the process so that it can be tested or verified.[801] Here functional also relates to actionability of the information, but phrased more in terms of a requirement of systems or process.

Taking these intrinsic and instrumental values into account, it is clear that for example data subjects should be given far more than a one-sentence overview of how the algorithmic decision-making system works, to count as meaningful information to them.[802] The question remains how to shape this exactly. Brkan presents the following ideal of what explanations under the GDPR would include: "(a) information about the data that served as the input for automated decision, (b) information about the list of factors that influenced the decision, (c) information on the relative importance of factors that influenced the decision, and (d) a reasonable explanation about why a certain decision was taken."[803] I would add to this, information on why factors are selected to be decisional factors, meaning how aggregated information, or group profiles, or profiles of others were used as a basis for this individual decision. The Article 29 Working Party supported this in its guidelines on providing information pertaining to profiling. In a list of recommendations for good practices, all of these factors are proposed:

> *"Instead of providing a complex mathematical explanation about how algorithms or machine-learning work, the controller should consider using clear and comprehensive ways to deliver the information to the data subject, for example:*

---

801 See: E. Bayamlıoglu, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391, p. 10.; Selbst A, Barocas S (2017) Regulating Inscrutable Systems. Available at: http://www.werobot2017.com/wp-content/uploads/2017/03/Selbst-and-Barocas-Regulating-Inscrutable-Systems-1.pdf; Lipton Z (2016) The Mythos of Model Interpretability, ICML Workshop on Human Interpretability in Machine Learning. (WHI 2016), New York. Available from URL: https://arxiv.org/pdf/1606.03490.pdf.

802 M. Kaminski, "The Right to Explanation, Explained," *Berkeley Technology Law Journal* 34, no. 1 (2019): 189-218, p. 211.

803 M. Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121, p. 112.

> *the categories of data that have been or will be used in the profiling or decision-making process; why these categories are considered pertinent; how any profile used in the automated decision-making process is built, including any statistics used in the analysis; why this profile is relevant to the automated decision-making process; and how it is used for a decision concerning the data subject."*[804]

Some scholars even propose information that is not suggested in these good practice recommendations could be provided as well, such as performance metrics.[805] These are good practices as there can be technical obstacles to providing the information under b) and c), limiting the explanations, likely, to 'only' information explaining crucial reasons for decisions.[806] Of course there are many more obstacles in practice that need to be taken into account, of both a technical and organizational nature, narrowing the gap between what is ideal and what is realistic.[807]

There is also another side of the coin. As Kaminski advocates, it also has to be prevented that data subjects would be flooded with large amounts of superficial meaningless information.[808] Article 12 GDPR requires that information provided to data subjects be comprehensible. Thus, information about the algorithmic decision-making must be in-depth, legible, meaningful and actionable, presented in a form that is understandable to data subjects rather than in complex jargon or hidden in a flood of superficial information.[809]

The third part that information rights mention is that also, at least, information about the significance and predicted consequences of the processing for the data subject should be provided. In literature, different interpretations of this requirement are offered. One way to interpret this wording is that information should be provided about how the decision-making will impact the data subject or how the automated

---

804 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 3 October 2017, p. 31.

805 L. Edwards and M. Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1; Malgieri and Comande, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 4.

806 M. Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, 2019, 27, 91–121, p. 112.

807 On limits to explanations and transparency see: Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 2053951715622512.

808 M. M. Kaminski, "The Right to Explanation, Explained," *Berkeley Technology Law Journal* 34, no. 1 (2019): 189-218, p. 212 & 213.

809 Kaminski, "The Right to Explanation, Explained," *Berkeley Technology Law Journal* 34, no. 1 (2019): 189-218, p. 212 & 213.

decision is used, so providing information about the consequences as such.[810] This information would not concern the analysis that goes on in the decision-making step, but would require information about the step that comes after.[811] For example, taking the classic GDPR illustration of a credit decision, first meaningful information about the logic involved in deciding to refuse credit will be provided, as well as information about the significance and the envisaged consequences of deciding to refuse providing the credit. Selbst and Powles offer an alternative interpretation in which 'as well as the significance and the envisaged consequences' pertains directly to the part of meaningful information about the logic involved.[812] Under such an interpretation of the text, meaningful explanations should be provided not only of the logic involved in the decision but also of the consequences or impact of the decision. This might seem like a semantic difference, but it would entail more than just information about the use of a decision, as an explanation can be argued to delve into more detail and complexity than just providing information. There is not much incentive to follow this latter interpretation though, as it is not supported by guidelines; for example, the Article 29 Working Party seemed to see information about the significance and consequences of the decision separately from an explanation of the logic in the decision.[813]

It is important that the GDPR also requires information about the significance and consequences of the decision to be provided, as this information is crucial to data subjects to exercise rights. Data subjects need to be aware of the concrete results and the risks arising from the contextual use of the data.[814] Again, in the example of credit scoring, it is relevant for data subjects to know whether the result of the analysis will be used for subsequent evaluations and which third parties might have access to the

---

810 See for example: Selbst and Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 237; Veale, Binns and Van Kleek, Some HCI Priorities for GDPR-Compliant Machine Learning. The General Data Protection Regulation: An Opportunity for the CHI Community? (CHI-GDPR 2018), Workshop at ACM CHI'18, 22 April 2018, Montréal, Canada.

811 See chapter 2, section 2.3.1, on information on the different stages of the profiling process.

812 A. Selbst and J. Powles, Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 237.

813 See for example the following wording used by the Article 29 Working Party on p. 10 of the Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 3 October 2017: "(…)the existence of automated decision-making referred to in Article 22(1) and (4), the logic involved, and the significance and envisaged consequences of such processing."

814 See also E. Bayamlıoglu, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391, p. 10.

results.[815] Only then is the data subject able to decide whether to contest a decision or take other actions. Malgieri and Comandé focus on the importance of receiving meaningful information about the impact of the decision as well and talk of a right to legibility rather than a right to explanation.[816] Malgieri and Comandé propose a legibility test, an assessment for data controllers to perform in order to provide meaningful information. The test requires both the architecture or functionality of the system and the implementation or actual use of the system to be assessed, combining both ex ante and ex post elements. [817] Thus in their approach, the information is to be provided on the process as a whole. Malgieri and Comandé describe this as a 'legibility-by-design' system, which enables the autonomous capability of individuals to understand the functioning and the impact of algorithms concerning them.[818] It is clear that the information about the significance and predicted consequences of the decision and profiling is just as important as information concerning the logic involved in the processing.

There is a major difference between the GDPR and LED when it comes to information rights. While, as discussed above, the recital pertaining to profiling and explanations is very similar in both instruments, the opposite is true for the provisions on data subjects' rights. The information concerning the existence of automated decision-making and profiling, meaningful information about the logic involved, as well as information on the significance and the envisaged consequences of such processing for the data subject, does not have to be provided to data subjects under the scope of the LED.[819] In other words, there are no provisions under the LED mirroring 13(2)(f), 14(2)(g), 15(1)(h) GDPR.

Since the LED is a directive, it is important to see how the data subject rights are fleshed out in national legislation, as Member States are given the discretion to draft

---

[815] See also E. Bayamlıoglu, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391, p. 10.

[816] G. Malgieri and G. Comandé, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 4.

[817] G. Malgieri and G. Comandé, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 244.

[818] G. Malgieri and G. Comandé, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 244.

[819] See also Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International journal of law and information technology*, 27(2), 91-121; Bygrave, "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions." Version 1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (Forthcoming); University of Oslo Faculty of Law Research Paper No. 2020-35 (2020).

safeguards and shape the rights. I examined Dutch legislation on automated decision-making and profiling and information rights pertaining to those. The Dutch system is interesting since legislation for law enforcement actors on processing personal data already followed the 2008 FD, also for domestic processing.[820] The Police Data Act[821] and the Judicial Data and Criminal Records Act[822] contain the data protection legislation for processing of personal data by Dutch law enforcement actors. These two instruments already encompassed some obligations that are now in the LED, but new articles are added for example on subject rights.[823] The Dutch legislator emphasized that some data subjects rights from the GDPR should be applied to the law enforcement context as well. The Dutch legislator puts forward that it is important also in the criminal law context to provide information about automated decision-making and profiling and thus the information concerning the logic involved in the decision-making should also be offered under the LED, not just under the GDPR.[824] Originally, in the draft bill, the only safeguard that was in place for automated decision-making was human intervention. The Dutch DPA criticized this narrow interpretation of subjects' rights and advocated that at least specific information provision to the data subject should be in place. The legislator agreed and incorporated that safeguard into the law. This requirement is implemented in article 24b (2)(e) of the Police Data Act, which stipulates that information should be provided to the data subject about:

> *"the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".*[825]

At first glance this seems very promising, from a point of view of providing transparency to data subjects in the context of law enforcement. However, article 24b (4) of the Police Data Act also stipulates that the rights under 24b (2) of the Police Data Act do not apply to those suspected of having committed or going to commit a crime, so suspects and defendants. Thus, the Dutch implementation of the LED only offers more information rights than the minimum LED requirements for those data subjects that are not suspects.

As explained, the LED limits data subjects' rights with regard to information and transparency of profiling and automated decision-making more than the GDPR

820 See: Tweede Kamer, 2017–2018, 34889, no. 3 p. 2 & p. 6.
821 In Dutch: Wet politiegegevens (Wpg).
822 In Dutch: Wet justitiële en strafvorderlijke gegevens (Wjsg).
823 Tweede Kamer, 2017–2018, 34889, no. 3
824 Tweede Kamer, 2017–2018, 34889, no. 3 p. 14 & 15.
825 Translation by the author; Tweede Kamer, 2017–2018, 34889, no. 3 p. 14 & 15.

does.[826] Leiser and Custers argue that having more limited data subject's rights under the LED may be satisfactory for data processing by law enforcement authorities, but the regime creates friction between data subject control and empowerment and the limits to that control and empowerment inherent in the LED.[827] Leiser and Custers deem the suggestion that data subjects under the LED are in control, through the introduction of data subjects' rights, misleading. Leiser and Custers explain that suspects have limited means of exercising their rights so as not to interfere with the investigation; the same goes for convicts, to avoid interference with criminal penalties.[828] There are more scholars that do not welcome too broad information rights for similar reasons: the idea of information rights for data subjects has been criticized in literature for relying on the capacity of data subjects to effectively exercise these rights, questioning whether data subjects have the access to justice they need and have the required expertise.[829]

Equally important though is how the nature of law enforcement activities influences data subjects rights. The opacity of law enforcement practices, allowed under the LED, puts extra strain on the exercise of data subjects' rights. Already it is very difficult for data subjects to be aware of who is processing their personal data and for which

---

826 For information on data subjects' rights under the LED see: P. Vogiatzoglou, K. Quezada Tavarez; S. Fantin; P. Dewitte, "From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 11, no. 3 (2020): 274-302; Dimitrova, D., and P. De Hert. "The right of access under the police directive: small steps forward." In: *Annual Privacy Forum*, pp. 111-130. Springer, Cham, 2018; Quintel, T. "Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive." *Eur. Data Prot. L. Rev.* 4 (2018): 104; Jasserand, C. "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?." *Computer law & security review* 34, no. 1 (2018): 154-165.

827 M. Leiser & B. Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, *EDPL* 2019 vol. 5, issue 3, doi:10.21552/edpl/2019/3/10.

828 M. Leiser & B. Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, *EDPL* 2019 vol. 5, issue 3, doi:10.21552/edpl/2019/3/10, p. 374.

829 L. Edwards and M. Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For', *Duke Law & Technology Review* 16, no. 1 (4 December 2017): 18–84; M. Ananny and K. Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability', *New Media & Society* 20, no. 3 (1 March 2018): 973–89, available at: https://doi.org/10.1177/1461444816676645; M. Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', p. 56, 2012, In: Bus, J. (ed.), *Digital Enlightenment Yearbook* 2012, pp. 41-56, available at: https://repository.ubn.ru.nl/handle/2066/94126; B. Goodman, 'A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection', 2016, 29th conference on neural information processing systems (NIPS 2016), Barcelona. NIPS foundation; Kaminski and Malgieri, Multi-layered Explanations from Algorithmic Impact Assessments in the GDPR, ACM, ISBN 978-1-4503-6936-7/20/02. https://doi.org/10.1145/3351095.3372875.

purposes, which rights they have in respect to that and how to exercise those rights.[830] With law enforcement profiling, awareness is all the more complicated because in general data subjects will not be aware they are being profiled or under investigation and for what purposes. In line with these problems, Leiser and Custers propose to focus on transparency and restrictions for data controllers instead of focusing on data subjects' rights that are hard to invoke.[831] While it is true that transparency and restrictions are of utmost importance in the law enforcement domain, the question is then how to strike the balance between creating data controllers' obligations and data subjects' rights. If the exercise of data subjects' rights is too complex in this field, requirements such as transparency and explanations should be met through obligations imposed on data controllers.

While the exercise of data subjects' rights can be more difficult due to opacity of law enforcement processing, the content of those rights also differs as opposed to exercising data subjects' rights under the GDPR. Under the LED, when data subjects exercise information rights concerning the processing of their personal data, they can receive a neutral reply.[832] When a controller provides a neutral reply this neither confirms nor denies, for example, the possession of certain personal data. For example, the wording of article 13 LED indicates that the right to information is a right of confirmation that collection of personal data has been carried out.[833] In addition, controllers can limit data subject rights under the LED, also largely as a consequence of that opacity. Controllers under the LED can even limit information about the refusal to provide information in response to data subjects exercising their information rights, which is very difficult for data subjects to challenge.[834] The difference in transparency thus creates a multitude of differences for data subjects between the GDPR and LED, which is important to keep in mind for law enforcement profiling.

---

830 M. Leiser & B. Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, *EDPL* 2019 vol. 5, issue 3, doi:10.21552/edpl/2019/3/10, p. 374.

831 M. Leiser & B. Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, *EDPL* 2019 vol. 5, issue 3, doi:10.21552/edpl/2019/3/10, p. 374.

832 For more on neutral replies see: J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

833 C. Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, *Computer Law & Security Review*, Volume 34, Issue 1, 2018, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.08.002, page 162.

834 J. Sajfert & T. Quintel, The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

4.4. Conclusions

This chapter discussed the many data protection instruments and provisions relevant to risk profiling by law enforcement actors. Although the CoE and EU approach have developed quite similarly over the years, there are still some differences in their approaches. The Convention 108+ and the CoE Recommendations rely more on principles while within the EU law the LED is more detailed. Compared to EU data protection legislation, the Convention 108+ is very compact. Also with regard to profiling, article 9 (1)(a) of Convention 108+ on automated decision-making is much more compact than article 11 of the LED. CoE data protection law focuses on the core principles of fair information practices or data processing, following the original idea of data protection from the 1970s and 1980s, whereas the EU legislator has taken the policy option to harden these principles and elaborate on them in detail in other provisions.[835] Some scholars see the advantages of using a principle-based approach in terms of comprehensibility and flexibility.[836] When it comes to automated decision-making and profiling, De Hert and Papakonstantinou argue that article 9(1)(c) Convention 108+ offers broader protection than article 15 GDPR, in the sense that the Convention grants data subjects access to the decision-making process and expands the right explicitly beyond automated decisions.[837] Indeed, the text of Convention 108+ grants this information right in a broader context, whereas under the GDPR there has to be an automated decision as defined by the GDPR before the data subject can request information about the logic involved. The LED has possibly strict requirements for profiling and automated decision-making, depending on national implementation, but has fewer information rights for profiling and no principle of transparent processing.

Data protection law regulates profiling when aspects of the profiling process include personal data. In this chapter I focused predominantly on the detailed secondary legislation of the EU: the LED and GDPR. We see a two thronged approach there in

---

835 P. De Hert & V. Papakonstantinou, Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review* 40 (2021), p. 6-7; Bygrave, The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review*, October 2020, https://doi.org/10.1016/j.clsr.2020.105460.

836 P. De Hert & V. Papakonstantinou, Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review* 40 (2021), p. 6-7; Bygrave, The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review*, October 2020, https://doi.org/10.1016/j.clsr.2020.105460.

837 P. De Hert & V. Papakonstantinou, Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review* 40 (2021), p. 7.

regulation profiling, on the one hand through the general data protection principles, on the other hand through a specific provision on automated decision-making including profiling. The data protection principles say something about the way in which data are to be processed in general (e.g. the principle of fair and lawful processing and the principle of accuracy) and where the limitations are in data processing, most prominently in collection and use of personal data (e.g. the principle of data minimization and the principle purpose limitation). The provisions specific to profiling, article 11 LED and article 22 GDPR, focus on the application of profiles, namely in automated decisions. The focus in regulation of automated decisions in the law enforcement sector is in the role of the human in the process (notably to assess the decision) and in requiring safeguards in the use of special categories of data.

Data protection law strives for protection of multiple values at the same time. Such a combined approach can focus on mitigating multiple challenges simultaneously, such as achieving fairness, a contribution to non-discrimination, protecting privacy goals in limiting the collection of data, preventing errors of data analysis through data accuracy and data subject rights, and so forth. But at the same time, there are shortcomings in the regulation of profiling specifically. Looking at EU data protection law, the LED (and GDPR) contains a specific provision on profiling, but that provision is quite limited in scope. For example, article 11 LED does not take into account the important group dimension of the profiling process; it only focuses on the application of a profile on the individual level. In addition, the rest of the LED, mainly the data protection principles, seem to assume a too simplistic view on data processing and profiling: some of the principles, such as fairness and accuracy, might clash (as described in chapter 3); and some principles are dependent on other factors, such as fairness needing a level of transparency; principles might offer flexibility but at the same time also leave uncertainty, such as when it comes to implementing the purpose limitation principle properly. Overall, for profiling, the provisions of data protection law still seem very focused on the collection and use of data. The provisions and principles do not address the use of non-personal data (such as statistics), do not set quality standards for the analysis beyond the general ideas of accuracy and fairness, do not set rules for the categorization or ranking of people, do not contain rules on accuracy in terms of predictions and probabilities, nor strong safeguards on preventing discrimination.

The next two chapters similarly discuss how risk profiling is regulated from non-discrimination law and criminal procedural law. The concluding chapter to the dissertation further discussed the gaps in data protection law that are identified here and presents recommendations on how to regulate risk profiling more adequately from a point of view of fundamental rights protection.

Chapter 5

Risk profiling & non-discrimination law

5.1 Introduction

As the datafication of society grows, so do concerns of discrimination. Everything can be datafied and analyzed and create a sense of objectivity. While the human mind is not always rational and we cannot track thoughts and explain every decision or action we make, it could seem appealing to attribute more rationality and objectivity to data and decision-making through data than to human analysis and decision-making. An overreliance on the perceived objectiveness of data can lead to subjectivity creeping in. Just as any other process, data processing has an inherent risk of being biased, excluding or over-including. This aspect is all the more prominent for data intensive processes such as profiling, because of the objective appearance of being rooted in statistics and analysis, and because bias can be hidden in a complicated and opaque process. Many scholars are calling for increased attention for the risks of discrimination through the use of AI, algorithms, and developments such as automated decision-making and profiling.[838] While profiling and automated decision-making rely heavily on statistics and data and are often presented as neutral or scientifically objective processes,[839] it is widely acknowledged that there is an ever-present risk of discrimination in such processes.[840]

---

838 For example: S. Barocas and A. Selbst "Big data's disparate impact" *California Law Review* vol. 104 no. 3 pp. 671-729 Jun. 2016, available at: https://ssrn.com/abstract=2477899; X. Ferrer, T. v. Nuenen, J. M. Such, M. Coté and N. Criado, "Bias and Discrimination in AI: A Cross-Disciplinary Perspective," in *IEEE Technology and Society Magazine*, vol. 40, no. 2, pp. 72-80, June 2021, doi: 10.1109/MTS.2021.3056293; Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567; Frederik J. Zuiderveen Borgesius (2020) Strengthening legal protection against discrimination by algorithms and artificial intelligence, *The International Journal of Human Rights*, 24:10, 1572-1593, DOI: 10.1080/13642987.2020.1743976; Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719895805; Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, 45(5), 494–511. https://doi.org/10.1177/0967010614544204; Xenidis, R. (2020). Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. *Maastricht Journal of European and Comparative Law*, 27(6), 736–758. https://doi.org/10.1177/1023263X20982173; Žliobaitė, I. Measuring discrimination in algorithmic decision-making. *Data Min Knowl Disc* 31, 1060–1089 (2017). https://doi.org/10.1007/s10618-017-0506-1.

839 Williams, P. and Kind, E. (2019) Data-driven Policing: The hardwiring of discriminatory policing practices across Europe. Project Report. European Network Against Racism (ENAR).

840 For example, see: Balayn and Gürses, "Beyond Debiasing: Regulating AI and its Inequalities", EDRi September 2021, available at: https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf; Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic-decision-making/1680925d73; Veale, M., and R. Binns. "Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data." *Big Data & Society* 4, no. 2 (2017): 2053951717743530.

Also outside of scholarly debates, examples can be found of profiling and automated decision-making that appear objective but nonetheless lead to discriminatory results, such as in the case of COMPAS used in the USA, which exacerbated negative bias and created discriminatory results against black defendants.[841] For example, in the USA, risk assessment is predominantly tied to prior criminal history of individuals, and in turn data on prior criminal history is heavily influenced by racial factors. The development of risk instruments in the law enforcement context shows that the evolution from race to risk can be traced through the factors used in the risk-assessment tools, where nationality, race, and religion became staples of prediction assessments.[842] Perhaps risk prediction tools for sentencing and incarceration are not so far developed yet in Europe, but they will undoubtedly face similar challenge of data and risk assessment algorithms being biased against people of certain race, ethnicity, nationality or religion. In profiling conducted in a law enforcement context there is especially a risk of ethnic or racial profiling, even more so when it concerns counter-terrorism profiling, which tends to focus on people (who appear to be) from certain countries.[843] The struggle of conducting profiling that is not discriminatory demonstrates a need for a critical assessment of legal protection against discrimination. Non-discrimination legislation comes into play in the profiling process in various ways: in profiling, various characteristics that are used for grouping individuals in categories can be used to differentiate, whereas non-discrimination law limits which differences are legally allowed to be used in treatment of individuals. In principle, the protected grounds of non-discrimination law are characteristics that should not be considered relevant unless they can be adequately justified. Non-discrimination law applies to different stages of the profiling process, from the selection of data to be used in profiling to the application or use of the profile.[844] Therefore, for the comprehensive study of the regulatory framework of profiling, it is essential to assess the protection against discrimination.

For the European context, there is a distinction between non-discrimination law of the EU and of the CoE. The EU has laid down the general non-discrimination principle

---

841 J. Angwin, J. Larson, S. Mattu, L. Kirchner, "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks," ProPublica, 23 May 2016; www.propublica.org/article/machine-bias-risk-assessmentsin-criminal-sentencing; see chapter 2 & 3 for more information on COMPAS.

842 Harcourt, B.E. Risk as a proxy for race. John M. Olin Law & Economics Working Paper no. 535, (2d series), Public Law and Legal Theory Working Paper no. 323, September 2001. Available at: https://ssrn.com/abstract=1677654.

843 De Schutter, O., and J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008): 358-384.

844 Lammerant, H., and P. De Hert. "Predictive profiling and its legal limits: Effectiveness gone forever. PP. 145-173" In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, p. 158.

in article 21 of the CFREU and the CoE has laid down the general non-discrimination principle in article 14 of the ECHR.[845] While each instrument has case law of their own expanding on these primary provisions, from the CJEU and the ECtHR respectively, and has secondary or other legislative instruments, the core concepts of non-discrimination law remain the same for both jurisdictions, as will be discussed in the respective sections. Therefore, both jurisdictions will be analyzed for their role in regulating non-discrimination in profiling, focusing on their common elements, scope and steps taken by the ECtHR and CJEU in their case law. The main focus is on the case law of the ECtHR regarding article 14 ECHR, as individuals can file complaints about states to the ECtHR, while this is not possible with the CJEU; this fact has led to jurisprudence on non-discrimination between states and individuals under the ECtHR but not under the CJEU. The CJEU has ruled on cases involving article 21 CFREU, but these mainly involve prejudicial questions that accompany a reference to a more-established, domestic law source, and there is not much case law on article 21 CFREU to date.[846] The case law in this chapter is not so much specifically on risk profiling practices, but nonetheless shows how the concepts of non-discrimination law are applied to state practices.

This chapter has two aims. The first aim is to analyze how non-discrimination law of the EU and the CoE, more specifically their primary provisions, namely article 14 ECHR and article 21 CFREU, regulate non-discrimination and create safeguards against discrimination. The second aim is to assess the challenges in applying the legal framework on non-discrimination to law enforcement risk profiling. These two sub-goals together answer the question: *How do article 14 ECHR & article 21 CFREU regulate risk profiling by national law enforcement actors, and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?*

This chapter, together with the chapters on data protection legislation and criminal procedural law (chapters 4 and 6 respectively), forms the discussion on the regulatory framework for risk profiling by law enforcement actors. A clear view of the regulatory framework for law enforcement risk profiling is necessary to assess to what extent the challenges of law enforcement risk profiling, identified in chapter 3, are addressed by the legal framework and to move to chapter 7 of the dissertation where recommendations are made to address gaps between the protection awarded by the

845 Below, in section 5.4, I will also briefly explain which related provisions and secondary legislation there are.

846 Muir, E. "The Added Value of the EU Charter of Fundamental Rights: at the Intersection of Legal Systems." Jean Monnet Working Paper 15/20, (2020). See also: A. Ward. "The Impact of the EU Charter of Fundamental Rights on Anti-Discrimination Law: More a Whimper than a Bang?." *Cambridge Yearbook of European Legal Studies* 20 (2018): 32-60.

legal framework and challenges for those subjected to risk profiling that remain. Non-discrimination law has an interesting approach in regulating risk profiling. Non-discrimination law is focused on a result, namely achieving a non-discriminatory treatment.[847] There are many laws and provisions pertaining to non-discrimination in different situations, there is not one framework with different levels of legislation. Non-discrimination law is strongly connected to data protection legislation, since data protection legislation also contains safeguards against discrimination.[848]

The chapter is based on legal doctrinal research. As a starting point for the legal literature, commentaries, and handbooks about both the ECHR and CFREU were used to lay a foundation for the discussion on both these legal instruments as such and their role in non-discrimination, and to identify key authors and find further literature for the discussion on article 14 ECHR and article 21 CFREU. The literature on these two provisions was also used to identify relevant case law from the ECtHR. This literature about non-discrimination comes from a mix of scholars based in the EU, writing on non-discrimination law, and some Anglo-Saxon scholars who write on discrimination in policing in the UK or USA to add more practical examples or information about discrimination in practice; concerning the latter, literature predominantly stems from the UK and USA. Literature on discrimination in law enforcement practices on racial or ethnic profiling lays the foundation for exploring discrimination especially on the basis of the protected grounds of race, ethnicity, nationality and religion. In order to understand how risk profiling can lead to discrimination, it is important to go beyond

847 See for example: Gellert, R., de Vries, K., de Hert, P., Gutwirth, S. (2013). A Comparative Analysis of Anti-Discrimination and Data Protection Legislations. In: *Custers, B., Calders, T., Schermer, B., Zarsky, T. (eds) Discrimination and Privacy in the Information Society*. Studies in Applied Philosophy, Epistemology and Rational Ethics, vol 3. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-30487-3_4.

848 See for example: F. J. Zuiderveen Borgesius (2020) Strengthening legal protection against discrimination by algorithms and artificial intelligence, *The International Journal of Human Rights*, 24:10, 1572-1593, DOI: 10.1080/13642987.2020.1743976; Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719895805; Gellert, R., de Vries, K., de Hert, P., Gutwirth, S. (2013). A Comparative Analysis of Anti-Discrimination and Data Protection Legislations. In: *Custers, B., Calders, T., Schermer, B., Zarsky, T. (eds) Discrimination and Privacy in the Information Society.* Studies in Applied Philosophy, Epistemology and Rational Ethics, vol 3. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-30487-3_4; Schreurs, W., Hildebrandt, M., Kindt, E., Vanfleteren, M. (2008). Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In: *Hildebrandt, M., Gutwirth, S. (eds) Profiling the European Citizen*. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-6914-7_13; Le Métayer, D., Le Clainche, J. (2012). From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles. In: *Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (eds) European Data Protection: In Good Health?* Springer, Dordrecht. https://doi.org/10.1007/978-94-007-2903-2_15.

legal doctrinal research and also use sources such as policy reports by the EU Agency for Fundamental Rights (FRA) that provide empirical data and to use literature that explains the technology. These sources that do not focus on the legal framework are used in sections 5.2 and 5.3 to explain the empirical practices of risk profiling and what role data and profiling techniques play in discrimination.

The structure of this chapter is as follows. Section 5.2 first contains a brief description of discrimination as a challenge in law enforcement profiling, describing how this type of profiling can lead to discrimination; this extends and deepens the discussion on this topic in chapter 3. Section 5.3 discusses discriminatory profiling in the law enforcement context, focusing on the discourse on racial profiling and how different law enforcement profiling practices have different discrimination risks. Section 5.4 follows the steps from article 14 ECHR and article 21 CFREU and their case law. Section 5.4.1. first takes inventory of the system of non-discrimination law, providing a brief overview of non-discrimination law, a legal definition of discrimination, introduces article 14 ECHR and article 21 CFREU, and explores the approach of non-discrimination law. After that, sections 5.4.2. to 5.4.4 discuss the different components of article 14 ECHR and article 21 CFREU, namely, the system of protected grounds, the difference between direct and indirect discrimination, and the objective justification for discrimination, and their relevance to profiling.

5.2 Discrimination & profiling

As explained in previous chapters[849], one can distinguish between completely non-automated profiling versus profiling with automated components, or in some instances, profiling processes that are completely automated. It is important to note that all types of profiling processes have a risk of being discriminatory. For example, a general stop and search policy of police based on personal experiences of law enforcement officers rather than on (semi-)automated data analysis can focus on ethnicity and be discriminatory; similarly, a more data-driven, automated, predictive policing tool can discriminate against people of a certain religion living within the same geographical area. However, although all types of profiling can potentially be discriminatory, one can distinguish between risks of discrimination that are prevalent in all forms of profiling and specific risks of discrimination being exacerbated by automation of the profiling process. Risk profiling has automated components, thus there are specific discrimination challenges to that which need to be assessed.

[849] See chapter 2, section 2.3.4.1.

As an example of discrimination challenges tied to automation, the following ways in which discrimination risks are exacerbated by data-driven technologies can be used to illustrate the issue: First, technology can exacerbate existing discrimination because as an already over-policed group within society, minorities will be disproportionally impacted by negative effects of new technologies. Second, algorithmically driven identification technologies can disproportionately mis-identify people of colour and other minority ethnic groups. Third, predictive policing systems often present geographic areas and communities with a high ratio of people from an ethnic minority as high risk and subsequently increase police presence there.[850] For example, think of the risk assessment tool of COMPAS that over-targets black defendants, while black defendants might already be in a less favorable position than white defendants in the American criminal justice system. Or consider facial recognition used by border controls that has a higher error rate for people of colour, producing a biased result towards them.[851] In addition, the predictive policing systems have usually been developed based upon data that reflects ethnic or racial profiling, resulting in hardwiring of historical racist policing into present day practice.[852] The most difficult point about biased data is that bias is not readily apparent, bias can creep into the system in different ways: bias can unintentionally creep into labelling of data or in the rules that are coded into the algorithm; the data underlying the analysis can be biased because of assumptions inherent in the data or in the way it was collected; or bias creep can occur due to technical defects, or problems with the system itself, which can lead to more false positives and false negatives.[853] Thus the reliance on data introduces further risks of discrimination.

The specific risks of discrimination caused by the introduction of AI, such as in automated decision-making and profiling, are discussed into great length and detail by Zuiderveen Borgesius in his 2018 report for the CoE.[854] Zuiderveen Borgesius maps five ways in which AI-driven decision-making can lead to discrimination, based on

---

850 Williams, P. and Kind, E. (2019) Data-driven Policing: The hardwiring of discriminatory policing practices across Europe. Project Report. European Network Against Racism (ENAR).

851 FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement, available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

852 Williams, P. and Kind, E. (2019) Data-driven Policing: The hardwiring of discriminatory policing practices across Europe. Project Report. European Network Against Racism (ENAR).

853 Van Brakel, R. "Pre-emptive big data surveillance and its (dis) empowering consequences: The case of predictive policing." In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data,* p. 125.

854 Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic- decision-making/1680925d73.

-also seminal- previous work by Barocas and Selbst.[855] The first is the way how the target variable and the class labels are defined, which can have a negative connotation for certain groups. For example, a company can choose 'rarely being late' as a class label to assess whether an employee is 'good', while the people who live closest to work are people with a higher income and own means of transportation and people from a minority group live further away from the center and rely on public transportation. Thus, this target variable and these class labels chosen by the company can lead to discrimination against minorities. Second, problems of discrimination arise in labelling the training data, as the AI system might be trained on biased data or the AI system learns from biased samples, reproducing that bias from the training data. Third, problems of discrimination arise in collecting and selecting the training data, as the sampling procedure can be biased. This can happen for example in the classic example of police stopping more people with an immigrant background, thus creating more data about those groups and therefore over-representing them in the system, which can teach the AI that people with an immigrant background are more likely to commit crime. Fourth, problems of discrimination arise in the features selected for the AI system. The context needs to be simplified for the AI system, thus choices have to be made about which attributes to include. This selection can introduce bias against specific groups, as an attribute can represent or include one group and exclude another group. Fifth, problems of discrimination arise using proxies, as data can seem not to represent protected grounds but can still correlate to those protected grounds in a more indirect way. A well-known example of a proxy is that of postal codes correlating with racial origin or ethnicity.[856] In addition to this classification, Zuiderveen Borgesius adds that a sixth way in which AI systems can introduce discrimination is by using them on purpose for discriminatory ends, for example by intentionally using proxies to discriminate.[857] This oversight of six ways in which AI and automation play a role in discrimination issues is crucial for a basic understanding for this chapter of the dissertation, to distinguish traditional problems of grouping people and differential treatment based on group characteristics from challenges caused by AI and thus prominent in risk profiling.

---

855 Barocas, S. and Selbst, A.D., Big Data's Disparate Impact (2016). 104 *California Law Review* 671 (2016), available at http://dx.doi.org/10.2139/ssrn.2477899.

856 Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic- decision-making/1680925d73, p. 10-14.

857 Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic- decision-making/1680925d73, p. 13-14.

Similarly, Gerards and Xenidis published an extensive report for the European Commission, which is the most comprehensive overview on the challenges of algorithmic discrimination, in which they identify six main challenges that the use of algorithms poses for non-discrimination law. Thus the perspective of this study is not the challenges that algorithms create in terms of discrimination, but rather the other way around, in which ways the law struggles to regulate algorithmic practices. The six challenges they list are: 1) the human factor and the stereotyping and cognitive bias challenge; 2) the data challenge; 3) the correlation and proxies challenge; 4) the transparency and explainability challenge; 5) the scale and speed challenge; and 6) the responsibility, liability and accountability challenge.[858] The first challenge relates strongly to the human influence in the algorithmic process: implicit biases, stereotypes and discriminatory prejudices held by humans can infect the algorithms they create and anchor biases, reinforcing these risks. The second challenge pertains to the data itself and Gerards and Xenisdis use it to describe how data embodies the historically consolidated patterns of discrimination that structure society and how training algorithms with such biased data, or with incorrect, unrepresentative or unbalanced data, leads to the reproduction of structural inequalities by these algorithms. The third challenge can be split into two parts. The one part explains how algorithms might put further emphasis on discriminatory correlations by treating them as causalities and using them as causal factors in decision-making. The other part pertains to the use of proxies and outlines how removing protected characteristics from the pool of input variables is insufficient, as algorithms can have the ability to detect proxies for these protected characteristics. The fourth challenge focuses on the tension between opacity of systems and human abilities to understand these systems, for example difficulties in detecting and proving algorithmic discrimination in light of the opacity of inner workings of algorithms. With the fifth challenge, Gerards and Xenidis refer to how algorithmic discrimination can take place on a larger scale and at a faster pace than 'human discrimination'. The final challenge that they outline focuses on the question of who is liable, responsible or accountable for discrimination in complex human-machine relationships.[859]

Taking a step back and viewing all the issues of discrimination and AI or use of algorithms outlined by all the EU scholars above, one can see that there is a clear challenge for the EU legal framework safeguarding against discrimination to tackle

858 Gerards & Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law. European Commission, Luxembourg: Publications Office of the European Union, 2021.

859 Gerards & Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law. European Commission, Luxembourg: Publications Office of the European Union, 2021.

exacerbated bias and discrimination due to reliance on data, through scale and complexity and because of mismatches or unclear roles for humans in these systems.

While all these examples of discrimination being exacerbated by or originating through technology focus on the use of data or AI, one should not forget that profiling as a practice is an inherently differentiating process, whether automated or not. Profiling is used to classify or group people and can be used to differentiate according to that classification. When discussing profiles, people usually refer to non-distributive profiles[860], in which the people classified together within a group do not share all of the same attributes, they just share most of the relevant characteristics.[861] A problem occurs, however, when people in a group are treated as if they match all the characteristics, and are treated according to group characteristics that they do not share, as if it were a distributive profile. This leads to stereotyping and can lead to discrimination.[862]

While automation of profiling can exacerbate discrimination or inequalities, it is equally important to note that there are also scholars who make appealing arguments as to why and how automation can curb discrimination and that automation does not necessarily exacerbate discrimination. For example, law enforcement can use profiles to make a more objective selection of which individuals to investigate, instead of relying on the personal and sometimes biased intuition of investigative officials.[863] Another example is that the omission of data in a profiling process that reveals information about protected grounds can actually lead to discrimination, despite the aim of trying to protect this sensitive information.[864] Such scholars also advance arguments proposing that there is a tendency to an overly protective reading of requirements from data protection legislation, especially when it concerns special categories of data, which makes combatting of ethnic profiling more difficult.[865]

---

860 See chapter 2, section 2.3.4.2.

861 Vedder, A. KDD: The challenge to individualism. *Ethics and Information Technology* 1, 275–281 (1999). https://doi.org/10.1023/A:1010016102284.

862 See chapter 2; Vedder, A. KDD: The challenge to individualism. *Ethics and Information Technology* 1, 275–281 (1999). https://doi.org/10.1023/A:1010016102284; Lammerant, H., and P. De Hert. "Predictive profiling and its legal limits: Effectiveness gone forever." PP. 145-173, In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, p. 148.

863 Custers, B., Risicogericht toezicht, profilering en Big Data, *Tijdschrift voor Toezicht 2014* (5) 3, p. 12.

864 Žliobaitė, I. and B. Custers. "Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models." *Artificial Intelligence and Law* 24, no. 2 (2016): 183-201.

865 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 360; Van Bekkum & Zuiderveen Borgesius, Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? (2022), available at: arXiv:2206.03262.

I would therefore be cautious not to present a one-sided, intrinsically negative, view on automation and discrimination. It is important to keep in mind that there is criticism of the current approach – of both data protection law and non-discrimination law – to always try to shield data related to protected grounds.

5.3 Discrimination in the law enforcement context

5.3.1. The use of protected characteristics

When analyzing discrimination in risk profiling in the law enforcement sector, discrimination can of course pertain to a wide variety of characteristics that relate to protected grounds. Nevertheless, traditionally, most debates center on law enforcement profiling and racial and ethnic discrimination.[866] For example, there are discussions concerning incidents of individuals being singled out by law enforcement based on ethnicity or religion, more so than based on behaviour: or, ethnic or religious backgrounds being used as a determining factor in law enforcement decisions; assumptions of law enforcement officials of a correlation between membership in a religious group and the likelihood of committing certain crimes such as in the context of terrorism.[867]

The FRA, in research into unlawful law enforcement profiling, concluded that most discrimination issues revolve around the question when profiling that uses race, ethnicity or religion will be considered unlawfully discriminatory and under which circumstances reference to these characteristics can be permissible.[868] It appears to be a well-established principle of international law that direct discrimination on the grounds of race, ethnicity or religion can never be justified or lawful, not even in times of public emergency or times of high security threats.[869] Of course this then raises the question what is considered direct discrimination, which will be discussed in the next section. Nonetheless, the ECtHR has ruled on a number of cases centered on racist

---

866 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008): 358-384.

867 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 358-359.

868 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 5-6.

869 For example see, Article 4(1) of the International Covenant on Civil and Political Rights (ICCPR). European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 17.

violence committed by police[870], raising the question whether in practice race might play a role in policing regardless of whether it is prohibited or not. Discriminatory conduct or policy by law enforcement actors merits an added discussion to that of discriminatory conduct by other public actors or by private actors, since the context of policing and the security domain is so specific and has its own challenges and in addition to that the consequences of discrimination in this sector are very severe.

According to the ECtHR, ethnicity and race are related and overlapping concepts: race is rooted in the idea of biological classification of human beings into subspecies on the basis of morphological features such as skin colour or facial characteristics; ethnicity stems from the idea of societal groups marked in particular by common nationality, tribal affiliation, religion, shared language, or cultural and traditional origins and backgrounds.[871] The FRA operates the term 'discriminatory ethnic profiling' to describe the practice of basing law enforcement decisions or actions solely or mainly on an individual's race, ethnicity or religion. The FRA chooses to include the term 'discriminatory' because the term 'ethnic profiling' – and racial profiling as well one could argue – has been used widely by media and scholars without a precise or uniform meaning. Thus, discriminatory ethnic profiling is used as a more specific term than just ethnic profiling.[872] This definition by the FRA seems comprehensive and precise enough. In addition, speaking of discriminatory ethnic profiling versus ethnic profiling distinguishes the situation where race, ethnicity or religion are used as part of a profile without violating the law.[873] Note that there is a thin line between when factors such as race, ethnicity and religion are to some extent part of a profile, and the prohibition against direct discrimination based on these grounds.

---

870 For example: ECtHR, *Nachova and Others v. Bulgaria* [GC], 2005; ECtHR, *B.S. v. Spain*, 2012; ECtHR, *Stoica v. Romania*, 2008; ECtHR, *Bekos and Koutropoulos v. Greece*, 2005; ECtHR, *Turan Cakir v. Belgium*, 2009; ECtHR, *Adzhigitova and Others v. Russia*, 2021, or by private individuals ECtHR, *Abdu v. Bulgaria*, 2014; ECtHR, *Moldovan and Others v. Romania* (no. 2), 2005; ECtHR, *Šečić v. Croatia*, 2007; ECtHR, *Makhashevy v. Russia*, 2012; ECtHR, *Fedorchenko and Lozenko v. Ukraine*, 2012. See: European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

871 ECtHR, *Sejdić and Finci v. Bosnia and Herzegovina* [GC], 2009, para. 43; ECtHR, *Timishev v. Russia*, 2005, para. 55 & 56; European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

872 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 6.

873 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 15.

An example of how ethnic profiling is conceptualized in academic literature can be found in the comprehensive and critical piece on ethnic profiling and human rights law by De Schutter and Ringelheim, who use the term ethnic profiling to refer to the practice of using race or ethnic origin, religion, or national origin, as either the sole factor, or one of several factors, in law enforcement decisions, on a systematic basis, whether or not individuals are identified by automatic means.[874] De Schutter and Ringelheim rightly point out that if these protected grounds have to be the sole criteria in profiling for it to be considered ethnic profiling, this would be too narrow and hide discrimination, since the risk of discrimination is no less if these grounds are only one component of a profile and combined with other factors when deciding to stop, search, arrest, or put under surveillance a person.[875] In that sense this aligns with the FRA definition, which also does not require these factors to be the sole factors used in decision-making. However, De Schutter and Ringelheim add to their concept that there is a systematic basis for these practices, which is in my opinion too narrow, as it would exclude racial or ethnic automated profiling that can be discriminatory in effect or incidental but not proven to be systematic.

Lastly, a body with specific expertise in discrimination, the European Commission against Racism and Intolerance (ECRI), defines 'racial profiling' as:

"The use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or national or ethnic origin, in control, surveillance or investigation activities".[876] So instead of using as a defining feature that these grounds are the sole or one of the main determining factors, the ECRI chooses to focus on objectivity and justification.

From the discussion on definitions above it is important to note that when racial or ethnic profiling is discussed, reference is often made to police profiling that relies at least in part, but not necessarily solely, on characteristics such as race, ethnicity, nationality and religion.

---

874 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 363.

875 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 362.

876 Council of Europe: European Commission Against Racism and Intolerance (ECRI), ECRI General Policy Recommendation N°11 on Combating racism and racial discrimination in policing, Adopted by ECRI on 29 June 2007, 4 October 2007, CRI(2007)39, https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/recommendation-no.11.

The focus in police profiling on race or ethnicity is certainly not a new development: the examples are numerous and date back decades. In 1999, a Chechen lawyer travelled by car from the Ingushetia Republic to Nalchik and was stopped and refused entry by police. Police officers had received an oral instruction from the Ministry of the Interior of the Kabardino-Balkaria Republic not to admit persons of Chechen ethnic origin. The order was aimed at preventing the infiltration into towns and villages by individuals with terrorist aspirations. The ECtHR ruled this practice a violation of the non-discrimination provision of article 14 ECHR in combination with the freedom of movement.[877] In the 1990s, in the USA, the term 'driving while black' was coined to describe the police practice of stopping African American or Hispanic drivers in disproportionate numbers compared to white drivers, under the pretext of minor traffic violations, to look for evidence of crimes such as drug trafficking.[878] Later, the term started being used more generally to refer to the influence of racial or ethnic factors in law enforcement decisions, whether in stop and search practices, anti-terrorism policing or other areas of policing work.[879]

Despite earlier examples, law enforcement profiling focusing on ethnicity, race, or religion has become much more prominent in reaction to terrorist bombings, such as in the USA in 2001, Madrid in 2004 and London in 2005, as well as in response to concerns over illegal immigration.[880] This increased importance of race, ethnicity and religion in law enforcement decision-making and profiling fueled the societal and scholarly debates on discrimination in policing even more, especially since the groups or minorities being increasingly targeted already suffer from disadvantage and stigmatization.[881] The EU even recommended Member States to construct profiles of terrorists on the basis of characteristics such as nationality, age, education, birthplace,

---

877 ECtHR, *Timishev v Russia* ECtHR (2nd section), App Nos 55762/00 and 55974/00, judgment of 13 December 2005.

878 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 360.

879 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 360.

880 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 5; D. Moeckli,'Discrimination Profiles: Law Enforcement After 9/11 and 7/7' (2005) 5 *European Human Rights Law Review* 517; J. Goldston,'Ethnic Profiling and Counter-Terrorism: Trends, Dangers and Alternatives' (2006) Open Society Justice Initiative, available at: https://www.justiceinitiative.org/publications/ethnic-profiling-and-counter-terrorism-trends-dangers-and-alternatives; O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008): 358-384.

881 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 358-359.

'psycho-sociological characteristics', or family situation, to aim to identify terrorists or to reveal the presence of terrorists in their territory, in cooperation with the immigration services and the police.[882] An example of risk profiling in relation to a factor such as ethnicity or religion can be seen in the German Rasterfahndung method, where police screened datasets of public and private bodies, such as universities, employers, and health and social insurance agencies, to track individuals presenting suspicious criteria.[883] These criteria, established at the national level, included various combinations of factors such as being male, Muslim, a national of or born in one of 26 listed countries with a predominantly Muslim population, a current or former student, or a legal resident in Germany.[884] In 2006 the Bundesverfassungsgericht ruled this Rasterfahndung method to be unconstitutional.[885] Nonetheless, in more recent case law, for example the ECtHR is still striking down law enforcement profiling practices as violations of the right to non-discrimination[886], meaning that practices of discriminatory racial or ethnic profiling are far from over.

Ethnic or 'racial' profiling has been widely studied and debated in the United States since the 1990s; in contrast, in Europe, this debate is younger.[887] Increasingly there is an interest in the topic in EU Member States, especially on a national level. According to the FRA in 2010, the UK especially had been building up research and policy responses to ethnic profiling, while the recognition of discriminatory ethnic police profiling had not developed to the same extent in other EU Member States.[888] For example, in 2021, the Netherlands Institute for Human Rights published a report in which they explain

---

882 JHA Council of 28 and 29 November 2002, Council of the EU doc 14817/02 (press 875), Annex II, 21. (For the recommendation itself, which is not mentioned in the summary of the conclusions, see Council of the EU doc. 11/11858/02.'Terrorist profile' is defined in this document as 'a set of physical, psychological or behavioural variables, which have been identified as typical of persons involved in terrorist activities and which may have some predictive value in that respect'.)

883 See, Lammerant, H., and P. De Hert. "Predictive profiling and its legal limits: Effectiveness gone forever." PP. 145-173, In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, or, O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), for more on this.

884 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008): 358-384.

885 Bundesverfassungsgericht, Decision of 4 April 2006 (1BvR 518/02) (2006) 59 Neue Juristische Wochenschrift 1939.

886 See for example *Lingurar v. Romania* (Application No. 48474/14), 16 April 2019.

887 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 360.

888 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 5.

the discrimination risks of risk profiling, especially focusing on the use of ethnicity or racial origin in risk profiling by governmental actors.[889]

5.3.2 The division between profiling related to protected grounds and unlawful discriminatory profiling

Factors that pertain to protected grounds such as race or ethnicity can play a role in policing, but the question is to what extent and in what context that is allowed. To determine to what extent these grounds can play a role, it is needed to fall back on the principle determining the threshold for a lot of police interference, namely 'reasonable suspicion'. The baseline of fundamental rights is that everyone should be treated in the same way, unless there is a specific reason to treat someone differently. For example, ethnicity, race or religion cannot be the sole reason for a police officer to use police powers, the officer must have something else to go on in addition. What this 'something else' amounts to depends on the requirements of national law, in most cases national law will require as a starting point that there are reasonable grounds that form a suspicion.[890] Furthermore, a guideline is that profiling should be based on objective and reasonable grounds, which, according to the FRA, has several implications: police powers such as stops and checks have to be based on reasonable and objective grounds of suspicion; personal characteristics can be used as legitimate factors but there must also be reasonable grounds for suspicion based on information other than protected characteristics; actions based on specific and up-to date intelligence are more likely to be objective; a decision to stop an individual or refer an individual for a check should not be based solely on an officer's feeling about them, as this risks being based on bias, stereotypes and/or prejudice.[891]

In chapter 2, I described that in risk profiling one can distinguish between practices of general policing and risk profiling used in specific criminal investigations and trials. For discrimination this distinction is relevant as well. Profiles can be based on specific intelligence, such as a suspect description. For example, specific intelligence suggests that a robbery will take place in a particular part of a city and that it will be carried out by a criminal organization with people of a Chinese nationality. Under these circumstances officers could perhaps consider racial appearance as relevant to

---

889 The Netherlands Institute for Human Rights, 'Discriminatie door risicoprofielen - Een mensenrechtelijk toetsingskader', available at: https://publicaties.mensenrechten.nl/publicatie/61a734e65d726f72c45f9dce.

890 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 20

891 European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide (2018). doi:10.2811/73473.

determining whether an individual becomes a potential suspect.[892] The more detailed a profile is and the more characteristics it includes, the less likely it is that it will rely heavily on broad categorizations, such as race, ethnicity or religion, and thus the less likely the profile is discriminatory.[893] National criminal law usually requires that there must be some reason other than this person's racial origin or ethnicity for the officer to treat this person differently from other members of the public and that the reason must be specific to this person and not a group trait.[894]

There are also profiles that are not based on specific intelligence, but are used for detecting crimes, predictive policing or general policing for public order, such as identifying individuals who might be secretively committing a crime or are likely to commit a crime in the future. These profiles are more reliant on educated assumptions derived from experience and training, or statistics and historical data, with a focus on suspect behaviour rather than racial, ethnic or religious characteristics.[895] For example, profiles can be used by police officers to search for individuals who repeatedly visit specific locations, meet and swap items before going separate ways, act nervously, or repeatedly make large cash purchases.[896] These profiles are more general, but still more focused on behaviour rather than categorizations such as race, ethnicity or religion. Over the past years, generally speaking, policing strategies such as the use of profiles have focused more on behaviour than on personal characteristics, to deal with problems of racial profiling such as present in stop and search practices.[897] When individuals are now identified as possibly dangerous it is done so on the basis of behaviour.[898]

---

892 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 20 & 21.

893 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 12-13.

894 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 20 & 21.

895 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 12-13.

896 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 12-13.

897 Van Brakel, R., and P. De Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies." *Technol. Led Policing* 20 (2011): p. 177.

898 Van Brakel, R., and P. De Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies." *Technol. Led Policing* 20 (2011): p. 177.

In contrast, when profiles are not focused on personal behaviour nor on specific intelligence, the risk of discrimination is significantly higher, since risk analysis will fall back on general categorizations. Traditional criminal profiling is focused on suspect descriptions and the suspects' mind or reasoning, whereas risk profiling is focused on possible behaviour, prediction and pre-emption.[899] The profiles are based to a large extent on generalizations about groups of people[900], which increases the risk of discrimination in predictive or pre-emptive profiling compared to traditional criminal profiling. Pre-emptive policing leads to social sorting where people are placed into categories based on assumed risk, such as whether people conform with norms. These assumptions or generalizations can lead to discrimination, for example when groups who match the profile suffer more government control.[901] The FRA concludes in its research that when profiles are not based on behaviour nor on specific intelligence, minorities from particular racial, ethnic or religious backgrounds could be routinely associated by the police with criminal behaviour, leading to discriminatory profiling.[902] The decision to take action then is determined by the race, ethnicity or religion of individuals, instead of other more relevant factors related to suspect behaviour.[903]

In addition to the type of policing that profiles are used for, and the type of intelligence used, the context in which police tasks are conducted matters as well. I distinguish between policing in the context of immigration, asylum and border control versus policing for other purposes. When profiles are used for policing in the context of possible illegal immigration or border control, factors such as nationality, race, ethnicity or religion are more likely to have relevance or to be admitted in decision-making than in policing for other purposes such as crowd control or investigations into violence, where such factors should be awarded less relevance in decision-

899 McCulloch, J., and D. Wilson. Pre-crime: Pre-emption, precaution and the future. Routledge, 2015.

900 D. Moeckli,'Discrimination Profiles: Law Enforcement After 9/11 and 7/7' (2005) 5 *European Human Rights Law Review* 517; D. Moeckli,'Terrorist profiling and the importance of a proactive approach to human rights protection' (16 December 2006), available at the Social Science Research Network (SSRN): http://ssrn.com/abstract=952163; O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 362.

901 Van Brakel, R., and P. De Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology-based strategies." *Technol. Led Policing* 20 (2011): p. 176; Lammerant, H., and P. De Hert. "Predictive profiling and its legal limits: Effectiveness gone forever." PP. 145-173, In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, p. 152.

902 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 12-13.

903 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 12-13.

making.[904] A good example of this can be found in recent Dutch case law: The Dutch Military Police uses ethnicity as a factor in decisions whether to submit an individual to a mobile screening at the internal borders of the EU to detect illegal migration. Several parties, such as Amnesty International, had started legal proceedings against the Dutch state claiming that the use of risk profiles for the mobile screenings or for making decisions whom to select and stop, where ethnicity is used as a factor, violate the principle of non-discrimination. However, the district court of The Hague ruled that the use of ethnicity here did not constitute illegal discrimination. According to the court, nationality can play an important role in these screenings and ethnicity can be an objective lead in determining an individual's potential nationality. However, the court does emphasize that ethnicity is never the only indicator and decisions on which individuals to stop and check have to be explainable. Performing random checks or not selecting at all and checking all individuals are not viable alternatives in this case. Thus, the court finds that the use of ethnicity is admissible.[905]

The FRA distinguishes between organizational and operational profiling and what this means for discrimination.[906] As I explain below, this distinction in my opinion does not have much added value. Unlawful discriminatory profiling would be relatively easy to identify at the organizational level, according to the FRA. One can think for example of explicit written or oral instructions issued at a high level in the chain of authority instructing police officers to target particular groups with enforcement actions. When profiling is used at an operational level, it would often be used in a more subtle manner, such as individual police officers applying stereotypes or generalizations based on race, ethnicity or religion. This profiling could be done somewhat consciously based on personal prejudices, or it can be that police officers are not conscious of the degree to which they are applying generalizations and stereotypes.[907] This distinction that the FRA makes in more traditional forms of profiling can be translated to the practices of risk profiling researched in this dissertation, which are more automated. The risk profiling system or algorithm is trained with specific data and programmed with a specific goal, such as to find individuals who commit fraud. If the system makes use of data with a negative bias towards people of a specific race, ethnicity, or

---

904 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 11.

905 22 September 2021, District Court The Hague, ECLI:NL:RBDHA:2021:10283.

906 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 13.

907 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 13.

religion, for instance because their data are overrepresented, or if the risk categories themselves are based on factors such as race, ethnicity, or religion, this poses a risk of organizational discrimination. Whether intentional or not, the risk profiling system then has instructions to create profiles that are based on factors such as race, ethnicity, or religion. If the risk profiling system creates a suspect profile, and an individual police officer decides, consciously or not, to focus the search on the factors of race, ethnicity, or religion from those profiles, or awards those factors a higher risk level than factors such as discrepancies in bank statements, it can amount to discriminatory profiling on an operational level. De Schutter and Ringelheim make a distinction similar to an organizational and operational level, by distinguishing between formal ethnic profiling where competent authorities establish the profile, and informal ethnic profiling where it is a de facto practice based on law enforcement officers' memories of significant experiences or assumptions about the typical features of offenders.[908] Formal profiles can be deployed by law enforcement officers to try and identify people who meet the characteristics by automatic means through the screening of data, or directly on the ground based on visual observation and in-person identity checks.[909]

The question is whether this type of distinction, between more organizational and operational profiling, and this assumption that it is easier to identify discrimination in organizational profiling than in operational profiling, is meaningful. Partially in support of the FRA's view, Barocas and Selbst for example, in their seminal work on the disparate impact of Big Data technology, put forward that discrimination through data mining is almost always unintentional and related to the algorithm's use rather than a conscious choice by its developers, with the result that it can be unusually hard to identify the source of the discriminatory problem.[910] This argument aligns with the FRA statement in that discrimination here stems more from operationalization and is difficult to detect in use. On the other hand, this stance can be criticized. For example, Van Brakel rightly points out that the observation by Barocas and Selbst is not underpinned by empirical evidence, and that one can also argue that, especially in the context of anti-terrorism and anti-radicalization policies, this observation is not entirely true as the discrimination in this context is possibly a conscious choice

---

908 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 362. See also: D. A. Harris, *Profiles in Injustice - Why Racial Profiling Cannot Work* (New York: The New Press, 2002) 16-18.

909 O. De Schutter & J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008), p. 362.

910 Barocas, S. and Selbst, A.D., Big Data's Disparate Impact. 104 *California Law Review* 671 (2016), Available at SSRN: https://ssrn.com/abstract=2477899.

by the programmers as a form of ethnic or racial profiling.[911] Following this line of reasoning brings us back full circle in that especially in automated profiling, and especially in certain law enforcement contexts such as anti-terrorism policy, racial or ethnic profiling can actually be a choice, whether valid or not, and be completely intertwined with the system. That could mean that organizational discrimination is maybe just as difficult to signal as operational discrimination, especially in complex algorithmic systems where it is not clear how design choices relate to results. In addition, organizational discrimination is certainly just as difficult to challenge as operational discrimination, as the individuals or groups suffering from such profiling do not have the necessary information about the organization or system, such as the risk factors that the system is based on or the data that is processed in the system. So it would be better to not over-target operational discrimination as the main issue.

In chapter 2, I distinguished between risk profiling pertaining to individuals and to locations.[912] While the risk of discriminatory profiling is the highest when profiles concern individuals or groups, as the profiles include possible protected grounds, profiles pertaining to geographical areas are not excluded from discriminatory effects. Just as in chapter 3, I can point to discussions of stigmatization and self-fulfilling prophecies.[913] If, for example, data on arrest records are used as a factor in predicting which areas are high risk for crime and thus require more police patrols, and the arrest rates are disproportionately higher for certain groups due to minorities living in that area, this bias exacerbates discrimination against those groups.[914] Reliance on a stereotyping profile can also increase the overall offending rate for that crime over time, because people who are criminally stereotyped may – for instance, when tired of being stopped and searched all the time – decide to live up to that stereotype, and because groups that are not associated with certain crimes may be able to commit

---

911 Van Brakel, R. "Pre-emptive big data surveillance and its (dis) empowering consequences: The case of predictive policing." In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, pp. 117-141: p. 125.

912 See chapter 2 and 3, on hotspot policing and the use of the Dutch Crime Anticipation System.

913 See also Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12.

914 See for example: Van Brakel, R. "Pre-emptive big data surveillance and its (dis) empowering consequences: The case of predictive policing." In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, pp. 117-141: p. 125; Schuilenburg, M. "Predictive policing: de opkomst van een gedachtenpolitie." *Ars Aequi* 65, no. 12 (2016): 931-936, p. 935.

these crimes while police focus on another group.[915] Patterns of offending can thus respond to and mirror patterns of policing.[916] For these reasons one should not exclude risk profiles of locations from an assessment of non-discrimination.

5.4. EU & CoE non-discrimination law: article 14 ECHR & article 21 CFREU

5.4.1. The system of non-discrimination law

Given the problems of discriminatory law enforcement profiling described in the previous sections, especially when it concerns group traits such as race, ethnicity, nationality and religion, it is useful to analyze how such a differential treatment is regulated from the legal perspective. This helps in understanding whether such discrimination is lawful or unlawful.

A first glance at non-discrimination law in the European context reveals two complex layered systems, the system of EU non-discrimination law and of CoE non-discrimination law, both consisting of a variety of instruments and provisions.

For the CoE, a prohibition of discrimination is established in article 14 of the ECHR from 1953, which guarantees equal treatment in the enjoyment of the other rights set out in the Convention. The provision reads as follows:

> *"The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."*

---

915 Harcourt B., 'Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally', 71.4 *University of Chicago Law Review* (2004); European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 37.

916 See also chapter 3, section 3.3 & 3.4; Harcourt B., 'Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally', 71.4 *University of Chicago Law Review* (2004); European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 37.

In 2000, Protocol 12 to the ECHR[917] was adopted, which expands the scope of the prohibition of discrimination to not just include non-discrimination in rights under the Convention, but also to equal treatment in the enjoyment of any right, including rights in other CoE instruments and under national laws. Article 14 ECHR, and its expanded scope through Protocol 12, is further shaped through case law of the ECtHR. In addition to the ECHR, the Council of Europe's other main human rights treaty is the European Social Charter (ESC), the ESC being the counterpart of the ECHR in the sphere of economic and social rights. Since 1996, the ESC contains a general discrimination prohibition in article E, which determines that enjoyment of the rights in the ESC shall be secured without discrimination based on similar protected grounds to the ECHR.[918] For the law enforcement context the ESC is not relevant so I will focus on article 14 ECHR.

In 1957 the EU adopted the Treaty of Rome, which required, inter alia, equal pay between men and women and prohibited discrimination on grounds of nationality between Member States. While secondary instruments related to gender equality in employment originated afterwards in the 1970s[919], it was not until 1997 when the Treaty of Amsterdam was adopted that the EU created the power to combat discrimination on various grounds, namely sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.[920] In 2000, two directives were adopted, the Employment Equality Directive (2000/78/EC) and the Racial Equality Directive (2000/43/EC), focusing on the context of employment, welfare and social security. After the Lisbon Treaty entered into force in 2009, the powers of the EU relating to non-discrimination were enhanced and since then there is a growing convergence between the EU human rights framework –including rights of equality – and other jurisdictions such as the CoE and United Nations.[921] The EU non-discrimination law now consists of legislative

917 Protocol no. 12. to the Convention for the protection of human rights and fundamental freedoms, Rome, 4.XI.2000, No. 177.

918 The ESC includes health as a protected ground, which is not present under article 14 ECHR; article 14 ECHR includes property as a protected ground, which is not present in article E of the ESC.

919 Such as the Equal Pay Directive of 1975 and the Equal Treatment Directive of 1976.

920 This power follows from article 13 of the Treaty of the European Community.

921 The European Union Agency for Fundamental Rights, Handbook on European non-discrimination law. Luxembourg: Publications Office of the European Union, 2018. doi:10.2811/792676.

measures (such as non-discrimination directives)[922], provisions of the EU treaties,[923] the CFREU[924] and the jurisprudence of the CJEU.[925] The use by the EU legislator of various directives to regulate discrimination in different contexts has been criticized as being too fragmented an approach, resulting in an asymmetrical scope for EU non-discrimination law where what is considered illegal discrimination differs depending on which protected ground is at stake.[926] Article 21 CFREU is the one provision of EU non-discrimination law that contains a general non-discrimination principle, regardless of the context. The provision reads as follows:

> *"1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.*
>
> *2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited."*

Article 21 CFREU provides a constitutional anchorage to the judiciary with a clearer mandate to enforce the right to equal treatment.[927] Article 21 CFREU links to the

---

922 The Employment Equality Directive (2000/78/EC), Racial Equality Directive (2000/43/EC), Gender Goods and Services Directive (2004/113/EC), Gender Equality Directive (recast) (2006/54/EC), Equal Treatment Directive (recast) 2006/54/EC (5 July 2006), Commission Recommendation 92/131/EEC on the protection of the dignity of women and men at work, Council declaration on the implementation of the Commission Recommendation on the protection of the dignity of women and men at work (19 December 1991), Council Directive 79/7/EEC on the progressive implementation of the principle of equal treatment for men and women in matters of social security (19 December 1978).

923 Articles 2, 3 (3), and 9 of the Treaty on the European Union and article 10 of Treaty on the functioning of the European Union.

924 Articles 20 (equality before the law) of the EU Charter of Fundamental Rights and 21 (non-discrimination) of the EU Charter of Fundamental Rights.

925 For a complete discussion on all discrimination law provisions of both jurisdictions, see the European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law*. Luxembourg: Publications Office of the European Union, 2018. doi:10.2811/792676.

926 Gellert, R., K. De Vries, P. De Hert, and S. Gutwirth. "A comparative analysis of anti-discrimination and data protection legislations." In: *Discrimination and privacy in the information society*. Springer, Berlin, Heidelberg, 2013. Similarly, as a critique on a lack of horizontal approach or lack of foundation see: O'Cinneide, C., "The uncertain foundations of contemporary anti-discrimination law." *International Journal of Discrimination and the Law* 11, no. 1-2 (2011): 7-28; Zaccaroni, G., "Differentiating Equality? The Different Advancements in the Protected Grounds in the Case Law of the European Court of Justice." In: *The Principle of Equality in EU Law*, pp. 167-195. Springer, Cham, 2017.

927 Muir, E. "The Essence of the Fundamental Right to Equal Treatment: Back to the Origins." *German Law Journal* 20, no. 6 (2019): 817-839.

various secondary EU laws providing protection on specific grounds, but the wording of article 21 CFREU is broader than those instruments, containing an open list of grounds, as will be discussed in the next section. Nonetheless, article 21 CFREU only offers protection against discrimination by Member States in implementing Union law and against discrimination by Union bodies.[928] Article 21 CFREU does not create powers to enact further non-discrimination laws; instead it only addresses discrimination by EU institutions and bodies, when exercising their powers conferred by the Treaties, and discrimination by Member States but only in implementing Union Law.[929] A proposal was presented in 2008 by the European Commission for a Council directive on implementing the principle of equal treatment outside of the labour market, aiming at extending protection against discrimination through a horizontal approach.[930] However, unanimity has still not been reached in the Council on this proposal and the draft has remained blocked at that stage since then.[931] Because individuals are not able to file a complaint with the CJEU directly, the case law of the CJEU does not deal with cases between states and individuals for non-discrimination. Therefore, for this chapter the case law of the ECtHR is central, also because the ECtHR assesses discrimination in national legislation as well.

It is not exactly clear to what degree there is convergence between CoE non-discrimination law and EU non-discrimination law.[932] For example, while article 21 CFREU refers to a ban against discrimination 'on any ground' it does not refer to 'other status', like article 14 ECHR does. One can at least argue that the ECHR can be seen as a common baseline of human rights protection, and the CFREU should not be interpreted as offering a lower level of protection than the ECHR.[933] While interpreting

928 Kilpatrick, C. "Non-Discrimination." In: *The EU Charter of Fundamental Rights: A Commentary*. Ed. S. Peers, T. Hervey, J. Kenner and A. Ward. London: Hart Publishing, 2014. 579–604. Bloomsbury Collections. Web. 24 Jul. 2018. <http://dx.doi.org/10.5040/9781849468350.ch-024>.

929 Eklund, H. & Kilpatrick, C., Article 21 EU charter of fundamental rights, European University Institute: Academy of European Law, AEL working Paper 2021/01, ISSN 1831-4066, available at: https://hdl.handle.net/1814/71418.

930 For more on this see: Zaccaroni, G. "Differentiating Equality? The Different Advancements in the Protected Grounds in the Case Law of the European Court of Justice." In: *The Principle of Equality in EU Law*, pp. 167-195. Springer, Cham, 2017.

931 See: European Parliament, Legislative Train Schedule, 'Anti-discrimination directive: In "A New Push for European Democracy", available at: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-anti-discrimination-directive, last accessed 20-10-2021.

932 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 668.

933 See for example article 52(3) CFREU and in article 6(3) of the Treaty on European Union [2008] OJ C 115/01.

a general principle of equality or non-discrimination is very difficult,[934] the approach of both the CJEU and the ECtHR in non-discrimination analysis has been criticized for not explaining the *ratio legis* of the discrimination laws.[935] This has led scholars to put forward different constructions to attempt to explain the theoretical basis for non-discrimination under the ECHR.[936] Ultimately, this means that to understand the different aspects of article 14 ECHR and article 21 CFREU, such as the protected grounds they are built on and the requirements for justifications for discrimination, examining case law and assessing the main lines of reasoning therein is crucial, as is done in the following sections.

It is inherent for fundamental rights or human rights to aim to treat all human beings equally, that is why almost all fundamental right instruments guarantee equality and non-discrimination, and specialized instruments provide protection against specific types of discrimination.[937] The terms equality and non-discrimination are related, they can be seen as the positive or negative formulation of the same principle. Equality requires that equals are treated equally, and the prohibition of discrimination prevents differential treatment on unreasonable grounds.[938] The ECHR focuses on the negative formulation, creating a prohibition for discrimination for states to adhere to. In contrast, for example, the CFEU contains both a principle of equality and a principle of non-discrimination.[939] It is important to keep this context in mind for the following

---

934 Westen, 'The Empty Idea of Equality' (1982) 95 *Harvard Law Review* 537; Greenawalt, 'How Empty is the Idea of Equality?' (1983) 83 *Columbia Law Review* 1167.

935 Small, 'Structure and Substance: Developing a Practical and Effective Prohibition on Discrimination under the European Convention on Human Rights' (2003) 6 *International Journal of Discrimination and the Law* 45; Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 663-664; O'Cinneide, C. "The uncertain foundations of contemporary anti-discrimination law." *International Journal of Discrimination and the Law* 11, no. 1-2 (2011): 7-28.

936 Arnardóttir, 'Non-discrimination in International and European Law: Towards Substantive Models' (2007) 25 *Nordic Journal of Human Rights* 140 at 146–9; O'Connell, 'Cinderella comes to the Ball: Art 14 and the right to non-discrimination in the ECHR' (2009) 29 *Legal Studies* 211 at 228; Fredman, 'Providing Equality: Substantive Equality and the Positive Duty to Provide' (2005) 21 *South African Journal on Human Rights* 163; Gerards, 'The Discrimination Grounds of Article 14 of the European Convention on Human Rights' (2013) 13 *Human Rights Law Review* 99; De Schutter, 'Three Models of Equality and European Anti-Discrimination Law' (2006) 57 *Northern Ireland Legal Quarterly* 1; and Kimber, 'Equality or Self-Determination', in: *Gearty and Tomkins (eds), Understanding Human Rights* (London: Mansell, 1996) 266.

937 Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234, p. 148.

938 Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234, p. 149.

939 Article 20 (equality before the law) of the EU Charter of Fundamental Rights and 21 (non-discrimination) of the EU Charter of Fundamental Rights.

legal discussion that article 14 ECHR focuses on the states who have to justify an infringement of the prohibition of non-discrimination.

Discrimination law aims to strike a peculiar balance. On the one hand we want to treat people based on their own, individual, characteristics or merits. On the other hand, treatment of individuals based on individual characteristics such as their status, group membership, or irrelevant physical characteristics might not always be fair. Nonetheless not every distinction is discriminatory, for example, governments classify people into groups for a wide variety of reasons and a lot of those reasons are in fact legitimate. The challenge of discrimination law is how to determine which distinctions are considered discriminatory, and under which conditions this is unlawful or not.[940]

Non-discrimination law requires that comparable situations are not treated differently and that non-comparable situations are treated differently.[941] The ECtHR considers discrimination under the ECHR to be "*differences in treatment but only those based on an identifiable, objective or personal characteristic, or "status", by which persons or groups of persons are distinguishable from one another*".[942] I would say that non-discrimination law is focused on an 'end result', as it deals with the qualification of a difference of treatment, and not with the specificities of the practice leading up to the discriminatory or non-discriminatory 'end result'.[943] Non-discrimination law determines what is seen as a legitimate end-result, thus what treatment or outcome constitutes discrimination and which treatment or outcome does not. What differential treatment or outcome is considered discriminatory will for a large part depend on the justification proposed by the state, in this case the national law enforcement actors. Therefore, the justification

---

940 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 16; S. Fredman, *Discrimination Law*, Oxford University Press, 2011. 9780199584437, p. 109; Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, ISBN 0198767234, p. 148.

941 See for example: Muir, Elise. "The Essence of the Fundamental Right to Equal Treatment: Back to the Origins." *German Law Journal* 20, no. 6 (2019): 817-839; Lammerant, H., and P. De Hert. "Predictive profiling and its legal limits: Effectiveness gone forever." In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). (2016). Exploring the boundaries of big data*, p. 158; Judgment of the Court (Grand Chamber) of 16 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, ECLI:EU:C:2008:724.

942 ECtHR, *Molla Sali v. Greece* [GC], 2018, para. 134; ECtHR, *Fábián v. Hungary* [GC], 2017, para. 113; ECtHR, *Kiyutin v. Russia*, 2011, para. 56.

943 This focus of non-discrimination law on a certain end goal, rather than on offering safeguards during a certain process, can be clearly seen in its contrast to the approach behind data protection law, as explained in: Gellert, R., K. De Vries, P. De Hert, and S. Gutwirth. "A comparative analysis of anti-discrimination and data protection legislations." In: *Discrimination and privacy in the information society.* Springer, Berlin, Heidelberg, 2013, p. 66.

of different treatment is a central concept in non-discrimination law, as is discussed in detail in section 5.4.4.

According to the text of the ECHR, the core objective of non-discrimination is to ensure that people can enjoy their fundamental rights equally.[944] One could argue that the prohibition on discrimination is therefore focused on achieving a result, this equal enjoyment of rights.[945] Each piece of non-discrimination law further defines this result to be achieved in a certain context, such as achieving equal treatment for men and women in employment rights, or equal treatment in the right to education regardless of ethnicity. Because discrimination is attached to the notion of equal enjoyment of rights, the right to non-discrimination cannot be seen as separate from other rights. Article 14 ECHR therefore is an ancillary right, which means that for law enforcement profiling the right to non-discrimination needs to be read together with the fundamental rights to data protection and privacy and fundamental rights under criminal procedural law.[946] The ECtHR has frequently underlined that article 14 ECHR complements the substantive provisions of the Convention and Protocols, meaning that article 14 ECHR has no independent existence but forms an integral part of each of the rights and freedoms.[947] In the case of risk profiling, discrimination can for example mean that an individual does not enjoy the right to fair trial similarly to other individuals, or that an individual does not have equal enjoyment of the right to privacy. While Protocol 12 to the ECHR has expanded the scope to include differential treatment in the enjoyment of rights to rights outside of the ECHR, it did not erase the ancillary nature of the right to non-discrimination under CoE law. This ancillary nature of article 14 ECHR has led to debates from time to time concerning the added value of having a right to non-discrimination as such, depending on how the ECtHR

944 See for example article 14 ECHR: "The enjoyment of the rights and freedoms set forth in the European Convention on Human Rights and the Human Rights Act shall be secured without discrimination…".

945 There is also a discussion on substantive equality, but it is tied more to the right to equality than the prohibition of discrimination, see for example: S. Fredman, Substantive equality revisited, *International Journal of Constitutional Law*, Volume 14, Issue 3, July 2016, Pages 712–738, https://doi.org/10.1093/icon/mow043.

946 See chapter 4 for the assessment of the right to data protection and chapter 6 for rights under criminal procedural law and the holistic analysis in chapter 7 to see what the right to non-discrimination means in relation to these other rights.

947 European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

assesses the right in combination to violation of other fundamental rights.[948] As other fundamental rights are discussed in other chapters of this dissertation, I will discuss the assessment of non-discrimination as such in this chapter and assess its added value in the context of how it can regulate profiling.

5.4.2. The protected grounds

Both EU and CoE non-discrimination law work with a system of protected grounds. To explain further how their protected grounds systems work, I need to take a step back. One can distinguish between three ways in which non-discrimination laws globally make use of protected grounds.[949] The first way is to have an exhaustive list of grounds. This system can be found in UK non-discrimination law and some specific EU instruments. A second way to use protected grounds is the opposite, framing a broad and open-ended equality requirement without including particular grounds. This approach leaves it mainly open to case law to set out when a differential treatment is prohibited or not. Such an approach can be found in the constitution of the USA. The third approach is a mix of the first and second, in which there is a non-exhaustive list of protected grounds, using terminology such as 'grounds such as…', 'including…', 'in particular…', or 'other status'. This mixed approach gives some leeway to courts to expand the protected grounds.[950] This non-exhaustive enumeration is used under both the ECHR and the CFREU.[951] A list of protected grounds is in the text of article 14 ECHR and article 21 CFREU but article 14 ECHR uses the terminology 'such as…or other status' and article 21 CFREU uses 'such as…' to indicate that this enumeration is not exhaustive.

The political or social context has a major influence on the enumeration or focus of protected grounds. What is seen as equality is determined by politics, for the principle to have meaning, it must incorporate some values that determine which persons and treatments are important.[952] Thus it is needed to give substance to the idea by

---

948 For an elaborate discussion on the importance of having the right of non-discrimination as a separate fundamental right, despite its ancillary nature, see Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar*. SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913; The European Union Agency for Fundamental Rights, Handbook on European non-discrimination law. Luxembourg: Publications Office of the European Union, 2018. doi:10.2811/792676.

949 S. Fredman, *Discrimination Law*, Oxford University Press, 2011. 9780199584437 p. 112.

950 S. Fredman, *Discrimination Law*, Oxford University Press, 2011. 9780199584437 p. 112.

951 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 648.

952 Westen, P. "The empty idea of equality." *Harvard Law Review* (1982): 537-596; see also Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234, p. 148-149.

specific legislation on which criteria are used to assess what is acceptable.[953] Non-discrimination law, as the negative formulation of equality, determines which grounds for discrimination that particular society or jurisdiction chooses to focus on. In the USA, the development of non-discrimination law began with racial discrimination, while in the EU non-discrimination law started out with a focus on nationality and gender as a post-World War II context shaped the original protected grounds of the ECHR.[954] While in the USA racial divides had a large impact on society, in the EU context the attention went also to the creation of a common market, which sparked the interest in discrimination based on nationality and wages discrimination between genders as a means to rule out competitive advantages between Member States.[955]

Having the enumeration of protected grounds as non-exhaustive, such as under the ECHR and CFREU, has allowed courts to alter the protected grounds according to present-day conditions.[956] In the case of the ECHR, the ECtHR can also be said to have been reluctant in using fixed categories of grounds, instead treating the grounds as a fluid concept. This flexibility has led scholars to put forward that it is very rare for a case to be dismissed for not pertaining to discrimination based on a particular protected ground and that any discrimination ground can in principle be included in the scope of protection.[957] The Council of Europe in its explanatory report to Protocol 12 to the ECHR emphasizes as well that the grounds under the ECHR are not exhaustive and the addition of new particular grounds can give rise to unwarranted *a contrario* interpretations towards grounds not included. It is up to the ECtHR to apply non-discrimination law to grounds that are not included in the ECHR and the ECtHR has already done so in the past regarding article 14 ECHR.[958] The ECtHR can

---

953 Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234, p. 149.

954 S. Fredman, *Discrimination Law*, Oxford University Press, 2011. 9780199584437, p. 110

955 S. Fredman, *Discrimination Law*, Oxford University Press, 2011. 9780199584437 p. 114.

956 ECtHR, *EB v France* (2008) 47 EHRR 21, para 92.

957 For example, see: S. Fredman, *Discrimination Law*, Oxford University Press, 2011. 9780199584437 p. 125; Arnardóttir, Oddný Mjöll. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 648; The Council of Europe and the European Union Agency for Fundamental Rights, *Handbook on European Non-Discrimination Law* (Luxembourg: Publications Office of the European Union, 2011) p. 85; Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar*. SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913; Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

958 Council of Europe, 'Explanatory Report to the Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 XI. 2000)' <https://rm.coe.int/16800cce48>.

be lauded for flexibility in reviewing discrimination cases that pertain to a plethora of protected grounds. The requirement of discrimination pertaining to a protected ground to receive fundamental rights protection is thus not such a high threshold. Yet, the system of protected grounds does not protect fully against discrimination in risk profiling. There are multiple reasons for this, or challenges in applying non-discrimination law to risk profiling, which this section outlines.

5.4.2.1 Differentiating between protected grounds

The first challenge regarding applying non-discrimination law is that it might appear as if the courts consider all possible grounds equally, but in fact the ECtHR applies a certain hierarchy. The baseline idea is that any discrimination ground can come under the scope of protection of article 14 of the ECHR in the formal sense, but the ECtHR differentiates between the discrimination grounds when reviewing the possible justification for discrimination, thus applying a hierarchy. One the one hand there are the 'suspect' discrimination grounds where the states' margin of appreciation is narrower and it is most common for the ECtHR to find violations of article 14 ECHR as it applies a strict review.[959] The suspect grounds have been developed on an ad hoc basis in ECtHR case law; they include at least sex or gender[960], race or ethnic origin[961], religion[962], and disability[963].[964] On the other end of the spectrum, there are grounds that are labelled as being lower in the hierarchy, such as property, language, age, marriage

959 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 649; More on the justification and margin of appreciation therein can be found in section 5.2.4 of this chapter.

960 For example: ECtHR, *Abdulaziz, Cabales and Balkandali v United Kingdom* 1985 para 78; ECtHR, *Konstantin Markin v Russia* 2012, para 127.

961 For example: ECtHR, *Cyprus v Turkey* 2001, para 306; ECtHR, *Timishev v Russia* 2005, para 56.

962 For example: ECtHR, *Hoffmann v Austria* 1993, para 36; ECtHR, *Milanovic´ v Serbia* 2010, para 97.

963 For example: ECtHR, *Glor v Switzerland* 2009, para 84; *Kiyutin v Russia* 2011, para 64.

964 Since there is a mutual relationship between the case law of the CJEU and ECtHR for non-discrimination, it is not very surprising that the suspect grounds of the ECtHR mirror the discrimination grounds of the Amsterdam Treaty of 1997 that lays the basis for EU non-discrimination law. Also in the EU, non-discrimination directives aim to harmonize legislation for these protected grounds and thus create even more legitimacy for their special significance and the need to take a strict approach to any different treatment based on these discrimination grounds. See: Article 2(7) Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts [1997] OJ C 340/01; Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 651.

status, employment status, or education.[965] With the ECtHR using different levels of scrutiny for the various protected grounds comes a need to determine which category is relevant in a particular case.[966] Thus while the ECtHR claims to use a fluid approach towards protected grounds, it still aims to label differential treatment as pertaining to a particular ground to assess which level of scrutiny to apply. In other words, for article 14 ECHR to apply it does not matter really which ground the differential treatment is based on, but it does matter for the intensity of the scrutiny applied by the courts, rendering the distinction important nonetheless.[967]

The ECtHR is still focused on labelling and trying to fit discrimination in a certain category, while in reality, discrimination can take place based on a complex combination of factors, such as race, age, education, financial status, family size and so on. The ECtHR has ruled on cases involving multiple protected grounds,[968] but it is not clear if the ECtHR is completely prepared to handle the complex relations between the different characteristics in profiles.

A related complexity is that of intersectionality[969] of discrimination. For example, how should discrimination be assessed when the risk profile potentially includes racial origin, religion and gender? This is a challenge for non-discrimination law that is broader than just in its application to profiling, but opaque differential processes such as profiling certainly make the discussion even more important. The use of varied sources and types of data, and the focus on sometimes opaque correlations, create more entanglement of protected identities, forming new groups of people that can experience intersectional discrimination.[970] The phenomenon of intersectional

---

965 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 654-655.

966 S. Fredman, *Discrimination Law*, Oxford University Press, 2011. 9780199584437 p. 127.

967 Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar*. SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913; Arnardóttir, O M. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 666.

968 European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

969 See for example: Solanke, 'Putting Race and Gender Together: A New Approach to Intersectionality' (2009) 72 *Modern Law Review* 723; Timmer, 'Toward an Anti-Stereotyping Approach for the European Court of Human Rights' (2011) 11 *Human Rights Law Review* 707.

970 Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719895805, p. 5.

discrimination refers to the specific disadvantage borne by those discriminated against on more than one ground.[971] The idea is that to assess intersectional discrimination one cannot simply add together the grounds of discrimination, such as someone is discriminated against based on race, religion, and gender. Rather, with intersectional discrimination, someone suffers a specific form of discrimination being at the intersection of different characteristics. For example, being a black woman who suffers discrimination in the form of a distinctive melding of race and gender.[972] In risk profiling lies a pitfall of creating new forms of intersectional discrimination, possibly without even being aware of it, as risk profiling systems can create all kinds of categorizations based on various personal characteristics.[973]

Some authors put forward that currently EU non-discrimination law does not protect against intersectional discrimination and that adaption of EU discrimination legislation to the specificities of intersectional discrimination is necessary.[974] In this aspect I would argue that there is a difference between the CoE and EU approach to non-discrimination. While it is unclear how flexible the ECtHR actually is in its assessment of applicable grounds, the flexible approach to grounds under article 14 ECHR can be argued to be preferable to the system of EU non-discrimination law which relies on different instruments for different grounds. The focus of the EU non-discrimination directives on an exhaustive list of discrimination grounds or analysis by courts from the perspective of a single ground at a time, is less well equipped to

971 See for example Eklund, H. & Kilpatrick, C., Article 21 EU charter of fundamental rights, European University Institute: Academy of European Law, AEL working Paper 2021/01, ISSN 1831-4066, available at: https://hdl.handle.net/1814/71418; D Schiek and A Lawson (eds), EU Non-Discrimination Law and Intersectionality—Investigating the Triangle between Racial, Gender and Disability Discrimination (Aldershot, Ashgate, 2011); I. Solanke, 'Putting Race and Gender Together: A New Approach to Intersectionality' (2009) 72 *Modern Law Review* 723.

972 Eklund, H. & Kilpatrick, C., Article 21 EU charter of fundamental rights, European University Institute: Academy of European Law, AEL working Paper 2021/01, ISSN 1831-4066, available at: https://hdl.handle.net/1814/71418.

973 Leese M (2014) The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European union. *Security Dialogue* 45(5): 494–511, p. 504.

974 Eklund, H. & Kilpatrick, C., Article 21 EU charter of fundamental rights, European University Institute: Academy of European Law, AEL working Paper 2021/01, ISSN 1831-4066, available at: https://hdl.handle.net/1814/71418; Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719895805, p. 5.

handle complex situations where several grounds combine or intersect.[975] In fact, an approach with an enumerated list of grounds such as in the EU secondary instruments rejects intersectionality. This follows for example from the CJEU's ruling in *David L. Parris v Trinity College Dublin and Others*. The CJEU states that:

> *"(…)the referring court essentially asks whether Articles 2 and 6(2) of Directive 2000/78 must be interpreted as meaning that a national rule such as that at issue in the main proceedings is capable of creating discrimination as a result of the combined effect of sexual orientation and age, where that rule does not constitute discrimination either on the ground of sexual orientation or on the ground of age taken in isolation. In this respect, while discrimination may indeed be based on several of the grounds set out in Article 1 of Directive 2000/78, there is, however, no new category of discrimination resulting from the combination of more than one of those grounds, such as sexual orientation and age, that may be found to exist where discrimination on the basis of those grounds taken in isolation has not been established. Consequently, where a national rule creates neither discrimination on the ground of sexual orientation nor discrimination on the ground of age, that rule cannot produce discrimination on the basis of the combination of those two factors".*[976]

For risk profiling I believe we need an approach to non-discrimination that is much more flexible and tackles differentiation towards individuals or groups based on a single ground (e.g. being black), based on multiple grounds (e.g. being black and a woman), and based on an intersection of different grounds that creates a new protected group (e.g. being a black woman that works part-time and receives social benefits).

The focus of the current legislative approach of non-discrimination law on singular protected grounds does not work well for risk profiling. In the case of profiling,

---

[975] Arnardóttir, 'Multidimensional Equality from Within: Themes from the European Convention on Human Rights', in Schiek and Chege (eds), European Union Non-Discrimination Law: Comparative Perspectives on Multidimensional Equality Law (London: Routledge-Cavendish, 2009) 53 at 60–1; Fredman, 'Double Trouble: Multiple Discrimination and EU Law' (2005) 2 *European Anti-Discrimination Law Review* 13 at 16; Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics' (1989) *University of Chicago Legal Forum* 139 at 166–7; Hannett, 'Equality at the Intersections: The Legislative and Judicial Failure to Tackle Multiple Discrimination' (2003) 23 *Oxford Journal of Legal Studies* 65 at 69–70; Neuvonen, Päivi Johanna. "'Inequality in equality'in the European Union equality directives: A friend or a foe of more systematized relationships between the protected grounds?." *International Journal of Discrimination and the Law* 15, no. 4 (2015): 222-240.

[976] CJEU, Judgment of the Court (First Chamber) of 24 November 2016, *David L. Parris v Trinity College Dublin and Others*, Case C-443/15, para 79-81.

categories of grounds are blurring, rendering it difficult for all parties involved to determine which category someone is classified in and thus whether the category pertains to for example someone being of a certain nationality, owning a certain type of car, or living in a certain zip code. It is a challenge for non-discrimination law to be applied to profiling in that sense, as non-discrimination law is considered an instrument that serves the protection of specific groups, represented by specific traits, while data-driven profiling such as risk profiling causes the generation of new groups, where relevant traits or parameters are not simply a reflection of specific or tangible characteristics or traits.[977] Not only can it be difficult with profiling to pin differential treatment to a certain protected ground, the factor that underlies the differential treatment can change over time or become more difficult to grasp. Naudts illustrates this problem clearly in the following example:

> *"(…)analytics might show a correlation between geographic location, income and deviant behaviour. The combination of those parameters could serve as a proxy for ethnicity, e.g. when they would refer to a lower-income area where mainly minorities are living. A data-driven policy to heighten the control of that area however not only impacts those people that share the protected characteristic that is ethnicity. Due to the generalised nature of the profile, it will impact a larger group, i.e. all people living within that location, and as such the profile becomes, at least partially, detached from the parameter 'ethnicity'".*[978]

In this example, the differential treatment started out being based on ethnicity, or proxies for that ground, but over time it becomes based on the profile itself. This is the crucial point for profiling. The debate should not be on whether the grounds that non-discrimination law is based on are exhaustive or not, or which grounds are protected, but rather whether having a system reliant on protected ground works as

---

977 L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96; L. Naudts, 'How Machine Learning Generates Unfair Inequalities and How Data Protection Instruments May Help in Mitigating Them', in R. Leenes and others (eds) in: *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2019) ch 3; A. Vedder and L. Naudts, 'Accountability for the Use of Algorithms in a Big Data Environment' (2017) 31 *International Review of Law, Computers & Technology* 206; Leese M (2014) The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European union. *Security Dialogue* 45(5): 494–511, p. 504.

978 L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

such. The question is how to apply the idea of protected grounds to risk profiles, which are to a large extent assumptions, inferences or estimates. This problem ties into the discussion on the terms of personal characteristics, which I explain in the next section.

5.4.2.2. Personal characteristics and status[979]

Another reason why non-discrimination law is challenging to apply to profiling is the position adopted by the ECtHR on discrimination pertaining to personal characteristics or grounds of status. Originally the ECtHR viewed the word 'status' in article 14 ECHR as a feature of the non-exhaustive ground system, stating that the word 'status' is broad enough to include other grounds, such as in *Engel* where military rank was the underlying factor for differential treatment.[980] Following this formulation, each case of unequal treatment could be brought before the ECtHR regardless of the particular ground of discrimination underlying the state measure in question.[981] However, the ECtHR has also around the same time ruled differently on the meaning of 'status', for example in *Kjeldsen, Busk Madsen and Pedersen v. Denmark*, where the court stated that what truly matters is whether discriminatory treatment has as its basis or reason in a personal characteristic, i.e. "status", by which persons or groups are distinguishable from each other.[982] Following this case, the word status would have a different meaning, creating a restrictive approach by focusing on a requirement of linking a protected ground to the status of a person, rather than the flexible approach where status is just an indication of a protected ground. The problem is that the ECtHR seems to conflate and confuse different meanings of the concept of status within the context of article 14 ECHR, switching between the flexible and the restrictive approach in case

---

979 For this section, the works of O.M. Arnardóttir and L. Naudts on the relevant case law were of key importance; specific references are in the individual footnotes.

980 ECtHR, *Engel and Others v The Netherlands* 1976.

981 J. Gerards, 'The Discrimination Grounds of Article 14 of the European Convention on Human Rights' (2013) Vol. 13 *Human Rights Law Review* 99, 104-105.

982 ECtHR, *Kjeldsen, Busk Madsen and Pedersen v Denmark* Series 1976, para 56; see also Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar*. SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913; Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

law and sometimes combining some of the elements from both lines of case law.[983] This straightforward and flexible approach has been contrasted especially in case law since the early 2010s, in which the meaning of 'other status' became the focal point of the court's reasoning. For example, in *Carson*, the ECtHR stated that not every difference in treatment will amount to a violation of article 14 ECHR, rather, "only differences in treatment based on a personal characteristic (or "status") by which persons or groups of persons are distinguishable from each other are capable of amounting to discrimination within the meaning of Article 14".[984] In that case the ECtHR held that residence was such an aspect of personal status.[985] The court used the same reasoning in *Clift*, where the ECtHR ruled that article 14 ECHR does not prohibit all differences in treatment but only those differences based on an identifiable, objective or personal characteristic, or "status", by which persons or groups of persons are distinguishable from one another.[986] Ever since that case law, the approach of the ECtHR towards this has been ambiguous. Scholars such as Naudts and Arnardóttir propose that case law after 2010 also shows that the ECtHR seems to have settled on this more restrictive approach, following *Carson* and *Clift*, focusing on 'identifiable characteristics' or status, albeit sometimes leaving out the wording 'personal' characteristic.[987] For example, in *Big Brother Watch*, the applicants argued that persons outside of the UK were disproportionately likely to have their private communications intercepted compared to persons inside the UK and additional safeguards against the interception were only afforded to persons known to be in the UK, being indirectly discriminatory on grounds of nationality. The ECtHR dismissed an article 14 ECHR claim as it deemed geographic

983 For an extensive analysis of this case law, see: Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96; Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014); J. Gerards, 'The Discrimination Grounds of Article 14 of the European Convention on Human Rights' (2013) Vol. 13 *Human Rights Law Review* 99, 104-105.

984 ECtHR, *Carson and Others v. The United Kingdom* App no 42184/05, 2010, para 70.

985 ECtHR, *Carson and Others v. The United Kingdom* App no 42184/05, 2010, para 70.

986 ECtHR, *Clift v The United Kingdom* App no 7205/07, 2010, para 55.

987 L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96; OM Arnardóttir, 'Vulnerability under Article 14 of the European Convention on Human Rights' (2017) Vol. 4 *Oslo Law Review* 150; Such case law being: ECtHR, *Fabian v Hungary*, App no 78117/13, 2017; ECtHR, *Lupeni Greek Catholic Parish and Others v Romania* App no 76943/11 (Grand Chamber), 2016, para 163.

location to be the differential factor and the ECtHR does not consider it a personal characteristic, which it required for an article 14 ECHR claim.[988]

The question is what this focus on personal characteristics of protection against discrimination means for profiling. On the one hand one could argue that it is a matter of semantics. For example, Gerards proposes that it is not so strange for the ECtHR to focus on a differential treatment that is linked to personal characteristics, as the ECHR focuses on safeguarding individual rights and those are mostly impacted when the complaint sees to those traits rather than to differences based on for example geographical differences.[989] At the same time Gerards, rightly so, concedes that it is increasingly difficult to assess when a treatment pertains to a personal characteristic or not, for example when geographical differences are intrinsically linked to specific ethnic minorities.[990] I agree with that criticism. If the focus is on discrimination based solely on personal characteristics, it invites going down a slippery slope where proxies could be used to disguise the use of personal characteristics and circumvent legal protection against discrimination. It has already been shown for example in data protection that to make such distinctions, in the separation between special categories of data and other personal data, or between personal data and non-personal data, is extremely difficult.[991] Rather I propose that it could be interesting to use a broad concept of what constitutes a personal characteristic or status and include a risk profile as such. For example, Naudts proposes that while the profile can underlie differential treatment, it is unlikely that the profile itself would be considered as an inherent personal trait for those subject to the differential treatment. Naudts thus concludes that an approach where an inherent personal trait needs to be the basis for

---

988 ECtHR, *Big Brother Watch and Others v The United Kingdom* App nos. 58170/13, 62322/14 and 24960/15, 2018, para 516-518; see also Van der Sloot, B., and E. Kosta. "Big brother watch and others v UK: Lessons from the latest Strasbourg ruling on bulk surveillance." *Eur. Data Prot. L. Rev*. 5 (2019): 252; L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security.* Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

989 Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar.* SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913.

990 Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar*. SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913.

991 van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. WODC/TILT. https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y; Purtova N (2018) The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* 10(1): 40–81.

the court to condemn differential treatment is not equipped to deal with new profiling practices.[992] I fully agree with that point, given all the challenges of matching profiling with the current assessment of protected grounds as described above. There is no case law on this point yet, so it is to be seen how the CJEU or ECtHR would interpret this. Inspiration for such a reading can again be found in data protection law, where, for example, there are plenty of ongoing debates on the meaning of personal data in data protection scholarship,[993] the relation between personal data and profiles,[994] and questions are raised whether profiles constitute personal data as such.[995] The questions about the status or role of the profile as such brings me to the point of section 5.4.2.3.

5.4.2.3. Assumed characteristics and discrimination by association

Another question in applying non-discrimination law to profiling is what the status of the profile itself can be under non-discrimination law. More specifically: how does non-discrimination law treat characteristics that are assumed through profiling? I approach this challenge by looking at the notion of discrimination by association, as it is the concept that is most closely related.

Discrimination by association occurs when a person is treated worse than others based on their relation or association to a protected group. The idea is that the individual does not need to be a member of a protected group, for example a religious minority, but it is sufficient for an individual to be associated to it.[996] Looking at how this notion of discrimination is used by the ECtHR, it is defined in case law as situations where the protected ground in question relates to another person somehow connected to

---

992 L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

993 For example: Purtova, Nadezhda. "The law of everything. Broad concept of personal data and future of EU data protection law." *Law, Innovation and Technology* 10, no. 1 (2018): 40-81.

994 For example: A. Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in: *Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-46608-8_8>; A. Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection' (2016) Vol. 32 *Computer Law & Security Review* 238; Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 *Philosophy & Technology* 475.

995 For example in Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, 40, 1-13. [105486]. https://doi.org/10.1016/j.clsr.2020.105486.

996 S. Wachter, "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising," *Berkeley Technology Law Journal* 35, no. 2 (2020): 367-430.

the applicant.[997] Examples of discrimination by association are present in CJEU case law as well, for example in the *CHEZ case*, where the applicant ran a shop in an area dominantly populated by a Roma community and was disadvantaged by a measure which targets the whole community, even though she is not a part of the Roma herself. The CJEU ruled that 'discrimination on the grounds of ethnic origin', for the purpose of Council Directive 2000/43/EC of 29 June 2000 must be interpreted as being intended to apply irrespective of whether a collective measure affects persons who have a certain ethnic origin or those who, without possessing that origin, suffer, together with the former, the less favourable treatment or particular disadvantage resulting from that measure.[998] A similar ruling can be found in the *Coleman* case, where the CJEU ruled that the prohibition of direct discrimination is not limited only to people who are themselves disabled, but also includes less favourable treatment of an employee based on the disability of his child.[999] In the *Coleman* case, discrimination by association was not yet explicitly recognized by the CJEU, but it was done in the *CHEZ* case, opening the door for similar cases in the future.[1000]

To understand how the concept of discrimination by association can be applied to profiling, I use affinity profiling as a specific type of profiling to illustrate this. Affinity profiling is used for example for behavioural advertising purposes and concerns grouping people according to their assumed interests rather than solely their personal traits.[1001] In very simplistic terms, affinity profiling is about inferring someone's interests and likes and dislikes. Risk profiling is comparable to affinity profiling in the sense that it also relies on inferred characteristics or assumptions and not necessarily completely on actual personal characteristics or objective facts. To take a fictional example, from the characteristics of having family members with a criminal record for theft, living in a certain zip code, being unemployed and being part of an ethnic minority group, a risk profile would be composed that would indicate a high risk of committing a burglary for individuals who fit those criteria. The question is what the legal status is of such inferred characteristics or predications compared

997 ECtHR, *Molla Sali v. Greece* [GC], 2018; ECtHR, *Guberina v. Croatia*, 2016, para. 78; ECtHR, *Škorjanec v. Croatia*, 2017, para. 55; ECtHR, *Weller v. Hungary*, 2009, para. 37; see also European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

998 C-83/14, Judgment ECLI:EU:C:2015:480, 16/07/2015, *CHEZ Razpredelenie Bulgaria*, para 129.

999 CJEU, *Coleman v Attridge Law* (2008) C-303/06, ECLI:EU:C:2008:415, para 64.

1000 For more on these cases see: Benoît-Rohmer, Florence. "Lessons from the recent case law of the EU Court of Justice on the principle of non-discrimination." In: *The Principle of Equality in EU Law*, pp. 151-166. Springer, Cham, 2017.

1001 S. Wachter, "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising," *Berkeley Technology Law Journal* 35, no. 2 (2020): 367-430.

to personal characteristics related to protected grounds. Taking an example from behavioural advertising, one can have an affinity group "interested in Muslim culture"; would that grouping be awarded the same legal protection as grouping people under "religion"?[1002] It is a challenge for non-discrimination law how to award protection to newly invented groups, groups based on inferred characteristics, or groups for which the overarching label is not clear. In the context of affinity profiling, Wachter proposes the use of discrimination by association to close gaps in legal protection against discrimination, as the concept of discrimination by association challenges differentiating between assumed interests and personal traits.[1003] Wachter sees several advantages of applying discrimination by association to affinity profiling, for instance people do not have to 'out themselves' as being part of a protected group to receive protection, and individuals who have been discriminated against but are not actually members of a protected group -because they were for example misclassified- could also bring a claim.[1004] I propose it would be useful to apply a concept of discrimination by association to risk profiling as well. More legal protection would be offered if people can also seek protection against discrimination in assumed characteristics rather than only personal characteristics. Grouping people into a certain category based on predictions or assumptions exposes them to real life consequences, such as heightened police surveillance, and thus the courts should also assess discrimination complaints based on differential treatment or outcome *based* on such characteristics. The advantages of discrimination by association that Wachter proposes also apply to risk profiling. It would be easier for individuals to file a complaint based on an association made, rather than trying to fit their complaint within a certain protected ground, or in some cases it might not even be clear which protected ground would be at stake. Having the mere association with a certain group as a threshold would also lower the bar for individuals classified into a wrong group to seek redress for discrimination. To illustrate this, imagine an individual being profiled as being unemployed and discriminated against by the outcome of a policy on that basis, while that individual in fact is not unemployed, there would still be protection awarded against that discrimination whether the classification is correct or not. There is case law on a national level concerning this argument. For example, in the Netherlands there was a case before The Netherlands Institute for Human Rights where a man received differential negative treatment because he was thought to have certain political extremist sympathies. The Institute ruled that it did not matter whether that

1002 S. Wachter, "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising," *Berkeley Technology Law Journal* 35, no. 2 (2020): 367-430.

1003 S. Wachter, "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising," *Berkeley Technology Law Journal* 35, no. 2 (2020): 367-430.

1004 S. Wachter, "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising," *Berkeley Technology Law Journal* 35, no. 2 (2020): 367-430.

characteristic was assumed or true, he was still awarded protection on the grounds of political beliefs, because he was disadvantaged due to the assumption that he possessed that characteristic.[1005]

Thus, discrimination by association or a similar concept is very helpful for protection against discrimination in risk profiling. Nonetheless it is not without its own challenges. Individuals or groups still have to be aware of the predictions or assumptions made to be aware of possible discrimination therein and to file a complaint, which can be very challenging with complex risk profiles.

5.4.3. Types of discrimination: direct, indirect and harassment

There is a legal distinction between three different types of discriminatory treatment: direct discrimination, indirect discrimination, and harassment. Direct discrimination is defined for example in the Racial Equality Directive as: "*Direct discrimination shall be taken to occur where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin*."[1006] Looking at other EU law directives, such as the Employment Equality Directive, the Gender Goods and Services Directive and the Recast Gender Equality Directive, the definition is similar, adjusted to the scope of the directive in question.[1007] Thus direct discrimination pertains to a differential treatment based on a protected ground, such as racial origin for example. Under CoE non-discrimination law the concept has the same meaning: the ECtHR has described direct discrimination as difference in treatment of persons in analogous, or relevantly similar situations and based on an identifiable characteristic, or 'status'.[1008] Based on doctrine, direct discrimination can be explained as discrimination in the *treatment* of individuals while indirect discrimination is discrimination in the *outcome* of policy, practices, decisions and so forth.[1009] Non-discrimination aspires a form of formal equality, under which equals should be treated equally and thus direct discrimination is forbidden. Human rights bodies and courts have developed this notion further, as consistent treatment is not enough to achieve full equality, a discriminatory outcome should also be prohibited to achieve the goal of equality.[1010] That is why the notion of indirect discrimination was developed. Indirect discrimination occurs when a policy, practice, rule, or so forth, appears to be

---

1005 College voor de Rechten van de Mens, 22 July 2013, judgment 2013-94.

1006 Article 2(2)(a) of the Racial Equality Directive 2000/43/EC.

1007 The Employment Equality Directive (2000/78/EC), the Gender Goods and Services Directive (2004/113/EC) and the Recast Gender Equality Directive (2006/54/EC).

1008 ECtHR, *Biao v. Denmark* [GC], 2016, para. 89; ECtHR, *Carson and Others v. the United Kingdom* [GC], 2010, para. 61; ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007.

1009 Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234, p. 148.

1010 Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234, p. 155.

neutral but has a disproportionate impact on specific groups defined by reference to a protected ground, such as people of a specific race or a specific sexuality.[1011] With indirect discrimination there is no difference in treatment, but structural biases lead to treating unequals equally, thus leading to unequal results.[1012] A similar definition can be found in EU law, such as in the Racial Equality Directive:

> *"Indirect discrimination shall be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary."*[1013]

Thus, indirect discrimination can take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, has a particular discriminatory effect on a particular group,[1014] without requiring the *intent* to discriminate.[1015] To give an example of indirect discrimination: a rule can be applied that is neutral on the surface, such as stopping one in ten cars in a certain area between the hours of 21.00 and 0.00, but in practice mainly have a negative impact on one particular ethnic, racial or religious group compared with other groups, for instance when 60% of the population of that area driving during these hours is of Afro-Caribbean descent, while the Afro-Caribbean population of the town and the surrounding area does not exceed 30%.[1016]

According to the FRA, discrimination in profiling is usually a form of direct discrimination, such as stopping a member of an ethnic minority on suspicion of committing an offence solely or mainly because they are a member of that ethnic

---

1011 See for example: ECtHR, *Biao v. Denmark* [GC], 2016, para. 103; ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007, para. 184; Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic-decision-making/1680925d73, p. 19.

1012 Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234, p. 156.

1013 Article 2(2)(b) of the Racial Equality Directive 2000/43/EC.

1014 ECtHR, *Biao v. Denmark* [GC], 2016, para. 103; ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007, para. 184; ECtHR, *Sampanis and Others v. Greece*, 2008, para. 67.

1015 ECtHR, *Hugh Jordan v. the United Kingdom*, 2001, para. 154; ECtHR, *Hoogendijk v. the Netherlands*, 2005; ECtHR, *Biao v. Denmark* [GC], 2016, para. 103; ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007, para. 184.

1016 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 23 & 24.

minority.[1017] While this might be true for a lot of discriminatory problems with profiling, it seems a bit of an oversimplification. There will certainly also be a lot of cases where factors such as race are avoided but the profiling will in practice still impact certain racial groups more negatively than others, thus not constituting a difference in treatment but still a difference in outcome. Especially in the case of risk profiling where data and algorithms play a large role, the use of algorithms can appear to be a 'neutral' application of a rule but lead to an unjustified burden on specific groups.[1018] This is another challenge for non-discrimination law in regulating profiling: the more data is used, the more a policy can seem to be either neutral or to be justified as the least burdensome or most proportional option. The question is whether more data leads indeed to more neutral practices or simply to a façade of neutrality. On the one hand there is discrimination that is potentially exacerbated by bias in data and system design, as explained in section 5.2 of this chapter, while on the other hand data can be used as a factor to either diminish discriminatory outcomes or at least expose non-neutrality through statistics.

There is a difference between the direct and indirect discrimination from a legal point of view. For indirect discrimination, it first needs to be proven that a seemingly neutral rule, practice or decision disproportionately affects a protected group or individuals connected to a protected ground and is thereby prima facie discriminatory. For example, a suspicion of indirect discrimination can be rebutted before the ECtHR if the state can invoke an objective and reasonable justification.[1019] The same can be said for EU non-discrimination law where indirect discrimination can be objectively justified by a legitimate aim and when the means of achieving that aim are appropriate and necessary.[1020] Requiring a justification for indirect discrimination provides protection from apparently neutral provisions, criteria or practices or the use of a neutral proxy which have the 'side effect' of discriminating against one of the specific

---

1017 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 15.

1018 Lammerant, H., and P. De Hert. "Predictive profiling and its legal limits: Effectiveness gone forever." PP. 145-173 In: *van der Sloot, B., Broeders, D., & Schrijvers, E. (Eds.) (2016). Exploring the boundaries of big data*, p. 160.

1019 Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic-decision-making/1680925d73, p. 19-20; ECtHR, *Biao v. Denmark* (Grand Chamber), No. 38590/10, 24 May 2016.

1020 Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic-decision-making/1680925d73, p. 19-20; article 2(2)(b) of the Racial Equality Directive 2000/43/EC.

forbidden grounds.[1021] So indirect discrimination contains some steps to prove and can be more difficult to challenge than direct discrimination, as will be discussed in the next section.

It can be argued that with risk profiling the distinction between direct and indirect discrimination is increasingly difficult to maintain. This is because risk profiling relies heavily on the use of algorithms or machine learning. In turn, algorithms and machine learning systems work mainly with datafied proxies or variables. To give an example, an algorithm cannot operate with abstract concepts such as 'health' or 'education', instead the system requires concrete variables to process, such as different bodily measurements in the context of health, or data about grades and diplomas in the context of education.[1022] These proxies or variables can correlate with protected grounds. In machine learning systems using deep learning, a massive number of variables are mapped in relation to the target, creating an intricate and fluid relation between all the variables.[1023] It is then extremely difficult to determine which variable is a proxy for another variable, blurring the distinction between different variables and thus between different proxies for protected grounds. Scholars such as Hildebrandt, suggest that deep learning could enable developers to play around with the variables so as to obfuscate the relation to protected grounds and create an idea of accuracy and lack of bias, making the distinction between direct and indirect discrimination an illusion.[1024]

Next to direct and indirect discrimination, a third form of discrimination is harassment. The Racial Equality Directive defines harassment as occurring "*when an unwanted conduct related to racial or ethnic origin takes place with the purpose or effect of violating the dignity of a person and of creating an intimidating, hostile, degrading, humiliating or offensive environment*."[1025] Harassment and instruction to discriminate can be seen as particular manifestations of direct discrimination.[1026] For the purposes of this

---

1021 Gellert, R., K. De Vries, P. De Hert, and S. Gutwirth. "A comparative analysis of anti-discrimination and data protection legislations." In: *Discrimination and privacy in the information society*. Springer, Berlin, Heidelberg, 2013, p. 65.

1022 Hildebrandt, M. "Discrimination, Data-driven AI Systems and Practical Reason." *European Data Protection Law Review* 7 (2021): 358-366.

1023 Hildebrandt, M. "Discrimination, Data-driven AI Systems and Practical Reason." *European Data Protection Law Review* 7 (2021): 358-366.

1024 Hildebrandt, M. "Discrimination, Data-driven AI Systems and Practical Reason." *European Data Protection Law Review* 7 (2021): 358-366.

1025 Article 2(3) Racial Equality Directive 2000/43/EC.

1026 European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

research, which focuses on profiling conducted by law enforcement officials, this type of discrimination is not very relevant. Therefore, I focus on direct and indirect discrimination and assessment of justifications for those.

5.4.4. Objective justification and the margin of appreciation[1027]

A few steps need to be distinguished in the assessment of whether there is discriminatory treatment or not. There is only discrimination if there is no objective and reasonable justification, thus the weight of the determination is put on the justification.[1028] In the case law of the ECtHR the following steps can be distinguished in its assessment as to whether there is an objective and reasonable justification for differential treatment. The first question is if there has been a difference in treatment of persons in analogous or relevantly similar situations – or a failure to treat differently persons in relevantly different situations. If that is indeed the case, the second question is if such difference – or absence of difference – is objectively justified. Answering this question involves two steps. First the ECtHR assesses if there is a legitimate aim pursued and second if the means employed are reasonably proportionate to the aim pursued.[1029] This is a simplified overview of the steps, since, as discussed more extensively below, the ECtHR applies different levels of scrutiny which result in different ways this test is applied.[1030] In addition states enjoy a certain margin of appreciation in assessing whether and to what extent differences in otherwise similar situations justify a different treatment.[1031] The margin of appreciation awards either a wider or narrower margin to Member States that the ECtHR has to take into account in its assessment of justification, further complicating the test. In the following paragraphs I go through the different steps in more detail.

If an individual has the idea that they are subjected to discrimination, they will need to show that they have been treated differently from another person or group of persons placed in a relevantly similar situation, or equally to a group of persons placed in

---

1027 For this section, the works of O.M. Arnardóttir and L. Naudts on the relevant case law were of key importance; specific references are in the individual footnotes.

1028 S. Fredman, 'Emerging from the Shadows: Substantive Equality and Article 14 of the European Convention on Human Rights' (2016) Vol. 16 *Human Rights Law Review* 273, p. 278-279.

1029 See for example: European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf; C. McCrudden and S. Prechal, 'The Concepts of Equality and Non-Discrimination Inn Europe: A Practical Approach' (2009) European Network of Legal Experts in the Field of Gender Equality 21.

1030 S. Fredman, 'Emerging from the Shadows: Substantive Equality and Article 14 of the European Convention on Human Rights' (2016) Vol. 16 *Human Rights Law Review* 273, 277.

1031 See for example: J. Gerards, Pluralism, Deference and the Margin of Appreciation Doctrine, 17 *Eur. L.J.* 80, 102 (2011).

a relevantly different situation, the other group being 'the comparator'.[1032] The comparator groups do not have to be identical, but an applicant has to demonstrate that taking into account the nature of the complaint, they are in a 'relevantly similar situation' to others who were treated differently and comparability is determined in the light of the subject-matter and purpose of the measure that creates differential treatment.[1033] The FRA concludes that in practice it can be difficult for individuals to prove a case of discrimination against states, because it is necessary to rely on statistics in order to prove that a group is being treated less favorably than other groups, while in most countries this kind of data is not available and when statistics are collected they rarely include racial, ethnic or religious categories.[1034] When there is an assumption of indirect discrimination, the state can attempt to rebut this by proving that the indirectly discriminatory effect is the result of objective factors that have nothing to do with discrimination. In other words, states have to demonstrate that, supported by evidence, the practice is reasonable and rational. If that fails and the assumption of indirect discrimination holds, the state has the possibility to put forward a reasonable and objective justification for the differential treatment and the ECtHR can begin the assessment of the justification.[1035]

When differential treatment has been established, the second step is to test if there is an objective and reasonable justification for it through the proportionality test. In the first part of that test, the court establishes whether there is a legitimate aim. The ECtHR has identified numerous legitimate aims in its case law throughout the years[1036], such as: restoration of peace[1037], protection of national security[1038],

---

1032 European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf

1033 European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf; See for example: ECtHR, *Fábián v. Hungary* [GC], 2017, para. 113; ECtHR, *Clift v. the United Kingdom*, 2010, para. 66.

1034 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 24 & 25; And see: the Opinion of the European Data Protection Supervisor 2009/C 276/02; European Parliament Resolution 2010/C 16 E/08, p. 44–49; Commission Communication on the application of Directive 2000/43/EC (COM (2006) 643).

1035 Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar*. SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913.

1036 For a complete oversight see European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

1037 ECtHR, *Sejdić and Finci v. Bosnia and Herzegovina* [GC], 2009, para. 45.

1038 ECtHR, *Konstantin Markin v. Russia* [GC], 2012, para. 137.

maintenance of economic stability and restructuration of the debt in the context of a serious political, economic and social crisis[1039], facilitation of rehabilitation of juvenile delinquents[1040], or protection of women against gender-based violence, abuse and sexual harassment in the prison environment[1041]. States will not have many difficulties with establishing a legitimate aim for the profiling that causes differential treatment, for example the aim to counter the threat of terrorism is widely accepted in case law.[1042] Continuing with that example, combatting terrorism presents a very elusive target for law-enforcement actors, so that it can be argued that the only effective action for the state to take is employing broad generalizations that impose burdens on specific groups. This dilemma was illustrated in the case against the Dutch state concerning the Dutch military police, discussed in section 5.3, where ethnicity was used as a broad categorization as the alternative would be to screen a random sample of all persons passing the border.[1043] The same could be said for the prevention of crime, it is an elusive target as well. Profiling can be defended on the ground that it pursues a legitimate objective through a means as narrowly tailored as possible without forfeiting effectiveness.[1044] Law enforcement actors often argue that profiling using broad racial or ethnic categories is simply effective policing and socio-economic and demographic characteristics, such as race or ethnicity, are commonly used in policing as indicators to detect offending patterns, with certain types of crime being considered as more common among members of particular minorities.[1045] This argument can be difficult to properly assess, as it requires to determine effectiveness and requires the necessary data from law enforcement to do so.[1046] On the other hand, one can advocate that law enforcement agencies are subject to a heightened scrutiny for establishing

1039 ECtHR, *Mamatas and Others v. Greece*, 2016, para. 103.

1040 ECtHR, *Khamtokhu and Aksenchik v. Russia* [GC], 2017, para. 80.

1041 ECtHR, *Khamtokhu and Aksenchik v. Russia* [GC], 2017, para. 82.

1042 Baker & Phillipson (2011) Policing, profiling and discrimination law: US and European approaches compared, *Journal of Global Ethics*, 7:1, 105-124, DOI: 10.1080/17449626.2011.556142, p. 110.

1043 22 September 2021, District Court The Hague, ECLI:NL:RBDHA:2021:10283.

1044 Baker & Phillipson (2011) Policing, profiling and discrimination law: US and European approaches compared, *Journal of Global Ethics*, 7:1, 105-124, DOI: 10.1080/17449626.2011.556142, p. 110.

1045 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 33.

1046 European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252, p. 33.

an objective reasonable justification.[1047] For example, the Commissioner for Human Rights of the CoE put forward:

> *"Member states should apply the highest level of scrutiny when using AI systems in the context of law enforcement, especially when engaging in methods such as predictive or preventive policing. Such systems need to be independently audited prior to deployment for any discriminatory effect that could indicate de facto profiling of specific groups. If any such effects are detected, the system cannot be used."*[1048]

In that sense it should be the responsibility of the state to ensure that the profiling systems they use are not discriminatory and it is up to them to develop a system that is effective yet not discriminatory. This argument was presented in the example of the Dutch SyRI system as well, as explained in chapter 2, where the Dutch court struck down the legal basis for the fraud detection system SyRI for multiple violations of fundamental rights, which stemmed in part from it being an opaque system.[1049] The challenge, therefore, is for the state to design a system that does take into account full fundamental rights protection.

It has been proposed by some that courts tend to afford a favorable position to public bodies as it would be sufficient to indicate that a decision was (seemingly) rational,[1050] and that the margin of appreciation for states, in combination with the reasonable relationship that should exist between the measure and the aims pursued, can make

---

1047 L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security.* Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

1048 Council of Europe, Commissioner for Human Rights, 'Unboxing Artificial Intelligence: 10 steps to protect Human Rights' (May 2019) 11 <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>.

1049 District Court The Hague, 05 February 2020, ECLI:NL:RBDHA:2020:1878; Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12; Van Schendel, S. (2020). Inzet SyRI onvoldoende inzichtelijk en controleerbaar en strijdig met fundamentele rechten. *Privacy & Informatie*, 2020(2), 69-71. [66]. https://www.uitgeverijparis.nl/reader/206858/1001485529.

1050 Christopher McCrudden and Sacha Prechal, 'The Concepts of Equality and Non-Discrimination Inn Europe: A Practical Approach' (2009) European Network of Legal Experts in the Field of Gender Equality 21; see also L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security.* Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

it easy to establish rationality for differential treatment.[1051] In more data driven forms of profiling it might even become easier for states to claim objectivity and rationality. As Barocas and Selbst put forward, data mining is a form of statistics and therefore seemingly rational if used in discrimination, as the point of "data mining is to provide a rational basis upon which to distinguish between individuals and to reliably confer to the individual the qualities possess those who seem statistically".[1052] Profiling also relies heavily on statistics and aims to increase neutrality the more data that is involved. As the same statistics also play a role earlier in the assessment of discrimination, in making a claim for differential treatment by using statistics to show a less favorable treatment, data and statistics play a crucial role in non-discrimination law but at the same time also in the profiling practices itself, exacerbating the impact of data. Naudts illustrates this well:

> *"Big data analytics can be used to argue both sides of the coin: it allows to see the similarities between individuals, as well as their differences. In other words, a rational ground to either treat similar situations differently, or different situations alike, can always be found where technologies are used that have as their exact goal to look for these commonalities or dissimilarities."*[1053]

I would therefore argue that data should be used in advancing fundamental rights protection, using the inherent characteristic of risk profiling being rooted in statistics and being data driven as an advantage from a fundamental rights perspective, requiring states to be transparent about the data underlying their policies.

However, as establishing a legitimate aim for risk profiling in the law enforcement sector through either protecting national security, the security of individuals, or the prevention of crime and public disorder, will likely not be difficult, the question of the justification of differential treatment will mainly depend on the second step in the proportionality test, assessing the proportionality between the aim and the measures used. The difference in treatment has to strike a fair balance between the aim pursued

---

1051 L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security.* Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96; N. Bamforth, M. Malik and C. O'Cinneide, *Discrimination Law: Theory and Context* (Sweet & Maxwell 2008) 73.

1052 S. Barocas and A.D. Selbst, 'Big Data's Disparate Impact Essay' (2016) 104 *California Law Review* 671, p. 677.

1053 L. Naudts "Criminal Profiling and Non-Discrimination: On firm grounds for the digital era?" In: *Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, 2019; 63-96.

and respect for the rights and freedoms of the individual.[1054] In its assessment of the reasonable relationship between the means employed and the aim sought to be realized, the ECtHR leaves states a certain margin of appreciation, determined by the circumstances, the subject-matter and the background of the case.[1055] Examples where states enjoy a wider margin of appreciation are cases where public interest based on social or economic grounds is at stake, since national authorities are in principle better positioned to assess those, and the Court will generally respect the legislature's policy choice.[1056] Examples where the margin for states is narrower are cases of differential treatment based on ethnic origin, as no difference in treatment based exclusively or to a decisive extent on a person's ethnic origin is capable of being objectively justified,[1057] and differences in treatment on the basis of gender or sexual orientation can only be justified by very weighty reasons[1058].

As was already mentioned before, the ECtHR seems to apply a certain hierarchy where discrimination based on suspect grounds is scrutinized more heavily by the ECtHR and the states are awarded a narrower margin of appreciation. The suspect grounds being sex or gender[1059], race or ethnic origin[1060], religion[1061], and disability[1062]. On the other hand, there are grounds that are deemed as being on the lower end of the spectrum, such as the aforementioned grounds of property, language, marriage status, employment status, or education.[1063] The case law on article 14 ECHR with regard to the margin of appreciation in objective justifications is very complex and not completely uniform. Nonetheless, at least a distinction by the ECtHR can be derived between a narrow margin of appreciation and a strict review of the suspect discrimination

---

1054 ECtHR, *Belgian linguistic case*, 1968, para. 10

1055 ECtHR, *Molla Sali v. Greece* [GC], 2018, para. 136; ECtHR, *Stummer v. Austria* [GC], 2011, para. 88; ECtHR, *Burden v. the United Kingdom* [GC], 2008, para. 60; ECtHR, *Carson and Others v. the United Kingdom* [GC], 2010, para. 61.

1056 ECtHR, *Belli and Arquier-Martinez v. Switzerland*, 2018, para. 94; ECtHR, *Mamatas and Others v. Greece*, 2016, para. 88-89; ECtHR, *Stummer v. Austria* [GC], 2011, para. 89; ECtHR, *Andrejeva v. Latvia* [GC], 2009, para. 83; ECtHR, *Burden v. the United Kingdom* [GC], 2008, para 60; ECtHR, *Stec and Others v. the United Kingdom* [GC], 2006, para. 52; ECtHR, *Carson and Others v. the United Kingdom* [GC], 2010, para. 61.

1057 ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007, para. 176; ECtHR, *Sejdić and Finci v. Bosnia and Herzegovina* [GC], 2009, para. 43-44.

1058 ECtHR, *Abdulaziz, Cabales and Balkandali v. the United Kingdom*, 1985, para. 78; ECtHR, *Konstantin Markin v. Russia* [GC], 2012, para. 127; ECtHR, *Schalk and Kopf v. Austria*, 2010, para. 97.

1059 For example: ECtHR, *Abdulaziz, Cabales and Balkandali v United Kingdom* 1985, para. 78; ECtHR, *Konstantin Markin v Russia* 2012, para. 127.

1060 For example: ECtHR, *Cyprus v Turkey* 2001, para. 306; ECtHR, *Timishev v Russia* 2005, para. 56.

1061 For example: ECtHR, *Hoffmann v Austria* 1993, para. 36; ECtHR, *Milanovic´ v Serbia* 2010, para. 97.

1062 For example: ECtHR, *Glor v Switzerland* 2009, para. 84; ECtHR, *Kiyutin v Russia* 2011, para. 64.

1063 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 654-655.

grounds on the one hand and a wider margin and a more lenient review of non-suspect discrimination grounds.[1064] For the suspect grounds it can be concluded that they all relate to innate personal characteristics or core choices that have a significant influence on a person's identity and existence.[1065] Arnardóttir analyzed cases on the grounds on the lower end of the spectrum and found that they often lead to a ruling of no violation, except for the following circumstances: violations seem to occur in instances where the distinction is found to be clearly arbitrary, where the distinction is far from being necessary to achieve the legitimate aim intended, where the interference has particularly severe consequences for the applicant, where the social situation of the applicant is one of relative vulnerabilities, stigma plays a role, or a suspect discrimination ground is implied.[1066] The latter situation, strict scrutiny when suspect grounds are implied in lower end grounds, negates possible criticism that some grounds for differential treatment are not protected but can be used as proxies for protected grounds in differential treatment, as the ECtHR would still award only a narrow margin of appreciation for situations where the discrimination indirectly impacts suspect grounds as well.

A development that might be beneficial for protection against discrimination in law enforcement profiles, is the trend in ECtHR case law that focuses on discrimination grounds related to persistent forms of stereotyping, prejudice, and stigma, which result in social marginalization or a 'social–contextual approach' to article 14 ECHR.[1067] Under the social-contextual approach these discrimination grounds that result in social marginalization are a priori suspect as not being legitimate reasons for differentiating between people, denoting the idea that non-discrimination analysis should be conscious of how structural patterns of social disadvantage and exclusion function to keep marginalized groups in the margins.[1068] Along with the case law, in literature concerning the ECtHR, similar claims on the importance of considering

---

1064 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 655.

1065 See also: Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 655.

1066 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 656.

1067 This approach can be seen in for example: ECtHR, *Alajos Kiss v Hungary* 2010, ECtHR, *Kiyutin v Russia* 2011; ECtHR, *Konstantin Markin v Russia* 2012.

1068 Arnardóttir, OM. "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014), p. 663-664.

social marginalization have been put forward.[1069] A strict level of scrutiny for such differential treatment, with the Court paying particular attention to the broader effects of stereotyping and persistent assumptions, is important for tackling racial or ethnic profiling, or other forms of law enforcement profiling that structurally disadvantage certain societal groups. If the ECtHR continues this line of case law, it is not only beneficial for the context of specific cases but can also have a broader effect on police practices that are prone to social marginalization.

An important aspect in the assessment of the objective justification is on which party the burden of proof lies. The ECtHR uses the standard of 'proof beyond reasonable doubt' for all rights set forth by the Convention and in principle the ECtHR relies on '*affirmanti incumbit probatio*', meaning that the applicant has to prove the allegation.[1070] In its case law, the ECtHR has established that once the applicant has shown a difference in treatment, the state has to show that it was justified.[1071] This is the general rule but the circumstances of the case can shift the burden of proof slightly, for example when the events at stake are completely or for a large part within the exclusive knowledge of the authorities, the burden of proof can be on authorities to provide a satisfactory and convincing explanation.[1072] Or when it would be extremely difficult for the applicant to prove the discrimination, the ECtHR has also shifted the burden of proof in some cases.[1073] If there is a presumption of discrimination it is up to the state to disprove that, for example by proving the comparator situation does not apply, that the differential treatment is in fact not based on protected grounds but objective differences, or that the differentiation is justified.[1074] The ECtHR also emphasizes the critical role that statistics play, especially in the cases of indirect discrimination where applicants first have to create an assumption of discrimination; at the same time, it is also lenient towards individual applicants as these statistics are not always easy to come by. According to the ECtHR, when an applicant can show, based on undisputed official statistics, the existence of a prima facie indication that a rule that appeared

---

1069 See: Solanke, 'Putting Race and Gender Together: A New Approach to Intersectionality' (2009) 72 *Modern Law Review* 723; Timmer, 'Toward an Anti-Stereotyping Approach for the European Court of Human Rights' (2011) 11 *Human Rights Law Review* 707.

1070 European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

1071 ECtHR, *Timishev v. Russia*, 2005.

1072 ECtHR, *Salman v. Turkey* [GC], 2000, para. 100; ECtHR, *Anguelova v. Bulgaria*, para. 111; ECtHR, *Makuchyan and Minasyan v. Azerbaijan and Hungary*, 2020.

1073 See for example: ECtHR, *Cînța v. Romania*, 2020.

1074 ECtHR, *Khamtokhu and Aksenchik v. Russia* [GC], 2017, para. 65; ECtHR, *Chassagnou and Others v. France* [GC], 1999, para. 91-92; ECtHR, *Timishev v. Russia*, 2005, para. 57; ECtHR, *Biao v. Denmark* [GC], 2016, para. 114; ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007, para. 177.

neutral affects a clearly higher percentage of a group in comparison to another group, it is for the state to show that this is the result of objective factors unrelated to any discrimination.[1075] Following the case *D.H. and Others v. the Czech Republic*, statistics which appear on critical examination to be reliable and significant will be sufficient to constitute the prima facie evidence. Nonetheless it does not mean that indirect discrimination cannot be proved without statistical evidence, it is only that statistical evidence can help the claim of the applicant.[1076] In *Opuz v. Turkey*, there were no statistics provided to show that victims of domestic violence were predominantly women, but Amnesty International submitted that there were no reliable statistics and the ECtHR accepted the assessment of Amnesty International, a reputable international NGO, and the assessment of the United Nations Committee on the Elimination of Discrimination Against Women that violence against women was a significant problem in Turkey.[1077] Sometimes practices or beliefs of others belonging to the same protected category can constitute sufficient proof.[1078]

To conclude, the complexity in the assessment of whether there is discrimination through varying levels of scrutiny, and different models for the burden of proof, make it difficult to offer a uniform level of protection against discrimination in profiling. In their seminal work on discrimination and the gaps between the legal and technical dimension, Wachter et al. explain in detail why this complicated approach to remedy against discrimination is problematic and will be even more problematic in the future where more and more instances of discrimination are tied to data driven systems or AI.[1079] Watcher et al. conclude that there is a clear gap between statistical measures of fairness and the context-sensitive, often intuitive and ambiguous discrimination metrics and evidential requirements used by the ECtHR.[1080] Furthermore, they put forward that the admissibility and relevance of statistical tests, the make-up of disadvantaged and comparator groups, and the potential justifications for

---

1075 European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf; See for example: ECtHR, *Hoogendijk v. the Netherlands*, 2005; ECtHR, *D.H. and Others v. the Czech Republic*, 2007, para. 180; ECtHR, *Di Trizio v. Switzerland*, 2016, para. 86.

1076 ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007, para. 188.

1077 ECtHR, *Opuz v. Turkey*, application no. 33401/02, 9 June 2009.

1078 ECtHR, *Oršuš and Others v. Croatia* [GC], 2010.

1079 Wachter, S., B. Mittelstadt, and C. Russell. "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI." *Computer Law & Security Review* 41 (2021): 105567.

1080 Wachter, S., B. Mittelstadt, and C. Russell. "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI." *Computer Law & Security Review* 41 (2021): 105567.

discrimination are traditionally decided on a case-by-case basis.[1081] This heterogeneity in the interpretation and application of EU non-discrimination law poses a problem for building considerations of fairness and discrimination into automated systems.[1082] Thus Wachter et al. present the argument that it is not easy to design profiling systems adhering to ECtHR standards of non-discrimination.

I would argue that at the same time, together with the criticism on the role of data or statistics, this raises the question whether the ECtHR system for protection against discrimination is up to the challenge of a data driven reality. The question is not so much how to design systems that meet all the legal requirements, but rather how to apply the legal framework in such a way that it can be operated in a data-driven world with practices such as risk profiling.

5.5 Conclusions

Risk profiling creates dangers and challenges of discrimination, not just due to the inherent nature of profiling focusing on groups and generalizations, but specifically creating issues correlated to the predictive elements focusing evermore on statistics and large-scale data. Bias pertaining to group characteristics can be ingrained in system design and in data itself, which can have negative effects when it comes to the fore in differential treatment. Discrimination, such as excluding or over-targeting people based on risk profiles, is particularly serious in risk profiling conducted by law enforcement actors because of the potentially far reaching consequences in coercive and privacy infringing measures. Due to these reasons, the protection offered to individuals and groups through the principle of non-discrimination is of paramount importance. The system of non-discrimination law is situated to mitigate or address issues of discrimination in risk profiling in some ways but less in others. On the one hand, non-discrimination law has developed a lot over time including protection for so many characteristics that differential treatment can be based on. At the same time the complexity of risk profiling is that it is extremely difficult to pinpoint or substantiate which factors feed into differential treatment and how those factors rank.[1083] Combined

---

1081 Wachter, S., B. Mittelstadt, and C. Russell. "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI." *Computer Law & Security Review* 41 (2021): 105567; Wachter et al. refer to this approach as 'contextual equality'.

1082 Wachter, S., B. Mittelstadt, and C. Russell. "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI." *Computer Law & Security Review* 41 (2021): 105567.

1083 See also: Kamiran, F., & Žliobaitė, I. (2013). Explainable and non-explainable discrimination in classification. In: *Discrimination and Privacy in the Information Society* (pp. 155-170). Springer, Berlin, Heidelberg.

with the creation of new unforeseen groupings, this blurring of known categories of identifying factors and opacity of the process make it almost impossible to exercise a right of non-discrimination. For individuals to get more insight into risk profiling processes I would argue that it is crucial to see the connections with other fundamental rights, such as the right to data protection and due process rights and obligations under criminal procedural law, which can create information obligations. A second way in which the principle of non-discrimination is not ideally situated to address discrimination in law enforcement risk profiling, is in the complexities with the objective justification. There is a big role to play for data in creating legitimacy for practices and policies. Since risk profiling is still relatively new and there is not yet much case law from the ECtHR -there is some on the national level as described in the Dutch examples-, it needs to be seen how this role for data will play out: either data can be used in favor of fundamental rights protection by exposing bias and discrimination, or data could be used to grant objectivity to policies and practices and used for discrimination in unforeseen ways.

In the next chapter I will discuss a different regulatory framework, namely that of criminal procedural legislation. In the concluding chapter to this dissertation I delve further into what the regulation of risk profiling from a point of view of non-discrimination law means, as in to what extent there are unresolved issues in the law and what recommendations are on how to regulate risk profiling more adequately from a point of view of fundamental rights protection.

Chapter 6

The regulation of risk profiling used by national law enforcement actors under Dutch criminal procedural law

6.1 Introduction

After having explored the data protection and non-discrimination regulatory frameworks for risk profiling used by national law enforcement actors in chapters 4 and 5, the final regulatory framework to discuss is that of criminal procedural law. As set out in the introduction of this dissertation, criminal procedural legislation is drafted on the national level rather than the EU level, making it necessary to choose a national jurisdiction to analyze the legislation.[1084]

Criminal procedural law regulates, in more or less detail, multiple aspects of the risk profiling process: it determines which powers national law enforcement actors have to gather data for risk profiling; under which conditions they can conduct the analysis of the data; how risk profiles can be used; and which safeguards guide the process and under which oversight risk profiling by law enforcement actors takes place. The conditions and safeguards of criminal procedural law that create boundaries for the law enforcement actors to gather data or deploy the use of profiles stem from several fundamental rights that criminal procedural law builds on, such as the right to respect for private and family life (article 8 ECHR) as well as the freedom of expression (article 10 ECHR), and the right to liberty and security (article 5 ECHR) as well as the right to a fair trial (article 6 ECHR). The CCP[1085] is the main body of criminal procedural law in the Netherlands and thus the focus of this chapter. In addition to the CCP, the Police Act[1086] can play a role as well in the regulation of investigatory police powers, which can sometimes also include parts of the risk profiling process. This chapter will explain the scope of both these instruments when it comes to regulating powers for risk profiling. In addition, the chapter includes a discussion on the Dutch Police Data Act[1087] and the Dutch Judicial Data and Criminal Records Act[1088], as these acts play a role in regulating safeguards in collecting and analyzing data and implement specific requirements from the EU LED.

In contrast to data protection legislation, and similar to non-discrimination law, criminal procedural law does not regulate profiling as a practice as such. However,

---

1084 This chapter is dedicated to Dutch criminal procedural law for three reasons, as explained in chapter 1 in section 1.4.

1085 In Dutch: Wetboek van Strafvordering, legislation no. BWBR0001903, available at: https://wetten.overheid.nl/BWBR0001903/2023-01-01.

1086 In Dutch: Politiewet 2012, legislation no. BWBR0031788, available at: https://wetten.overheid.nl/BWBR0031788/2023-01-01.

1087 In Dutch: Wet politiegegevens, legislation no. BWBR0022463, available at: https://wetten.overheid.nl/BWBR0022463/2022-10-01.

1088 In Dutch: Wet justitiële en strafvorderlijke gegevens, legislation no. BWBR0014194, available at: https://wetten.overheid.nl/BWBR0014194/2022-07-01.

the CCP regulates investigatory powers, such as pertaining to data collection and sometimes data analysis, which can be relevant in the context of the risk profiling process, as well as provisions on checks and balances in executing those powers.

The doctrinal research in this chapter features mostly literature from Dutch criminal law scholars, and focuses on Dutch handbooks, journals and case law, due to the focus on national law. As the CCP contains an extensive catalogue of relevant investigatory powers that can be deployed for data collection, the exploration in this chapter is potentially quite broad in scope. In addition, as discussed in chapter 2, risk profiling is used in multiple phases of the criminal justice chain: in detection of crimes or finding suspects (early investigation stage), in prosecution (late investigation stage), and in trial decisions. To scope the focus of this chapter and to illustrate the sometimes-abstract discussion, I make use of examples from practice. The EncroChat court cases[1089] are used as examples to illustrate the large-scale data collection in the early investigation phase; the OxRec tool[1090] is used to illustrate the use of risk assessment in trial decisions.

Just as many other legal instruments pertaining to data, the CCP and its later amendments stem from a time when there were fewer possibilities to gather and analyze data. With the use of risk profiling tools, such as to identify suspects, gather evidence, forecast crime, or conduct a risk assessment for sentencing, tensions can arise with the fundamental rights protection awarded to those subjected to risk profiling, exactly because the legal framework is not drafted with such technological capabilities in mind. Therefore, it is important to explore to which extent the CCP and Police Act are fit to address the challenges of risk profiling as discussed in chapter 3 of this dissertation. An interesting development in this context is the trajectory to amend and modernize the CCP, which has been in the making since 2014 and culminated in a draft bill in July 2020. This draft bill on 'modernizing the Code of Criminal Procedure'[1091] (hereafter: Modernization Bill) was introduced because of numerous reasons. The most relevant reason for the purposes of this chapter was the change in technologies over the years, which led to the piecemeal and therefore fragmented introduction of

---

1089 For example: District Court Rotterdam, 25 June 2021, ECLI:NL:RBROT:2021:6113; District Court Rotterdam, 24 June 2021, ECLI:NL:RBROT:2021:6050; District Court Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1273; District Court Midden-Nederland, 12 April 2022, ECLI:NL:RBMNE:2022:1389, District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584; District Court Rotterdam, 11 April 2022, ECLI:NL:RBROT:2022:2809.

1090 For information on OxRec, see the official website: https://oxrisk.com.

1091 Tweede Kamer, 2020-2021, 35869, no. 2, 'Wijziging van het Wetboek van Strafvordering ter bevordering van innovatie van verschillende onderwerpen in het kader van de modernisering van het Wetboek van Strafvordering (Innovatiewet Strafvordering)'.

many new powers to gather and use digital data. With the Modernization Bill, the legislator hopes to introduce a more systematic approach to regulating investigation powers in the era of digital data.[1092] The Modernization bill includes several important changes for data gathering, analysis and oversight that are relevant for the topic of risk profiling and thus will be referred to in this chapter where relevant.

The research question that this chapter answers is as follows: *how do Dutch criminal procedural law, and accompanying data protection law related to criminal matters, currently regulate risk profiling by national law enforcement actors and to what extent does this legal framework address challenges caused by the use of risk profiling by these actors?*

In order to answer that question, section 6.2. first explains what criminal investigation entails under the CCP and how this relates to the Police Act as a potential basis for police powers. The scope for the legal basis is important to understand as a basis in order to explore different investigatory powers. In addition, it is not a given that all risk profiling activities fall within the scope of the criminal investigation; therefore, the scope of the criminal investigation phase must also be discussed in the context of risk profiling.

Section 6.3 discusses investigatory powers used for large-scale or bulk-data collection and analysis, to place these powers in the context of risk profiling. Section 6.3 discusses the collection and analysis of data originating from large scale police hacks and the use of software to perform automated search and data comparisons. To give examples of the various provisions for large scale data collection, the EncroChat cases are used as an example to illustrate how these powers can be used in practice. There are no publicly available case studies of the use of risk profiles in the investigation phase due to the covert nature of police investigations; nonetheless the large-scale data-driven investigations in in EncroChat can sometimes lead to the creation of risk profiles and can be used as an analogy in general. The goal of 6.3 is to describe and explain the regulatory framework; an assessment of this framework in its adequacy for regulating risk profiling will be conducted in 6.6.

Section 6.4 discusses the regulation of use of risk profiling in later phases of the criminal justice chain, namely in decision-making on parole and sentencing. To illustrate the use of risk profiling in those later phases, the example of OxRec is used. The legal basis and safeguards for such risk profiling stem not only from the CCP but also, indirectly, from the right to a fair trial.

[1092] Tweede Kamer, 2020-2021, 35869, no. 3, explanatory memorandum.

Section 6.5 analyses the legislation on processing data in the criminal justice chain: the Police Data Act and the Judicial Data and Criminal Records Act, with section 6.5.1. acting as a short introduction to the legal landscape and outlining the scope of the different instruments. Where chapter 4 discussed EU data protection law in this regard, namely the LED, section 6.5.2 discusses the national implementation of the LED, using the Police Data Act and the Judicial Data and Criminal Records Act to illustrate on a more detailed level which safeguards are derived from the profiling and automated decision-making provision and other relevant provisions, as well as where Dutch law deviates from EU law.

Lastly, section 6.6 continues on the building blocks of sections 6.3 through 6.5, in which the regulatory framework was explored, to discuss to what extent the current criminal procedural law regulates risk profiling, and where there are possible points of improvement. Section 6.6 also builds on chapter 3 of this dissertation, which identified the challenges of risk profiling, as these challenges inform what the legal framework is meant to address. Section 6.6 splits the analysis of the Dutch criminal procedural framework in addressing the challenges of risk profiling into three parts. Section 6.6.1. bundles the challenges created by the shift from reactive policing to preemptive and predictive policing; section 6.6.2. discusses the interplay of, and gaps between, the different provisions of the CCP and Police Data Act; and section 6.6.3. discusses the challenges related to the right to fair trial.

Finally, section 6.7 concludes the chapter by summarizing the main points and answering the overall question of the chapter.

6.2. The CCP & Police Act 2012 providing a legal basis for risk profiling

6.2.1 The concept of criminal investigation and risk profiling

When assessing how the use of risk profiling in criminal investigations is regulated it is necessary to first determine what the scope of the criminal investigation is. The main instrument for regulating investigatory police powers in the Netherlands is the CCP. Article 132a CCP contains the definition of criminal investigation: it is the investigation in relation to criminal offences, under the authority of the public prosecutor[1093], with the purpose of taking criminal justice decisions. Within this definition we can distinguish two types of criminal investigation: on the one hand what is dubbed as 'traditional criminal investigation' and on the other hand 'special

[1093] In Dutch: Officier van Justitie (OvJ)

criminal investigation'.[1094] In previous versions of the criminal investigation concept both were mentioned explicitly in the legal definition.[1095] However, a more general formulation for the criminal investigation was chosen in the current version of the CCP, because this opens the possibility to include various types of new forms of criminal investigation in the future.[1096] For special investigatory powers, the CCP distinguishes between criminal investigations into regular crimes, criminal investigations into organized crime, and criminal investigations into terrorist crimes. Thus, article 132a CCP is quite broad in scope.[1097] The scope of the criminal investigation is ultimately determined by the authority (under the authority of the Public Prosecutor) and the aim (to take criminal justice decisions).[1098]

In the criminal procedure we can distinguish between the phases of investigation, prosecution, and trial. In the traditional investigation, the investigation usually starts when there is a reasonable suspicion that a crime has been committed.[1099] This point can coincide with having a suspect, but this is not necessary, as in many cases there is not immediately a suspect. Article 132a CCP marks the start of the investigation phase. As the investigation phase is the first phase of criminal procedure, it is also the start of the safeguards from the CCP being applicable. For example, article 1 CCP contains the principle of legality for criminal procedural law, which entails that criminal procedure has to take place on a legal basis within the bounds stipulated by the law. The protection of fundamental rights within the criminal investigation can most strongly be seen through article 359a CCP. Article 359a CCP regulates the powers of the trial judge to assess violations of the law and of procedures by the police and prosecution during the pre-trial investigation. The criminal investigation of article 132a CCP also marks the start of the protection of article 359a CCP, meaning that from

---

1094 Van der Meij, Commentaar op artikel 132a Sv, Opsporingsonderzoek (T&C Strafvordering) (online), comment no. 2a.

1095 With the amendment of the CCP through an act for special investigatory powers the investigation concept was laid down in article 132a CCP and because of the introduction of these special investigatory powers it was desired back then to mention both types of powers explicitly. See: Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Tweede Kamer 1996-1997, 25403, no. 3, p. 4-9.

1096 Van der Meij, Commentaar op artikel 132a Sv, Opsporingsonderzoek (T&C Strafvordering) (online), comment no. 2b.

1097 See for example: Supreme Court, 4 March 2014, ECLI:NL:HR:2014:477.

1098 Van der Meij, Commentaar op artikel 132a Sv, Opsporingsonderzoek (T&C Strafvordering) (online), comment no. 4.

1099 Groenhuijsen, M. S., & Knigge, G. (Eds.) (2001). Het vooronderzoek in strafzaken. Tweede interimrapport onderzoeksproject Strafvordering 2001. Gouda Quint.

the moment the criminal investigation starts, violations of rights of suspects can have consequences in the criminal trial.[1100]

Over the years, police activities have aimed at earlier interventions. Nowadays, interventions can start even before there is a reasonable suspicion, prior to a possible criminal investigation.[1101] The criminal investigation itself can also start earlier in the case of investigations into organized crime or terrorist crimes. Where previously investigation was aimed at detecting committed crimes, organized crime requires a more proactive type of investigation not only aimed at gathering evidence and reconstructing committed crimes but also arresting members of organized crime for preparation of crimes.[1102] For terrorist crimes, prevention is the main goal, allowing for even earlier interventions where for some powers 'indications' that a terrorist crime might be committed are sufficient.[1103] Earlier interventions and 'indications' – a lower threshold than reasonable suspicion to use investigatory powers – have blurred the starting point of the criminal investigation to some extent.

While the starting point of the criminal investigation is relevant for the use of investigatory powers, that is not to say the police cannot perform preventative activities outside the context of a criminal investigation. The police also have a general policing task to maintain public order,[1104] and thus many activities of preventing crime can fall within that task. When it comes to risk profiling it is important to distinguish which activities fall within that general policing task and which activities can be seen as part of criminal investigation.

Intelligence-led policing or data-driven decisions where to send police patrols can be seen as an example of risk-based policing that is not a criminal investigation practice. Intelligence-led policing is used inter alia to get an insight into security and safety issues in society, the causes, trends, possible perpetrator profiles and intervention possibilities.[1105] Data are the driving force behind intelligence-led policing and allow for

---

1100 Groenhuijsen, M. S., & Knigge, G. (Eds.) (2001). Het vooronderzoek in strafzaken. Tweede interimrapport onderzoeksproject Strafvordering 2001. Gouda Quint.

1101 B.J. Koops, Criminal investigation and privacy in Dutch law, TILT Law & Technology Working Paper Series, version 1.0, September 2016, available at http://ssrn.com/abstract=2837483.

1102 Groenhuijsen, M. S., & Knigge, G. (Eds.) (2001). Het vooronderzoek in strafzaken. Tweede interimrapport onderzoeksproject Strafvordering 2001. Gouda Quint.

1103 See for example article 126zd CCP.

1104 See article 3 Police Act.

1105 For more on intelligence-led policing see: De Hert, P; Huisman, W; Vis, W. Intelligence led policing ontleed, *Tijdschrift voor Criminologie*; The Hague Vol. 48, Iss. 4, (Dec 2005): 5; L.T. ten Brink, Waakzaam tussen wijk en wereld: Nationaal Intelligence Model Sturen op en met informatie, available at: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/69628.pdf.

risk assessments in terms of broader developments. One example of risk assessment that is used to determine police deployment and is not part of criminal investigations is the use of the CAS to determine when and where to send police patrols.[1106] For example, police patrols can be sent to areas in Amsterdam that are classified as high risk for burglaries in the evening. This does not concern criminal justice decisions, but the generalized police task of maintaining public order. More broadly speaking, creating risk profiles as such (to be able to identify criminals as proactively as possible) is not necessarily part of any criminal investigation; more often than not it will fall under the more general policing task.[1107]

Nevertheless, risk profiling can also be used in criminal investigations. As section 2.5.2 of chapter 2 of this dissertation explained, one way in which risk profiles are used is in the early stages of criminal investigation. The question is to what extent these types of practices are included within the scope of the criminal investigation of article 132a CCP. This question is important as the safeguards from the CCP apply when there is a criminal investigation and at the same time investigatory powers are granted to the police at that point. We have risk profiles used for predictive identification to assess the likelihood of individuals or groups being perpetrators of crime, for example to identify suspects of fraud or drug trafficking. In this situation it can be difficult to determine whether the use of risk profiles falls within the scope of the criminal investigation. It can be that there is no indication yet that a crime has been or is being committed; whether taking criminal justice decisions can be the aim in such situations will depend on how much starting information there is available: it might not be enough concrete information yet to take such decisions and thus start an investigation. It is also possible to assess the risk that crimes will be committed, thus more in terms of predicting future crimes. For example, when there is a risk assessment of individuals likely to become perpetrators of domestic violence, is the mere placement of individuals on a high-risk list, even though no crime has been committed yet, already part of a criminal investigation? Some scholars argue that predictive identification can fall within the scope of criminal investigation, as this identification is used to select individuals against whom there is a reasonable suspicion, which will lead to investigative measures, such as their arrest.[1108]

The question is whether the current scope of the criminal investigation is also the most preferable one, from a point of view of protecting fundamental rights of those

---

[1106] See section 2.5.2.1.

[1107] Schermer, B.W., 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017, p. 208-209.

[1108] Das, A., & Schuilenburg, M. (2018). Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht. *Strafblad*, 2018(4), 19-26.

subjected to risk profiling. The more broadly the concept of criminal investigation is interpreted, the broader the scope of the fundamental rights protective function. Thus, if forms of preventive policing fall within the scope of article 132a CCP, individuals who are impacted by such police powers could gain protection from the CCP if they are in the end prosecuted or on trial.[1109] That is why it is appealing to see how practices such as risk profiling can fall within the concept of criminal investigation. Nonetheless, I would propose that there are also strong objections to a too broad interpretation of which activities can fall under the concept of the criminal investigation, as the concept of criminal investigation has not only a protective function but also a legitimizing function.

I would argue that the more broadly article 132a CCP is interpreted, the more preventive powers will also be legitimized to be used. For the prevention of terrorist attacks separate powers have been introduced in the CCP, as for crimes of that nature a specialized framework authorizing preventive powers is necessary. However, if forms of predictive policing outside of the context of prevention of terrorism are considered to be part of the criminal investigation, this creates a sliding scale under which police powers can increasingly encroach upon the right to privacy. The use of the criminal law system is an ultimum remedium, meaning that the use of the criminal law system has to be necessary for the situation and that there are strict boundaries to what force or measures can be used, while fundamental rights have to be respected.[1110] Hirsch Ballin has conducted important research into forms of preemptive policing and what this means for the concept of criminal investigation. Hirsch Ballin concluded that nowadays the criminal investigation concept does not solely mean the detection of crimes committed and punishment for those, but also includes the task to contribute to enhancing safety, investigating threats, and preventing threats from being realized. This preventative function is also bound by the ultimum remedium criterion.[1111] From the perspective of the ultimum remedium nature of criminal law, early interventions should be reserved for very serious crimes. The CCP follows this line of reasoning, as early interventions are aimed at either prevention of terrorism or organized crime, both forms of crime posing serious threats to the right to life of others. Thus, it is

1109 See for example Stevens, L., Hirsch Ballin, M., Galic, M., Buisman, S., Groothoff, B., Hamelzky, Y., & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2021(4), 234-245.

1110 Hirsch Ballin, M. F. H. (2012). Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States. T.M.C. Asser Press / Springer.

1111 Hirsch Ballin, M. F. H. (2012). Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States. T.M.C. Asser Press / Springer.

important to maintain this criterion and not envision preventative risk profiling for less serious crimes.

With the Modernization Bill, the Dutch legislator has the opportunity to revise the definition of the concept of criminal investigation used in the CCP, in order to align it better with the current reality of a more proactive investigation system, or to at least offer further guidance on when the criminal investigation starts. Nonetheless, the legislator has so far chosen to leave the definition from article 132a CCP unchanged in the Modernized CCP. The explanatory memorandum to the Modernization Bill outlines that the determination whether there is a criminal investigation is still dependent on the aim of the investigation (to take criminal justice decisions), rather than requiring a reasonable suspicion that a crime has been committed as a boundary marker, so as not to exclude investigations when there is no suspicion yet.[1112] At the same time, the explanatory memorandum mentions policing activities that fall within the scope of criminal investigation, such as stopping of ongoing crimes, investigating known repeat offenders, or trying to detect crimes that may have been committed.[1113] There is no mention of crime prevention or predictive policing in connection to the criminal investigation concept in the explanatory memorandum. However, there is a brief mention not necessarily of prevention of crime or predictive policing, but of a practice that can be part of risk profiling: searching for crimes that could have possibly been committed, with the aim of taking criminal justice decisions when indeed such a crime is discovered; this is also within the ambit of the criminal investigation. It is clarified that if an investigation commences but, in the end, does not result in a suspicion and it is decided not to pursue further investigation, this is also a criminal justice decision, and can thus also fall within the scope of criminal investigation. Thus, if a risk profile is for example used to investigate whether a crime has been committed but in the end no crime is discovered, this can also be criminal investigation.[1114]

6.2.2. The exploratory investigation

Another phase in the criminal prosecution that is important to introduce here is the exploratory investigation, regulated in article 126gg CCP. The exploratory investigation allows the public prosecutor to order an investigation which prepares for an actual criminal investigation into parts of society in which organized crime is suspected to

---

[1112] Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, July 2020, pp. 46-47.

[1113] Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, July 2020, pp. 46-47.

[1114] Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, July 2020, pp. 46-47.

play a role.[1115] This scope includes situations where the circumstances suggest that within collections of people, crimes serious enough for which pre-trial detention is possible, are being planned or committed that seriously breach the rule of law.[1116] Because of the exploratory nature of the powers, they are not coercive powers vis–à-vis individuals but rather competencies that allow the casting of a wider net, such as gathering personal data from open sources or collecting bulk data from third parties. These data can be analyzed and can lead to a reasonable suspicion and the starting of a criminal investigation. This type of data collection could be used to draft group risk profiles for example. The exploratory investigation is interesting in the context of risk profiling, as it introduces some powers for large-scale data collection. The exploratory investigation is not a part of criminal investigation, as the exploratory investigation does not have as its aim to take criminal justice decisions; rather the exploratory investigation is used to prepare conducting criminal investigations in concrete cases.[1117] However, it should be noted that in the explanatory memorandum of the Modernization Bill, the exploratory investigation is no longer described as having the aim to prepare criminal investigations for concrete cases. One of the reasons for this is that the exploratory investigation does not necessarily have to lead to a criminal investigation: at any time it can be decided to not further investigate or take any further criminal justice decisions. In addition, the legislator found this terminology of the exploratory investigation preceding the criminal investigation as means of preparation to be confusing. Criminal investigation can according to the legislator also take place when there is no concrete crime detected yet, so in a sense the criminal investigation itself can sometimes also be somewhat preparatory in nature.[1118] The goal of the exploratory investigation in the Modernized CCP is described as verifying or falsifying indications that could ultimately lead to a concrete suspicion.[1119]

6.2.3. The regulation of police powers

Another important provision to understand the system of regulating criminal investigation powers is article 141 CCP, in combination with article 142 CCP. These articles together determine which actors are charged with the detection of criminal

---

1115 Kamerstukken II 1996/97, 25 403, no. 3, p. 125; B.J. Koops, Criminal investigation and privacy in Dutch law, TILT Law & Technology Working Paper Series, version 1.0, September 2016, available at http://ssrn.com/abstract=2837483.

1116 B.J. Koops, Criminal investigation and privacy in Dutch law, TILT Law & Technology Working Paper Series, version 1.0, September 2016, available at http://ssrn.com/abstract=2837483.

1117 Van der Meij, Commentaar op artikel 132a Sv, Opsporingsonderzoek (T&C Strafvordering) (online); Kamerstukken II 2004/05, 30164, no. 3, p. 17.

1118 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie July 2020, pp. 46-47.

1119 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie July 2020, p. 531.

offences, such as public prosecutors and police officers. In charging those actors with that role, articles 141 and 142 CCP also convey a general task to detect criminal offences.[1120] For that task, the actors of the criminal investigation can use the investigation powers laid down in the CCP.[1121] The use of investigatory powers contained within the CCP is legitimized by specific provisions which provide a foreseeable legal basis. However, it is also possible for police officers to gather information outside of those powers: article 3 of the Police Act in combination with article 141 and 142 CCP is used as a legal basis to deploy investigation activities that do not require a separate legal basis.[1122] Article 3 of the Police Act lays down the task of the Dutch police as executing its task under the dependency of the competent authority and in accordance with the applicable legal rules, to ensure the effective maintenance of the rule of law and to provide assistance to those who need it.

The use of police powers based on article 3 of the Police Act is referred to as involving (at most) 'light infringements' of fundamental rights.[1123] The Dutch Supreme Court has developed standard jurisprudence on the system. Light infringements by police officers allow them to conduct investigations that are not foreseen in the CCP but constitute (at most) a relatively light infringement of the fundamental rights of citizens and do not pose a high risk to the integrity and controllability of the investigation.[1124] If an investigative act is expected to create more than a light infringement to a fundamental right, or contains a high risk for the integrity and controllability of the investigation, a specific legal basis is required. If a specific legal basis does not exist for that power in question in that situation, the investigative action cannot be used. Thus, in assessing investigatory powers, sometimes specific legal bases from the CCP are used and other times the use of police powers relies on the 'light infringements' regime of article 3 of the Police Act.

The use of article 3 of the Police Act is relevant for risk profiling, as some data collection powers, but especially data analysis powers, do not always have a specific legal basis (yet), requiring the police to consider if and to what extent using such methods infringe fundamental rights, such as the right to privacy, and whether such methods

---

1120 Groenhuijsen, M. S., & Knigge, G. (Eds.) (2001). Het vooronderzoek in strafzaken. Tweede interimrapport onderzoeksproject Strafvordering 2001. Gouda Quint.

1121 Groenhuijsen, M. S., & Knigge, G. (Eds.) (2001). Het vooronderzoek in strafzaken. Tweede interimrapport onderzoeksproject Strafvordering 2001. Gouda Quint.

1122 Borgers, M. J. (2015). De normering van 'lichte' opsporingshandelingen. *Delikt en Delinkwent*, 2015(15), 143-155.

1123 Borgers, M. J. (2015). De normering van 'lichte' opsporingshandelingen. *Delikt en Delinkwent*, 2015(15), 143-155.

1124 Borgers, M. J. (2015). De normering van 'lichte' opsporingshandelingen. *Delikt en Delinkwent*, 2015(15), 143-155; For example, Supreme Court, 1 July 2014, ECLI:NL:HR:2014:1562.

can be used under article 3 of the Police Act or not. The Modernization Bill does not alter this system for light infringements fundamentally. There will be a new specific legal basis for these types of light infringements, but in terms of rules the situation remains roughly the same. This new article 2.1.3.1 states: "Investigating officers, in the performance of their duties, are authorised to carry out investigative acts in accordance with the applicable rules of law".[1125]

The new legal basis will entail that investigative officers are authorized for the execution of their tasks to perform investigative acts in accordance with the applicable legal rules. However, 'legal rules' also include rules as set by the courts in case law, so the standards developed in the article 3 Police Act case law continue to apply.[1126]

In the Modernized version of the CCP, this type of assessment of possible privacy infringements plays a role throughout the regulation of some investigative powers in the criminal investigation that focus on data. The regulation of those powers will revolve around the criterion of 'systematicness' of the powers, which originates from case law from the Dutch Supreme Court (inter alia on smartphone searches) and the advice from the committee in charge of providing recommendations for revising the framework for digital investigative powers.[1127] The criterion of systematicness uses a scale of three steps to determine what level of authorization is required before a police power can be used. The authorization is connected to an estimation of the possible privacy infringement of the use of the police power in question: the larger the possible privacy infringement -minor, substantial or profound- of a police power, the higher the level of authority involved. An investigative officer can independently perform investigations on data, as long as the expected infringement of the personal life of the suspect is minor. When the infringement is major instead of minor because it has a systematic nature, an order from the public prosecutor is required. When the infringement is profound, an order from the investigative judge is required.[1128]

Thus, for certain types of data-related investigations, a specific legal basis is required when there is more than a minor infringement to an individual's privacy. To assess whether there is such a scenario of a more than minor infringement is dependent on whether there is a more or less complete image obtained of certain aspects of someone's

1125 Translation by the author.

1126 M. J. Borgers, 'Het gemoderniseerde Wetboek van Strafvordering: beginselen en uitgangspunten', *RM Themis* 2017-6, no. 6.

1127 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, July 2020, p. 32.

1128 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, July 2020, p. 32.

private life. The assessment of whether there is a minor infringement or a more than minor infringement is made before a power is used; the primary question is whether it is reasonably foreseeable in advance that the use of a power is systematic in nature, systematic thus referring in this context to the image of someone's personal life that will be obtained. What the foreseeable infringement is, is assessed based on the planned actions for gathering and processing data and all other relevant circumstances, including the information concerning the suspect that is already known.[1129] If the infringement is more than minor, the criterion refers to the systematic nature and the investigative officer cannot perform the activity independently. To determine whether there is a profound infringement, and thus whether the investigative judge has to be involved, depends on the same factors as discussed above and is referred to as invasive systematicness.[1130]

The system of the 'light infringements' regime, in combination with the introduction of the 'systematic' criterion, implies that for risk profiling, when police want to gather or analyze data in a way that is not specifically regulated (yet), it will depend on the expected privacy infringement whether an order from the public prosecutor or investigative judge is required as well. To what extent this system is an adequate way to regulate risk profiling is examined in section 6.6.

6.3. Investigative powers for bulk-data collection and analysis

To illustrate how risk profiling can play a role in criminal investigations and how this is regulated by Dutch criminal procedure law, I will discuss an important type of investigations that has been used extensively in recent years, namely the access to bulk data in servers of crypto phones. One major example of this type of investigation was the EncroChat investigation, which will be used here as an illustrative case in point.

6.3.1. EncroChat data collection[1131]

EncroChat was a company that provided cryptophones, which contain their EncroChat application in combination with a subscription to use the EncroChat services that could be used for encrypted chats, phone calls within the application, and making notes. The user of the phone could only use the software provided by EncroChat; it

1129 Koops Committee, Regulering van opsporingsbevoegdheden in een digitale omgeving (Commissie modernisering opsporingsonderzoek in het digitale tijdperk), June 2018, p. 37-38.

1130 Koops Committee, Regulering van opsporingsbevoegdheden in een digitale omgeving (Commissie modernisering opsporingsonderzoek in het digitale tijdperk), June 2018, p. 37-38.

1131 This section is based on the description of facts from District Court Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1273, para. 3.2.

was not possible to install other applications on it. However, the EncroChat phones had several interesting options, such as a 'panic wipe' in which all the data from the phone can be completely erased by the user, and a burn-time after which messages would expire and be deleted. Because of these options, and because these types of phones had been found in the possession of individuals involved in serious crimes, police forces in several countries were under the impression that the EncroChat phones were almost exclusively used by individuals involved in (organized) crime. There was therefore a reasonable suspicion that the company of EncroChat and related persons were committing money laundering and participating in a criminal organization and users of EncroChat were also complicit in crimes. However, the phones were difficult to decrypt and search.

To make use of a more coordinated approach to target EncroChat, a joint investigation team (JIT) was founded, including inter alia the Dutch and French police. This JIT made the decision to hack the EncroChat server based in France to perform an update and install a hack tool on all EncroChat phones worldwide, securing all the data saved on the phones (such as usernames, passwords, chats, location data, etc.) and gathering live data from all the phones for the duration of two months. All the data were shared by the French police with the other members of the joint investigation team, including the Dutch police, through a safe remote connection. The EncroChat data concerned either the server itself or the EncroChat phones that communicated via the server (server data and phone data) and included three types of data: meta data from the server (such as usernames and International Mobile Equipment Identity numbers), live data from the phones from the two-month interception period, and communication data from the phones originating from before the two-month interception period.[1132]

Following the hack, the Dutch police and public prosecutor conducted several investigations and prosecuted several individuals. For a legal basis for analyzing the EncroChat data, the public prosecutor requested an authorization from the investigatory judge to be allowed to analyze and use the data based on articles 126uba CCP and 126t CCP, which are the competencies for police hacking and for the placing of a recording device, when there is a suspicion of organized crime.[1133] The argumentation of the public prosecutor entailed that Dutch users of Encro phones were suspected of various forms of organized crime, this suspicion originating from a list of investigations where it was already determined that Encro phone users were involved. It was estimated there were around 12,000 Dutch users of Encro phones.

[1132] For a full description of the facts see: District Court Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1273, para. 3.2.

[1133] See also section 6.6.1.3.

According to the authorization requested from the investigatory judge, the purpose of the investigation into the data was to identify Dutch users and to investigate their involvement in organized crimes that have been committed or are planned to be committed. The authorization was granted and in that warrant the investigatory judge put forward several important requirements and safeguards to limit privacy infringements and to prevent a fishing expedition.[1134] The safeguards included that the police provide information on what software they use to perform an automated search.[1135] Moreover, the dataset was searched by the Dutch police using algorithms and specific search terms related to already ongoing investigations and based on pre-determined categorized search terms.

To give an example from a specific case: a reasonable suspicion about an individual arose after searching in an EncroChat dataset centered on cocaine, on search terms such as 'shed', 'barn' and 'hexane' and receiving hits for the individual in question. The hits led to an analysis of the messages and images of the username in question which in turn created a reasonable suspicion that the individual was involved in drug labs. After there was a reasonable suspicion, a request was put forward to the investigatory judge to authorize a further investigation into a different EncroChat dataset to find data relevant to the suspicion of involvement in drug labs of the individual. After the Encro-data corroborated the suspicion of the existence of a drug lab, the investigation expanded beyond data analysis to uncover the location and find additional suspects.[1136]

There were several criminal investigations following the EncroChat operations and several individuals were prosecuted and tried with the evidence consisting largely of EncroChat data and the criminal investigation into their case originating from the EncroChat hack. Because of this role of the EncroChat data, in these criminal trials the defense also put forward arguments pertaining to the way in which the EncroChat data were gathered, analyzed and used in criminal investigations and prosecution, contesting procedures and claiming violations of fundamental rights.[1137] This forced the criminal courts to delve into and address fundamental questions of data-driven criminal investigations.

1134 These will be discussed in detail in section 6.6.2.

1135 These safeguards are discussed below in section 6.6.1.2.

1136 For a full description of the facts see: District Court Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1273, para. 3.2.

1137 For example: District Court Rotterdam, 25 June 2021, ECLI:NL:RBROT:2021:6113; District Court Rotterdam, 24 June 2021, ECLI:NL:RBROT:2021:6050; District Court Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1273; District Court Midden-Nederland, 12 April 2022, ECLI:NL:RBMNE:2022:1389; District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584; District Court Rotterdam, 11 April 2022, ECLI:NL:RBROT:2022:2809.

It is clear from the EncroChat investigations that we need to consider the regulation of investigatory powers when it comes to data collection; regulation needs to put in place safeguards to prevent investigatory powers from being too broad in data collection from a point of view of the fundamental rights to data protection and privacy. The EncroChat investigations raise the question of how to regulate large scale data processes where first data is collected that may ultimately be used as evidence, while only later this evidence will be matched to an alias or username, and only after that to an actual name of a suspect. Generally speaking, in other forms of criminal investigation, the situation will be the other way around, in that once there is a suspect, investigatory powers are used to further investigate that suspect and collect evidence against him or her for a criminal prosecution and trial. Another point that the EncroChat cases highlight is that the automated analysis of data, such as using algorithms, plays an increasingly crucial role in furthering the investigation, so the legal basis for that needs to be examined as well. The following section delves further into these practices and regulation thereof.

6.3.2. Police hacking and tools for automated searches and data analysis

The year 2016 marked a big transition in the scale of telecommunications and smartphone data collected by Dutch police. Where previously it was extremely difficult to get access to such data due to encryption, the operation into Ennetcom in 2016 brought a big change and was succeed by many other cryptophone operations, such as the EncroChat hack.[1138] One crucial aspect in this bulk data collection is the use of analysis software that enables the actual information extraction from hundreds of millions of messages. Special software has been developed to conduct searches in such massive data sets. A prominent example - the software that was used in the EncroChat operations - is Hansken.

Hansken can be described as a forensic big data-analysis platform, which is used to search data sets after the data have been decrypted. It is designed to give access to and insight in digital data and traces originating from seized and produced material. Since 2012, the Netherlands Forensic Institute has been developing a prototype of Hansken to provide Digital Forensics as a Service.[1139] Hansken is used for criminal investigations on request of and under the direction of police and the public prosecution service. The data in Hansken are supplied by the police or other investigatory actors; the data

---

[1138] For more on these operations see: Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02.

[1139] Hansken: https://www.hansken.nl/an-introduction-to-hansken.

can pertain to convicts, suspects, witnesses, victims or third parties.[1140] Third parties are individuals that in fact have nothing to do with the crime being investigated, for example individuals whose phone number or email address just happens to be in the contact list of a suspect. The data in a specific case are accessed by Hansken specialists; once the data are read, they are encrypted and data are only stored in encrypted form.[1141] Because there are so many data and types of data processed in Hansken, the developers specified design principles aligned with data protection rules.[1142] Nonetheless, Hansken can be used as a tool for profiling, for example using algorithms in Hansken to extract behavioural characteristics of a potential suspect.[1143] The use of tools such as Hansken is likely only to increase as the volumes of data gathered for criminal investigations increase, because automated analytical tools are necessary to extract the right information. The question is how the use of such tools is regulated under criminal procedural law.

As explained previously in section 6.2.3, the use of investigatory powers that constitute more than a light infringement requires a specific legal basis. It is safe to say software such as Hansken constitutes much more than a light infringement to the right to privacy. As the use of Hansken allows to very quickly and on a large scale bring information to the fore it can therefore be considered a privacy invasive tool. There are different legal provisions that are relevant to the use of tools such as Hansken, depending on the scenario of how the data analyzed in Hansken were gathered. I focus here on hacking, as that was the way in which the EncroChat data were gathered.

There are the provisions on police hacking that set the requirements for the hacking of devices such as computers or smartphones. This competence for hacking and searching devices was introduced in response to the increasing amount of encryption of data by suspects.[1144] These provisions thus say something about the way in which the smartphone data can be gathered. There are three different provisions for hacking depending on which type of crime is being investigated: article 126nba(1) CCP, article 126uba(1) CCP and article 126zpa(1) CCP. Article 126nba CCP refers to the hacking competence in cases of suspicion of a serious crime.[1145] Article 126uba(1) CCP can

---

1140 Seyyar, M. B., & Geradts, Z. J. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, 33, 200906, p. 4.

1141 Seyyar, M. B., & Geradts, Z. J. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, 33, 200906, p. 4.

1142 Seyyar, M. B., & Geradts, Z. J. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, 33, 200906, p. 2.

1143 Seyyar, M. B., & Geradts, Z. J. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, 33, 200906, p. 4.

1144 Kamerstukken II 2015/16, 34 372, no. 3, p. 7-10.

1145 A serious crime is here based on article 67 (1) CCP.

be used in investigations into organized crime. Article 126zpa CCP can be used in investigations of crimes of terrorism. For all three scenarios, the competence is granted to the public prosecutor to, under strict conditions, give an order to an investigative officer to forcefully gain access into a computerized device used by a suspect, such as a smartphone or server. This access will usually be secretive and remote. After having hacked the device, the investigative officer can, with or without a technical aid, perform follow-up investigative acts to achieve aims described in the order.[1146] The law exhaustively lists the aims for which investigation in the device is possible:

- determining the characteristics of the device or the user (such as identity or location) and recording those;
- executing an order for intercepting and recording of telecommunication or secretly recording communication with a technical aid;
- execution of an order for systematic observation of a person;
- copying of data that are stored in the device;
- making data inaccessible (e.g. erasing).

If we take article 126uba CCP as an example, concerning organized crime, paragraph 2 describes which information should be given in the order, which is the most predominant part when it comes to safeguards. The order should inter alia include: a description of the criminal organization including the name of an individual or a detailed description to the extent possible, an indication of the device that will be hacked, the facts and circumstances substantiating the conditions from paragraph 1, a description of the acts that will be conducted, and which part of the device and which category of data the hack pertains to. The provisions on hacking also say something about the tools to collect data from the hack, from the perspective that it has to be described; article 126uba (2)(d) CCP for example prescribes that the order given by the public prosecutor should include an indication of the nature and functionality of the technical tool. Further rules, on how exactly such a tool should be used from a more technical perspective and detailing what can be done after the hack, are described

1146 Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available at: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf, p. 7.

in a decree specifically on police hacking.[1147] A provision that is relevant to the data analysis after gathering it through a hack, is article 126dd CCP, which stipulates that data gathered through a tap or through a recording device can, after an order by the public prosecutor,[1148] be shared and used for another criminal investigation than the one for which they were originally gathered. It does not stipulate further conditions to this sharing though, only that the data should be erased when no longer necessary.

6.4 Powers for risk profiling after the criminal investigation phase

Thus far this chapter focused on the use of risk profiles in criminal investigation. However, risk profiles can also be used after the criminal investigation phase. As examples of the use of risk profiling in that stage, the examples of COMPAS[1149] used in the USA as well as the Dutch example of OxRec[1150] were referred to in chapters 2, 3 and 5. Both COMPAS and OxRec are risk assessment tools that help in decision-making for criminal justice decisions such as parole, probation or prison sentencing. In chapter 3 on the challenges of risk profiling, I outlined in general how the use of such risk assessment instruments comes with challenges in terms of bias and racial profiling in addition to challenges of errors in decision-making such as false positives and negatives.[1151] For this chapter, the question remains how the use of such instruments is regulated under criminal procedural legislation. To analyze the legal basis, I will discuss OxRec as an example, as it is a Dutch risk assessment tool and thus the most relevant to illustrate the Dutch criminal procedural law.

The three Dutch probation authorities[1152] use the RISc as a risk classification tool to advise them in an estimation of recidivism risk. RISc is used in all stages of the criminal trial: in arraignment before the Examining Magistrate, in the criminal

---

1147 Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), available at: https://wetten.overheid.nl/BWBR0041426/2019-03-01.

1148 Although in the EncroChat case law it was deemed that permission from the investigatory judge was necessary to share EncroChat data, after which the public prosecutor could give the order: District Court Midden-Nederland, 16 September 2021, ECLI:NL:RBMNE:2021:4480, para. 4.1.3.

1149 See chapter 2, section 2.5.2.3.

1150 See chapter 2, section 2.5.2.3.

1151 See chapter 3, sections 3.3 and 3.4.

1152 Reclassering Nederland, Leger des Heils jeugdbescherming & reclassering, and Stichting Verslavingsreclassering GGZ.

trial, in decision-making in penitentiary programs, in decision-making about 'placement at the discretion of the state'[1153], and in decision-making on the conditions of probation.[1154] OxRec is used as an actuarial risk assessment tool within the RISc system relying on both static and dynamic risk factors.[1155] OxRec was developed originally by Oxford University and is designed to make a statistical analysis of the risk of general recidivism and of recidivism for violent crimes. In 2017, OxRec was adapted for the Dutch criminal justice system with the use of data from Statistics Netherlands, the Dutch Research and Documentation Centre (WODC) and data from the three Dutch probation authorities.[1156] Actuarial risk assessment tools can be best described as tools that focus on the correlations between characteristics of a specific individual and recidivism data, generating an indication of the recidivism of groups of people with the same characteristic as the specific individual in question.[1157] Thus group risk profiles are applied to individuals to be assessed. In the use of OxRec in the Dutch system, the probation officer drafts an advice about the situation in question in addition to the advice that follows from the OxRec system. The probation officer's advice can deviate from the one resulting from OxRec.[1158] Through RISc, the results from the risk analysis per aspect -such as finances, relationships, substance use- are shown in a traffic light model, ranging from green to orange to red, next to the risk estimation from the OxRec.[1159]

As one of the goals of the criminal justice system is to ensure a safe society, the use of risk classification tools is important to achieve that goal by identifying and classifying dangerous individuals that pose a risk to society and removing them from society for as long as they pose a significant risk (e.g. by imprisonment).[1160] Over the past years this risk management function of the criminal justice system has come to the fore, leading

---

1153 In Dutch referred to as TBS. It is a hospital order that a court can impose if an offender has a serious psychiatric disorder.

1154 Probation Netherlands, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

1155 Static factors are factors that cannot be changed by the suspect or offender, such as age or criminal history. Dynamic factors are factors that are prone to change, such as employment status, address, financial situation, and so forth.

1156 Probation Netherlands, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

1157 Probation Netherlands, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

1158 Probation Netherlands, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

1159 Probation Netherlands, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

1160 Van Wingerden, S. G. C., Leonardus Martinus Moerings, and J. A. Van Wilsem. Recidiverisico en straftoemeting. No. 2011-3. Sdu Uitgevers, 2011, p. 9.

to an increase of automated tools to perform the risk assessment.[1161] Risk assessment tools, such as OxRec, are generally labeled as an assisting tool, meaning that it is not a form of fully automated decision-making but merely advisory in the decision-making process. This advisory function raises the question how its use relates to the decision-making process of for example judges and probation authorities. According to a study on the use of risk assessment in sentencing in the Netherlands, there are three not mutually exclusive ways in which results from tools such as OxRec can be used. The first is that a judge relies on the report of the probation authority, which is based on the RISc assessment. The second is that a judge makes their own risk assessment based on static risk factors (such as gender, age, criminal history), which are not the most prominent aspects in RISc assessments. The third is that a judge makes their own risk assessment based on dynamic risk factors, which are risk factors related to the social circumstances (such as employment status, substance use, etc.) and are also the prominent factors of the RISc assessment.[1162] RISc and thus OxRec can play a more or less prominent role varying per case in this manner.

While for investigatory powers the CCP is leading as it determines how to gather data, the regulation of risk assessment in sentencing decisions is more complicated. There are three legal frameworks at play here. First, there are principles from the CCP that apply when the analysis from OxRec is used in the criminal trial. Second, there is the landscape of legal instruments applying to the probation authorities, who are the ones responsible for the use of the tools. Third, there are provisions from the Police Data Act and the Judicial Data and Criminal Records Act that apply to the data analysis.

In the CCP, we can find provisions such as article 147 CCP which regulates that the Public Prosecution Service in the interests of investigation into criminal cases can call in the assistance of a probation institution and can commission a pre-sentence report. Other provisions about the pre-sentence report are laid down in articles 177 and 310 of the CCP, in which the same power is assigned to the examining magistrate or the judge to call in the assistance of probation authorities for advice. The CCP only regulates the competency to ask for advisory reports or the expertise of the probation authorities; it does not regulate in any way how the probation authorities conduct that assessment. When a report from a probation authority is used by the court to determine the type or severity of the sanction that will be imposed, general principles of sentencing apply:

1161 Van Wingerden, S. G. C., Leonardus Martinus Moerings, and J. A. Van Wilsem. Recidiverisico en straftoemeting. No. 2011-3. Sdu Uitgevers, 2011; de Vries, Max, Johannes Bijlsma, Anne Ruth Mackor, Floris Bex, and Gerben Meynen. "AI-risicotaxatie: nieuwe kansen en risico's voor statistische voorspellingen van recidive." *Strafblad* 2021, no. 2 (2021): 58-66.

1162 Van Wingerden, S. G. C., Leonardus Martinus Moerings, and J. A. Van Wilsem. Recidiverisico en straftoemeting. No. 2011-3. Sdu Uitgevers, 2011.

article 359 CCP requires the court to motivate its verdict, more specifically paragraph 5 and 6 require the court to explain which reasons have led to choosing the sanction in question. Thus, the court has to motivate why it follows or does not follow an advice from the probation authorities, including the OxRec assessment, and why a certain sanction is justified. This requirement of explanation does not stipulate in any way what type of advice from the probation authorities can or cannot be used, or what this advice has to look like.

For the second category of legislation specific to probation authorities, the most prominent instruments are the 1995 Probation Regulation[1163] and the 2005 Probation Implementation Act[1164]. These instruments regulate the organizational aspects of the probation authorities and determine when an advice or report has to be or can be drafted. However, neither of these instruments specifies how risk assessment tools can be used in probation advice or otherwise mentions the use of risk assessment tools. More specifically, the law does not regulate or prescribe which factors or data points should or cannot be used in the assessment, under what conditions the assessment should be performed such as whether an algorithm can be used or how factors should be weighed, nor what the accuracy of the risk assessment tool should be. Internally there can be guidance documents from the probation authorities on how to use OxRec, which outline which data can go into the assessment, what the rates are for false positives and negatives and guidelines on technical control measures and other methodological safeguards.[1165] These guidelines are not a part of the legislation, nor are they public, but nonetheless determine how OxRec is used.

Third, where personal data are processed, data protection legislation will apply. In the context of criminal prosecution this will be the Police Data Act but more importantly the Judicial Data and Criminal Records Act.[1166] We can distinguish two different scenarios here: on the hand systems like OxRec can be used to make automated decisions, such as determining the sentence, or systems such as OxRec can be used in an advisory function to the court. For automated decisions extra safeguards apply from the Police Data Act and the Judicial Data and Criminal Records Act, such as human intervention in the decision-making and information to be provided to the individual.[1167] In the case of OxRec, according to the reports from the probation authorities, OxRec is only used

1163 Reclasseringsregeling 1995, no. 455985/94/6: https://wetten.overheid.nl/BWBR0007120/2019-06-26.

1164 Uitvoeringsregeling reclassering 2005, no. DDS 5378751: https://wetten.overheid.nl/BWBR0019016/2005-11-25.

1165 See: M. Maas, E. Legters & S. Fazel, Professional en risicotaxatieinstrument hand in hand: Hoe de reclassering risico's inschat. *Nederlands Juristenblad*, 17 July 2020, issue. 28 pp. 2055-2600.

1166 See section 6.5 for an elaborate discussion.

1167 See for example article 7a of the Police Data Act. See also section 3.4.3.

in an advisory capacity: the advice on the sentence is always determined by the 'human decision-maker', the probation officer. In turn, the report is presented to the court, but the court still takes its own decision on the sentence. Thus, under the current legal framework there is no issue of automated decision-making in imposing a prison sentence or imposing or prolonging other measures. If OxRec processes personal data without using automated decision-making, the general rules of the Police Data Act and the Judicial Data and Criminal Records Act still apply, which contain rules such as purpose limitation and storage limitations.

One could argue that because the legal provisions do not specify how the risk assessment should be conducted, whether for example AI can be used or not, that it is not relevant to the risk assessment whether it is conducted using AI or not. However, while the use of AI or automated risk assessment might be more efficient than human risk assessment, it does not mean it does not come with its own challenges, such as in error rates, reinforced bias in data or opacity of the risk assessment towards the offender.[1168] Thus it would have made sense if the regulation framework for the probation authorities would have specifically regulated automation aspects of the risk assessment process to address these challenges, such as determining how the automated part of the assessment can take place and which safeguards apply in terms of oversight, allowing human intervention, creating transparency and explainability, and preventing biased or erroneous results.

6.5 Legislation on processing police data, criminal procedural data, and judicial data

6.5.1 Introducing the Police Data Act and the Judicial Data and Criminal Records Act

In 2002 the Judicial Data and Criminal Records Act and in 2007 the Police Data Act were enacted. In October 2018 both of these instruments were adapted to implement the EU LED. Prior to the LED, the Dutch Police Data Act and Judicial Data and Criminal Records Act already extensively regulated the topics of the current LED, because the predecessor of the Law Enforcement Directive had been implemented extensively in Dutch law. Thus, the Dutch legislator argued that the implementation of the LED did not require drastic changes to the Dutch legislative framework.[1169] Nonetheless, since the Law Enforcement Directive is an EU instrument that requires national implementation, it is interesting to see how its requirements and safeguards are given

[1168] See chapter 3, sections 3.3, 3.4, and 3.5.

[1169] Tweede Kamer der Staten-Generaal 2017–2018, 34 889, no. 3, p. 6.

shape under Dutch law. To have a more in-depth discussion it is important to first briefly explain the scope of both instruments.

The scope of the Police Data Act is determined in article 2 of this act, which entails that the Police Data Act applies to the processing, by a competent authority, of police data which form part of a filing system or are intended to form part of a filing system. The term police data is further explained in article 1 of the Police Data Act as being personal data that are processed in the context of the police task as referred to in articles 3 and 4 of the Police Act.[1170] The scope of the Judicial Data and Criminal Records Act is determined in article 2 of said act, which determines that for this act the Dutch Minister of Justice and Security processes judicial data, or such data is processed on behalf of the Minister mainly by the Public Prosecutor, in judicial documentation in the context of criminal justice. The act addresses the Minister directly; of course in reality it will not be the actual person of the Minister processing the data, but the Minister is accountable for the process. What is understood to be judicial data is further explained under the definitions of article 1(a) of the Judicial Data and Criminal Records Act. Judicial data are categories of personal data that are determined as such by an Order in Council, which concern the application of criminal law or criminal procedure and are or will be processed in a data file. The Act also defines the term criminal procedural data. According to article 1(b), those are personal data gathered in the context of a criminal investigation that are processed by the public prosecution authority in a criminal file or in an automated way in a data file. The Police Data Act and the Judicial Data and Criminal Records Act therefore apply to different actors, but they are very similar in terms of content. For the scope of this chapter, it is good to know that the former applies to the police while the latter applies for example to prosecution and judiciary authorities. As I focus for the majority on the police and their powers in the criminal investigation in this chapter, the Police Data Act is thus most important.

[1170] For article 3 Police Act see section 6.2.1. Article 4 of the Police Act similarly lays down the general task of the military police ('Koninklijke Marechaussee').

6.5.2 Requirements for risk profiling in legislation on police, criminal procedural and judicial data

To analyze how the Police Data Act and the Judicial Data and Criminal Records Act regulate aspects of risk profiling, I will focus on provisions that are key to the data analysis in creating risk profiles and risk assessment.

Articles 8 to 10 of the Police Data Act lay down the three legal bases that can be used for processing police data. In that sense the Police Data Act distinguishes between different police tasks and assigns a different role for data (analysis) to play in each of those tasks. Article 8 of the Police Data Act concerns the general policing task, article 9 of the Police Data Act is for specific investigations and article 10 of the Police Data Act can be relied upon for gathering further information related to involvement in serious crime. The explanatory memorandum to the Police Data Act explains the regime and general approach of these three provisions; the provisions in themselves are very technical, so this general explanation is helpful to keep in mind when going through the articles 8 to 10 of the Police Data Act below. The main points of the explanatory memorandum are as follows.[1171]

The Police Data Act implements EU data protection law and thus requires that data are processed for specified purposes stated in advance. To accomplish this, the Police Data Ac distinguished between two different categories of purposes that are determined by criminal procedural law. On the one hand there are purposes that fall within the daily or general policing task; for these purposes the idea is that during the period of one year the data are available for processing; subsequently, if necessary, those data can be accessible for four years afterwards, for comparisons or search queries for authorized police staff. On the other hand there is the so-called targeted or specified processing, which is when the police start processing large-scale data aimed at either specific individuals or specific topics (such as a category of offences or crimes). For this type of processing, the purpose limitation principle is followed in requiring a specific recorded purpose in advance and that only data necessary for that purpose are processed.[1172]

Regarding the latter point, the legislator points out that the more specific the data processing becomes (more specific or revealing towards one or more persons), more protection is required based on the principle of proportionality.[1173] Thus, in this memorandum the legislator also makes clear connections between data protection

---

1171 Translation is author's own.

1172 Kamerstukken II 2005/06, 30327, no. 3 (explanatory memorandum), p. 4.

1173 Kamerstukken II 2005/06, 30327, no. 3 (explanatory memorandum), p. 9-10.

legislation (such as purpose limitation and proportionality requirements) and criminal procedural law (the different policing tasks). It is also important to realize that for the processing grounds of article 8 to 10 of the Police Data Act, no distinction is made between data of suspects and non-suspects.[1174] Below I will go through articles 8-10 of the Police Data Act in detail.

6.5.2.1 Article 8 of the Police Data Act

Article 8 of the Police Data Act pertains to the general or daily policing task. In terms of risk profiling, one can think of location-based predictive policing as an example of such as task. Paragraph 1 of article 8 of the Police Data Act determines that police data can be processed for the execution of the general policing task for the duration of one year after the first processing of said data. The time limitation for the processing makes sense as the processing is not related to a specific criminal investigation. Nonetheless, for the compilation of general risk profiles it is important to have large volumes of data for identifying patterns and correlations; for this reason there is an incentive to be able to process data without a concrete criminal investigation in mind. Under article 8(1) of the Police Data Act, police data can be processed relatively freely for the policing task, but general overarching principles still apply, which follow from data protection legislation, such as that the processing has to be necessary and proportionate for the purpose of executing the general policing task.[1175] Comparing police data gathered on the basis of article 8 of the Police Data Act with large volumes of data from open sources or other external sources is seen as disproportionate by the Dutch legislator. Thus, article 8 of the Police Data Act is not intended as a legal basis for large-scale forms of data processing combined with data from other sources.[1176]

Ultimately, paragraph 6 of article 8 of the Police Data Act requires that police data processed for the general policing task are deleted once they are no longer necessary for the executing of the general policing task and that in any case, they have to be deleted ultimately five years after the first processing. In summary, for time limitations, this means that under article 8, data can be processed for a maximum of five years: under paragraph 1 data can be processed for a year and they can be available for a maximum of four years after that for automated comparison under paragraph 2 or a combined

---

1174 Kamerstukken II 2005/06, 30327, no. 3 (explanatory memorandum), p. 11.

1175 Article 3 of the Police Data Act contains the principles of necessity and lawfulness of the data processing and the purpose limitation principle. These principles originate from the data protection legislation on the EU level, i.e. the EU Law Enforcement Directive. For a discussion of data protection legislation see chapter 4 of this dissertation, chapter 6 only focuses on requirements on the level of national implementation.

1176 Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 8 Wpg, no. 2 (1 July 2022); Kamerstukken II 2005/06, 30327, no. 3 (explanatory memorandum), p. 38.

search under paragraph 3. While data are originally processed for the general policing task, this does not limit the data to only be processed for said task: article 8(4) of the Police Data Act determines that these data can be made available for further processing under article 9 or 10 of the Police Data Act, in which case the retention periods of those articles apply.

To allow for data comparison, article 8(2) of the Police Data Act determines that data that are older than a year can be compared in an automated way with other police data processed under article 8(1) of the Police Data Act, to determine whether there are connections between the data. However, after a year there is a less urgent necessity to establish connections between events, and the protection of the individual citizen and protecting their data against unlimited processing becomes stronger, therefore paragraph 8(2) of the Police Data Act poses some restrictions.[1177] Data that are older than a year can be made available for comparing under article 8 of the Police Data Act after a concrete incident and searches can only be performed in data that are older than one year using data that are not a year old yet (to search for a match). It should be noted that article 8(2) of the Police Data Act speaks of comparing data, which is more limited than processing of data: comparing in the Police Data Act means specifically that investigative officers can only compare data already known to them with other data; further searches are not allowed here.[1178] Another limitation in article 8(2) of the Police Data Act is that the comparison can only be performed for the purpose of the general policing task; for other purposes article 11 of the Police Data Act can sometimes serve as a basis, as will be discussed later in this section. If there is a match in data after the comparison under article 8(2) of the Police Data Act, the correlated data that resulted from the comparison can only be processed for the general policing task to the extent that it is necessary.

Similarly, article 8(3) of the Police Data Act determines that, in deviation from article 8(2) of the Police Data Act, police data for which the one-year term has passed can also be combined in a way with other data for which this term has passed to assess whether there are connections between the data. More specifically, paragraph 3 of article 8 of the Police Data Act allows for the analysis of data that are not available based on paragraph 1 of article 8 of the Police Data Act, but only to the extent that combined queries can be used to make connections between data for the general policing task; thus this describes the situation where older data can still be put together to shed light

---

1177 Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 8 Wpg, no. 3 (1 July 2022); Kamerstukken II 2005/06, 30327, no. 3, p. 10-11.

1178 See also: Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 8 Wpg, no. 3 (1 July 2022); Kamerstukken II 2005/06, 30327, no. 3, p. 40.

on an individual that might be interesting to open an investigation on. The idea behind this paragraph is to provide a legal basis for analysis to assess if an investigation in the sense of article 9 or 10 of the Police Data Act is required.[1179] Neither the Police Data Act itself nor the explanatory memorandum define what is meant by combined queries. Nonetheless, the memorandum does give an example of the importance of a search under article 8 of the Police Data Act in general: searches in the data for the general policing task are important to identify potential habitual offenders; the search results can indicate which individuals in what areas should be monitored more intensely, which ones are more likely to be arrested, or which ones should be referred to specialist institutions for help.[1180]

The most important goal of article 8 of the Police Act seems to be to allow the police to make connections between different reported or observed events and facts, to assess which individuals or events stand out and require further investigation. From a perspective of regulating the general policing task, article 8 of the Police Data Act has to offer on the one hand enough possibilities for the police to process all available data such as from police reports, witness reports, and statements, and distill the crucial information from those and deduce important connections, while on the other hand there have to be limitations to the collection and combination of data, and personal data have to be processed in a way that is proportional to the goal for which they were collected.[1181] In that sense article 8 of the Police Data Act functions as a first step in the risk profiling process: connections can be made between data points and data are combined that allow for the generation of risk profiles.

If risk profiles are constructed, the question is how this result of data processing under article 8 of the Police Data Act should be treated: what status does the risk profile itself have? More specifically, can the profile itself can be considered personal data? The answer to this question matters for the determination which legislation applies. As discussed in chapter 4, this is, however, not a question with a clear answer.[1182] Article 8 of the Police Data Act does not stipulate that the results of the analysis, such as the profile, have to be deleted. The question of how to treat risk profiles as pieces of data that do not always have a clear connection yet to a criminal investigation, is a question that is situated in a boundary area between data protection legislation and criminal procedural legislation: as it concerns the processing basis for data it would most naturally appear to be a question that should be regulated under data protection

1179 See also: Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 8 Wpg, no. 4 (1 July 2022).

1180 Kamerstukken II 2005/06, 30327, no. 3, p. 11.

1181 Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 8 Wpg, no. 1 (1 July 2022).

1182 See chapter 4, section 4.1.

legislation, but as discussed in chapter 4 of this dissertation, the EU LED does not provide an answer. The national implementation of the Police Data Act similarly does not regulate what happens to the results of processing under article 8 of the Police Data Act. At the same time, because bases for processing police data are not regulated in the CCP, no answers can be found there either. It can thus be argued that this is a normative question that currently falls in between two regulatory frameworks.[1183]

6.5.2.2 Article 9 of the Police Data Act

Article 9 Police Data Act concerns processing police data in a more targeted way than under article 8 of the Police Data Act. Article 9(1) of the Police Data Act determines that police data can be processed in a targeted way for the purposes of an investigation with a view to maintaining the public order in a specific case, i.e., the investigation of one or more specific crimes. The purpose of the investigation has to be put down in writing within a week after starting the processing, according to article 9(2) of the Police Data Act. In the context of risk profiling, article 9 of the Police Data Act can thus be used either when there is a suspect for which to conduct a specific risk analysis or for creating a risk profile for a specific criminal investigation to find a suspect for the crime at hand.

Article 9(3) of the Police Data Act determines that police data processed under article 9(1) of the Police Data Act can, after permission from a qualified officer, be made available for further processing if necessary for another investigation as referred to in article 9(1), article 10, article 12 of the Police Data Act or for execution of the daily policing task of article 8 of the Police Data Act. That the data can be made available for another purpose indicates a one-way connection: it is not allowed to use article 9(3) of the Police Data Act vice versa to assess if there are other relevant data available within the police organization. For the latter scenario there are other legal bases available, such as article 11 of the Police Data Act.[1184]

Lastly, article 9(4) of the Police Data Act determines that police data that are processed under article 9(1) of the Police Data Act and that are no longer necessary for the purpose

---

[1183] The status of profiles or the outcome of analysis is not explicitly mentioned, but Galič and Schermer do point towards a lack of regulation after the data collection, for data analysis and further use of the data: Galič, M. (2022), 'Bulkbevoegdheden en strafrechtelijk onderzoek: wat de jurisprudentie van het EHRM ons kan leren over de normering van grootschalige data-analyse', *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 8(2), pp. 130-137; Schermer, B. W., & Galič, M. (2022). Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen? *Nederlands Tijdschrift voor Strafrecht*, 3(3), 167-177. [2022/38], https://doi.org/10.5553/NTS/266665532022003003006; Schermer, B.W., 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017.

[1184] Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 9 Wpg, no. 4 (1 July 2022).

of the investigation shall be either deleted or processed for the term of maximum half a year to assess whether they give rise to new processing under article 9 or 10 of the Police Data Act and deleted afterwards. When exactly data are no longer necessary for the purpose of an investigation will depend on the situation: usually when data are processed for a criminal investigation in the sense of article 132a CCP, and the investigation leads to prosecution of the individual, the data are only no longer necessary when the trial judge has irrevocably decided on the case.[1185]

6.5.2.3 Article 10 of the Police Data Act

Article 10 of the Police Data Act provides the basis for processing police data to gain information of an individual's involvement in serious crime. Article 10 Police Data Act is in that sense a legal basis for the police to gather intelligence: an important difference between article 9 and 10 of the Police Data Act is that for the former the investigation of a specific crime at hand is the central factor, while for article 10 of the Police Data Act the main aim is building an information position rather than processing data about a concrete event.[1186]

Article 10(1) of the Police Data Act states that police data can be processed focused on creating insight in the involvement of persons in three categories of serious crimes. The categories of crimes listed are, first, crimes from article 67 paragraph 1 of the CCP (which are crimes for which pre-trial detention is allowed)) that concern organized crime and that pose a serious threat to public order; crimes that are punishable by a maximum prison sentence of eight years or more; and third, crimes under article 67 paragraph 1 of the CCP that are designated in an Order in Council[1187] and that pose a serious threat to public order. For the involvement in serious crime, article 10 of the Police Data Act includes not only committing such crimes, but also the preparation of such crimes. According to paragraphs 2 to 4 of article 10 of the Police Data Act, the processing can concern suspects of such crimes, persons against whom there is a reasonable suspicion that they are involved in preparing such crimes, but also persons that are 'in a certain relation' to the former two (what constitutes such a relation is not explained by the legislator).

Article 10(5) of the Police Data Act, similar to articles 8 and 9 of the Police Data Act, determines that police data processed under article 10(1) of the Police Data Act can be made available for further processing. Article 10(6) of the Police Data Act requires

---

1185 Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 9 Wpg, no. 5 (1 July 2022).

1186 Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 10 Wpg, no. 1 (1 July 2022).

1187 These crimes are listed in article 3:1 of the Police Data Decree [Besluit politiegegevens], which contains around two dozen serious crimes.

police data processed under article 10 (1) of the Police Data Act to be deleted when they are no longer necessary for the purpose of the processing; to make that determination the data should be checked periodically. The data shall be deleted ultimately five years after the last processing that shows the necessity of the processing.

6.5.2.4 Processing grounds

In summary, articles 8 to 10 of the Police Data Act thus determine for which police activities police data can be processed, regarding which persons these data can be processed, for how long the data can be processed, and when the data can be processed for another investigation or police activity. As described in section 6.2 of this chapter, in the CCP and Police Act there is the similar distinction between the general policing task, the criminal investigation and special investigatory powers that can be used in the investigation of serious and organized crime. The different legal requirements of the Police Data Act for processing police data along different tasks or stages of policing match the tasks as described in the CCP and Police Act. How long data can be processed or kept, and which data can be compared for risk profiling purposes will thus depend on the type of policing activity it is used in, which is either the general policing task, or a specific criminal investigation, and whether the investigation involves certain serious crimes or not.

6.5.2.5 Article 11 of the Police Data Act

In addition to the regulation of processing bases, the Police Data Act contains another provision that is extremely relevant for risk profiling, namely article 11 of the Police Data Act, as this provision regulates the process of automated comparison of or combining of data. Article 11 of the Police Data Act regulates automated searching in and combining of police data that are being processed for other purposes, for example, when while processing police data under article 9 of the Police Data Act for an investigation, an investigative officer needs to search police data processed under article 8 of the Police Data Act.[1188] Article 11(1) of the Police Data Act lays down these possibilities for investigations under article 9 of the Police Data Act; article 11(2) of the Police Data Act lays down these possibilities for intelligence gathering under article 10 of the Police Data Act.

Article 11 of the Police Data Act roughly distinguishes between two situations: automated comparison of data and combined processing of data. For automated comparisons, authorized investigative officers can put in queries that will either show 'a hit' or 'no hit' for police data processed for other purposes. For processing data processed for different purposes in a combined way, all police data can be queried and

[1188] Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 11 Wpg, no. 1 (1 July 2022).

used for the purpose of having to combine data: in case this leads to the discovery of relevant data or correlations, those can be further processed for the purpose for which the comparison was performed.[1189] Processing data in a combined way (paragraph 4) is a much broader analysis competency than automated comparisons (paragraph 1 and 2): the former can only be applied in situations where a strict requirement of necessity is met, such as processing data to prevent a terrorist attack, to investigate an ongoing hostage situation, or to investigate a series of serious crimes.[1190] For these situations there is a need to combine all relevant data about a situation, location or group of people. Authorization from the public prosecutor or the mayor is required for processing in a combined way under article 11(4) of the Police Data Act.

The legislator deemed it necessary to put up strict requirements for a search in police data given the potential far-reaching privacy implications; for example, keeping in mind situations that individuals can be labelled as a victim or witness in the system and through a search come to the police's attention in another capacity such as a suspect; or data that were gathered with far-reaching powers could through a search suddenly become available for a purpose for which such a far-reaching investigative power was not allowed. Another reason for caution is that data that were processed under article 9 or 10 of the Police Data Act have not always been checked yet for correctness, for example when it concerns bulk data gathered through seizing computer data or through a phone tap, and especially bulk data can also contain data of non-suspects.[1191] Article 11 of the Police Data Act is the main provision regulating big data type of analytics performed by the police, as it allows for combining data and deriving correlations.[1192] All in all, automated searches and combinations in police data should be far from unlimited. The main restrictions come in the form of authorizations: these can be found in more specific legislation, namely the Police Data Decree. The Police Data Decree further elaborates on provisions from the Police Data Act: this mainly concerns rules regarding authorizations, the grounds on which the provision of police data can be refused, but also the transparency and coding of police data for the purpose of automated comparison.[1193] Articles 2:1 and 2:2 of the Police Data Decree outline which types of investigative officers have the authorization to make use of article 11 of the Police Data Act.

1189 See also: Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 11 Wpg, no. 1 (1 July 2022).

1190 Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 11 Wpg, no. 5 (1 July 2022).

1191 Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 11 Wpg, no. 1 (1 July 2022).

1192 Schermer, B.W., 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017, p. 207-216.

1193 Groenhart, Lexplicatie, commentaar op regeling Besluit politiegegevens.

Article 2:11 of the Police Data Decree, which corresponds to article 11 of the Police Data Act in the sense that it stipulates further rules, is also relevant to risk profiling. Article 2:11 of the Police Data Decree determines how the correlations between the data following the automated comparison have to be made visible, based on data labeling or coding. The labels can be used to indicate prior to an analysis based on article 11 of the Police Data Act to the officer whether and to what extent the results will be visible to them and whether they require further authorization to use the results.[1194] There are various scenarios possible: it can be that only the data that are shown as 'related' by the system are visible to the officer; it can be that matching data are (partially) visible and in addition some related data as well; it is possible that permission from an authorized official is needed first before results can be reviewed; and so forth. The label of the data refers to the type of crime that is being investigated, for example whether the data concern the possible involvement of an individual in a crime, or whether the data concern the involvement of a person in serious crime that poses a threat to the public order. Again, the Police Data Decree follows the three-way distinction from the Police Data Act in the sense that data can pertain to the general policing task, a specific criminal investigation into crime, and the intelligence gathering into serious crime. The term 'matching data' refers to whether there is a hit or not between different data points and what the 'hit' consists of. Ultimately, these rules from the Police Data Decree determine which data is visible to whom within the police organization.

6.5.2.6 Categorization of data

A last aspect of the Police Data Act that is interesting to examine when it comes to national implementation related to criminal law, is how the regulation of police data relates to distinctions made in criminal procedural law. The EU LED requires Member States to make a distinction where possible in their national laws on police data between different categories of persons of whom data are processed: suspects, victims, witnesses or convicts. Following this requirement of the LED, article 6b of the Police Data Act determines that the controller from a data protection point of view indeed distinguishes between these four categories as much as possible.

In the explanatory memorandum on the implementation of the LED in Dutch law, it is explained that in general the information systems of the different criminal justice actors indeed distinguish between these categories of people. At the same time the explanatory memorandum also points out the practical dilemma of maintaining such a categorization, as this type of labelling is fluid: for example, an individual can be a suspect at one point in the investigation and later on in the investigation be no longer a suspect but a witness. The explanatory memorandum does not put much emphasis

[1194] Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 11 Wpg, no. 4 (1 July 2022).

on this fluidity; the fluidity between different categories of individuals is addressed by stating that a change in status of individual, such as being a witness instead of a suspect, is usually altered in the systems immediately.[1195]

The distinction between suspects, victims, witnesses and convicts is highly relevant for the criminal justice system in two aspects. The first of these aspects is safeguarding the presumption of innocence: individuals who are not convicted of a crime should not be treated as guilty, and thus their data should not be labeled as such.[1196] Therefore it is important to distinguish between different categories, to have clear at all times whether someone is for example convicted of a crime or not. The second aspect is related to the storage time of police data, as the LED requires Member States to regulate time limits for storage and review of different categories of police data from the perspective of proportionality and necessity.[1197] Although the explanatory memorandum does not seem to view the fluidity between the different actors of victims, witnesses, and suspects, as a problem, it will depend on police practices whether it is truly feasible to change these labels in the systems so quickly.

Not only can individuals move between categories over time, but especially in the case of risk profiling where large-scale data or unstructured data are collected and analyzed later, it will not be immediately clear which data belongs in which category. As was already discussed in section 6.3.2, data such as in tools like Hansken, concerns data of networks of individuals where it will not be clear for people in the social circle of a suspect if these people are victims, third parties, witnesses, suspects, and so on. Interestingly, the Police Data Act also does not set rules to safeguard a distinction between categories; for example in the legal bases of article 8 to 10 of the Police Data Act, there are no different rules for different data subject categories. Some scholars criticize that the LED does not require Member State law to distinguish between different policing purposes and the categories of personal data that should be accessible (personal data from convicts, suspects, witnesses, victims).[1198] Thus, the Dutch implementation in the Police Data Act negates this criticism to some extent,

---

1195 Tweede Kamer, vergaderjaar 2017–2018, 34 889, nr. 3, p. 66-67.

1196 LED, recital 31: "This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively."

1197 EPDS, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019. Available at: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf.

1198 C. Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, *Computer Law & Security Review*, Volume 34, Issue 1, 2018, page 161, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.08.002.

as there are different rules for different purposes, but within those rules there is no attention for the different categories of data subjects.

6.5.2.7 Interim conclusion

The legal framework of the Police Data Act and Police Data Decree differentiates between concrete actions, such as a specific criminal investigation, and between more untargeted actions such as building an information position or compiling risk profiles. The aim of the Police Data Act and Police Data Decree is to strike the precarious balance between these different tasks and the interests of individuals, most prominently the right to privacy. Thus, for risk profiles there is a difference in how the data can be analyzed depending on which type of police activity they are used for. The safeguards consist of three categories: purpose limitations, time limitations and authorizations.

Risk profiles are regulated in this legislation through different aspects. Processing grounds determine for which purposes data about whom can be processed -i.e. analyzed, combined, stored and used. For the actual analytics part of the risk profiling process, beyond the purpose, the law determines how data can or cannot be matched and combined. However, the legislation does not determine much of the actual analytical process beyond matching data. For the analysis most requirements seem to have to follow from EU data protection legislation (the EU LED), which would then have to be the general processing principles; on the national level the analytical safeguards are mostly directed at the authorizations and distinguishing between purposes. The Police Data Act and Police Data Decree do not regulate the gathering of data as such in terms of legality to collect the data (this falls within the scope of the CCP).

The explanatory memorandum to the Police Data Act explains how the Police Data Act meets the requirements of article 8(2) ECHR for interferences to the right to privacy. First, the Police Data Act would meet the requirements of foreseeability through the different bases of articles 8 to 10 Police Data Act and through requiring a specific purpose for the processing. In addition, the law should be of sufficient quality according to ECtHR jurisprudence, which would also require that the law is specific enough and contains safeguards against random interferences and against abuse of power. Lastly the law should also stipulate a competent authority and rules for transparency such as recording of processing activities.[1199] The legislator specifically mentions the ECtHR *Rotaru*[1200] case here, which according to the legislator, stipulated that the law has to indicate inter alia which categories of persons the data concerns,

---

[1199] Kamerstukken II 2005/06, 30327, no. 3 (explanatory memorandum), p. 8-9.

[1200] ECtHR, *Rotaru v. Romania*, 2000.

the circumstances of the data collection and the storage limitations.[1201] In conclusion, I would thus say that while the Dutch Police Data Act defines purposes of processing and storage limitations, these follow the different policing tasks rather than the categories of people to which the data pertains. This can mean one out of two things: either these data are in fact labeled but it happens in practice and is not stipulated as such in the law, or it is in fact too difficult to correctly categorize the persons to whom the data pertains before analysis of the data.

6.6 Difficulties in applying the legal framework to risk profiling

Where sections 6.3 to 6.5 described the legal framework applicable to risk profiling, this section entails a more normative examination of the legal framework. In some ways it seems that the current legal framework is not well equipped to be applied to risk profiling, which potentially leads to gaps in fundamental rights protection for those subjected to risk profiling. In this section I analyze these tensions between risk profiling and criminal procedural law according to three aspects: first, the different nature of risk profiling compared to other forms of policing through its combination of preemptive and large scale data collection and analysis; second the relation or interplay between the CCP and the Police Data Act, which is strained by the different nature of the two instruments; and third, the opacity and complexity of risk profiles in the context of the right to a fair trial.

6.6.1 The shift from reactive policing to pre-emptive and predictive risk-based policing

The idea of using risk profiles is to identify and classify the risk of crime occurring and to act accordingly. Therefore, an important advantage of such tools is the potential to intervene early before the risk manifests, for example to arrest suspects involved in the preparation of serious crime or to detain an individual for a longer period to avoid repeating of crime. From that pre-emptive perspective, in the most extreme risk-avoiding scenario, there would be a society with almost no crime because individuals could be apprehended while preparing their crimes before they can come to completion. However, that is a very far-fetched scenario. In addition, the reality is that like with any other technology or practice, there are limitations and risk profiles are not created and used in a perfectly preventative way.

[1201] Kamerstukken II 2005/06, 30327, no. 3 (explanatory memorandum), p. 8-9.

Instruments such as the CCP have as one of their functions to offer legal protection against the possible interferences of fundamental rights caused by investigatory police powers.[1202] For such a system of checks and balances to work properly it is important that the checks and balances come into effect in the right time in the criminal procedure. This is where a tension lies for risk profiling: while the practice of risk profiling is very much a preventative or preemptive process, the CCP with its system of checks and balances stems originally from reactive methods of policing.[1203]

6.6.1.1 Disruption as a new policing strategy

Risk profiles are not just used to prevent future crime but also to mitigate the effects of on-going crime: an increasingly popular strategy in policing in the Netherlands is to disrupt crime rather than to focus on the prosecution and trial of past crimes. The police strategy of disrupting crime was already extensively discussed in the early 2000s[1204]. More recently, disrupting crime rather than prosecuting specific crimes seems to be a recurring strategy to manage budget constraints and to measure performance of the police, especially in areas of crime such as cybercrime, more specifically in relation to anonymous online platforms used for digital crime.[1205] When focusing on disrupting crime it is not necessary to prevent crime from taking place altogether but rather disrupting it as much as possible while crimes are being committed, so that the benefits or pay-off for the perpetrators is lowered. Similar to the prevention of crime, the strategy of disrupting crime puts strain on the CCP as a regulatory framework. Because disruption of crime is targeted towards motivating offenders to not to commit crime any longer, instead of being able to prosecute or gather enough evidence for a trial, it requires a strong intelligence or information position rather than investigative skills.[1206] A concrete example of disrupting crime as a strategy can be found in the disruption of online drug markets, where the Dutch police infiltrates the market and

---

1202 See for example: R. Foqué & A.C. Hart, *Instrumentaliteit en rechtsbescherming*, Gouda Quint-Kluwer Rechtswetenschappen, Arnhem-Antwerpen 1990, p. 17; G.J.M. Corstens & M.J. Borgers, *Het Nederlands strafprocesrecht*, Kluwer, Deventer 2011, p. 6.

1203 See the work by Koops already on this in 2009: Koops, B. J. (2009). Technology and the crime society: rethinking legal protection. *Law, Innovation and Technology*, 1(1), 93-124.

1204 van Soomeren, P., Beerepoot, A., Meijer, R., & de Waard, J. (2005). Tegenhouden als nieuw paradigma voor de politie? Available at: https://www.dsp-groep.eu/wp-content/uploads/11abTegenhouden_als_nieuw_paradigma_voor_de_politie.pdf; Visiedocument, 2001/4: Projectgroep Opsporing (Raad van Hoofdcommissarissen), Visiedocument 'Misdaad laat zich 'tegenhouden"; Advies over bestrijding en opsporing van criminaliteit, Amsterdam, 2001.

1205 Oerlemans, J. J., & Wegberg, R. S. van. (2019). Opsporing en bestrijding van online drugsmarkten. *Strafblad*, 17(5), 25-31. Retrieved from https://hdl.handle.net/1887/83008; Rijksbegroting 2020 Justitie en Veiligheid (Kamerstukken II 2019/20, 35300-VI, no. 2, p. 21)

1206 See also: van Soomeren, P., Beerepoot, A., Meijer, R., & de Waard, J. (2005). Tegenhouden als nieuw paradigma voor de politie?, p. 37, available at: https://www.dsp-groep.eu/wp-content/uploads/11abTegenhouden_als_nieuw_paradigma_voor_de_politie.pdf.

servers, effectively taking control over the online market and its data.[1207] Another example is influencing the reputation of sellers on online illegal markets in a negative way with a wave of fake reviews, creating distrust towards a market by taking it offline, or going further and taking over a market or online infrastructure completely.[1208] Thus disruption focuses on removing a relevant motive, increasing the risk of being caught or lowering the pay-off. Especially in cybercrime more deterrent police strategies are important, as the risk of being caught by the police can be relatively low. Already the generation of media attention that comes with disruption operations can be a way for police to deter and prevent crime.[1209]

Risk profiles can facilitate disruptive police strategies by providing the police with an information position where in society the risk is highest of what crime. While the disruption of crime rather than the prosecution of crime is a fundamentally different approach to policing than the approach under the CCP, it is a practice not yet widely researched in the Netherlands[1210] and is also not a practice that receives special attention in the modernization of the CCP. Due to the different nature of disruption operations (of not focusing on evidence collection for prosecution or trial and focusing on a crime infrastructure rather than individual suspects) compared to more traditional policing operations, these policing strategies and powers require more fundamental legal research on the adequacy of the CCP in providing checks and balances to regulate this new approach in policing.

6.6.1.2 Reasonable suspicion and proportionality in large scale pre-emptive data collection

Apart from disruption operations, risk profiles are used in general in pre-emptive forms of policing focusing on risk mitigation. The tension between the CCP in regulating

---

1207 Oerlemans, J. J., & Wegberg, R. S. van. (2019). Opsporing en bestrijding van online drugsmarkten. *Strafblad*, 17(5), 25-31. Retrieved from https://hdl.handle.net/1887/83008.

1208 Zand, E. van 't, Matthijsse, S., Fischer, T., & Wagen, W. van der. (2020). Interventies voor cyberdaders. In: *J. J. Oerlemans & M. Weulen Kranenbarg (Eds.), Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (pp. 259-287). Den Haag: Boom criminologie. Retrieved from https://hdl.handle.net/1887/3307585.

1209 Zand, E. van 't, Matthijsse, S., Fischer, T., & Wagen, W. van der. (2020). Interventies voor cyberdaders. In: *J. J. Oerlemans & M. Weulen Kranenbarg (Eds.), Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (pp. 259-287). Den Haag: Boom criminologie. Retrieved from https://hdl.handle.net/1887/3307585.

1210 Oerlemans touches upon this topic in several works but also seems to conclude that disruption is used alongside the goal of gathering evidence for the prosecution of a suspect, see: Oerlemans, J. J. (2017). Normering van digitale opsporingsmethoden. Nederlandse Defensie Academie. See also this recent article which does touch upon the topic of disruptive strategies becoming a goal in addition to criminal investigation: M.F.H. Hirsch Ballin & J.J. Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijke optreden', *DD* 2023/2.

policing as a mostly reactive practice, apart from investigations into terrorist crime and certain forms of organized crime, and risk profiling as a preemptive process can be most clearly seen in the safeguards for suspects, defendants and others subjected to investigatory powers.

Data are increasingly collected on a large scale, possibly including data from individuals against whom a criminal investigation will not commence. For example in the EncroChat cases, such police practices include the gathering and analysis of all messages (related to Dutch users) on a server, meaning that there can also be analysis of text messages and files from individuals that are not suspects or of suspects who will ultimately not be further prosecuted. This wide casting of the net in some scenarios raises questions about proportionality of data collection and processing by the police. For the compilation of risk profiles large volumes of data are required to detect patterns and correlations between individual or group characteristics and crime risks. In addition, the profiles are applied to a large pool of individuals. Taking the EncroChat operations as an example demonstrates the difficulties with maintaining proportionality in large-scale inductive data collection: in the EncroChat cases communications data were intercepted on a large scale to determine patterns and analyze these subsequently to determine which individuals to investigate. This raises questions of how to determine which individuals can be included in data collection and which data can be collected if there is no specific suspect yet.[1211] There is a tension here in legal protection because the protection of the CCP is strongly connected to checks and balances ex-post, in the form of having a trial judge review the criminal investigation and prosecution. This is compensated only to a certain degree by existing forms of ex-ante checks and balances. For the latter, the main system of checks and balances is that of the supervision by the investigatory judge.

In the investigation involving EncroChat data, an authorization was given by the investigatory judge to analyze the data, based on article 126uba CCP and article 126t CCP, including specific safeguards, which can be summarized as follows:

- the way in which the hack of the device (in this case the EncroChat server) was performed has to be recorded, if the means were not already pre-approved;
- a description of the used software available for investigation, if the means were not already pre-approved;

[1211] The cases: District Court The Hague, 14 June 2022, ECLI:NL:RBDHA:2022:5762; District Court Limburg, 26 January 2022, ECLI:NL:RBLIM:2022:571; District Court Limburg 26 April 2022, ECLI:NL:RBLIM:2022:3227; District Court, Noord-Holland 4 May 2022, ECLI:NL:RBNHO:2022:3833; District Court Amsterdam, 11 May 2022, ECLI:NL:RBAMS:2022:2384; District Court The Hague 12 May 2022 ECLI:NL:RBDHA:2022:4504.

- the integrity of the stored information has to be guaranteed;
- the investigation in the data has to be reproducible and use listed search keys;
- it has to be prevented that privileged communications, i.e. between clients and attorneys, are captured;
- the information gathered using the search keys has to be provided within two weeks to the investigatory judge for assessment, and can only after approval be shared with the public prosecution authority and the police for the criminal investigation;
- this authorization from the investigatory judge is only for a limited duration (four weeks) and could only be prolonged through an official request. If the intermediate assessment described above would give rise to it, the four weeks authorization could also be ended early.[1212]

These safeguards were deemed sufficient by the investigatory judge 'to prevent a fishing expedition'.[1213] The safeguards set clear requirements on the transparency or reproducibility of the process, which matters for the defense to able to put up a proper defense during the trial. The safeguards limit the scope of the investigation through the required authorization of search keys. The scoping of the investigation is dependent on the assessment of reasonable suspicion conducted by the investigatory judge. All of the safeguards entail a judicial system of checks and can be applied in other situations of large-scale data collection by police as well. The court in the trial that followed from the investigation, ruled that these safeguards from the investigatory judge help achieve goals of proportionality and subsidiarity for the recording and searching of such large data sets.[1214] The court does perform a test of the reasonable suspicion criterion to assess the legality of the data collection and analysis from that perspective: more specifically the court assesses whether the investigatory judge was right to conclude that there was a reasonable suspicion that the *EncroChat users* were guilty of organized crime.[1215] It is important to note that this is not the same as an individualized reasonable suspicion; it is merely a suspicion against EncroChat users in general. Such a suspicion, against a group considered high risk of committing crimes, is exactly an example of risk profiling.

1212 District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584, para. 2.1; the authorization is discussed in other EncroChat case law as well, in the trial against other suspects following from the same EncroChat operation, e.g. in District Court Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1273.

1213 District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584, para. 2.1.

1214 District Court (criminal law) Noord-Holland 4 May 2022, ECLI:NL:RBNHO:2022:3899, para. 3.7.

1215 District Court (criminal law) Noord-Holland 4 May 2022, ECLI:NL:RBNHO:2022:3899, para. 3.7.

Applying this reasoning directly to the use of risk profiles, I would argue that it is important that criminal law courts perform this check of reasonable suspicion in large-scale data collection and analysis, for two reasons. First, there is the inherent risk when analyzing large-scale data for patterns or categorizing individuals that data are analyzed of individuals who are not involved in crime. Thus, even though no reasonable suspicion can be formed against specific individuals before the data are analyzed, there needs to be sufficient evidence that the dataset at large contains data of people involved in (organized) crime, and safeguards for proportionality, such as limiting the search keys that can be used, are crucial. Second, there is a challenge in the form of a chicken and egg problem: the police require data analysis to assess who is a suspect, but they first need to have some supporting facts on who is a suspect before they should be allowed to collect the data. Therefore, it is an important safeguard that the investigatory judge reviews the evidence prior to giving an authorization, to ascertain that there are indeed enough facts that point towards a reasonable suspicion, and the trial judge has to be able to review this decision afterwards in the trial stage.

Profiling practices raise questions of protection of groups and group interests. There is a shift in focus and impact of policing from the individual towards targeting groups and using aggregated data, for example in open-source intelligence and creating group profiles to facilitate detection of crimes and in risk assessment, and in some cases focusing on locations such as with hot spot policing. Or, profiles can result in a policy or practice towards groups, for example to stop and search individuals of a certain ethnicity and age based on a risk profile. Here there is an important interplay with legal frameworks other than criminal procedural law: data protection legislation and non-discrimination could play a role in the analysis of data, creation of group profiles and use of group profiles, but also have their own limitations in regulating the group aspect.[1216] The CCP in its regulation of investigatory powers for risk profiling is very much focused on the individual: in creating competencies for the investigatory powers, interferences to the right to privacy are created which require an appropriate legal basis. The privacy interests that are taken into account in this legal basis are however the privacy interests of the individual, not of groups.[1217] Both privacy law and criminal procedural law have an important shortcoming when it comes to profiling, in that they assume an identified individual as the subject of legal protection, while in group profiling processes, or risk analysis such as in the EncroChat investigation,

---

1216 See the conclusions of chapters 4 & 5.

1217 Stevens, L., Hirsch Ballin, M., Galic, M., Buisman, S., Groothoff, B., Hamelzky, Y., & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2021(4), p. 237.

the individual is not selected as an individual but as a part of the group;[1218] in the EncroChat investigations all EncroChat users were lumped together, and only later did a possible individual reasonable suspicion arise. The focus of the regulatory framework on the reasonable suspicion against the individual is also visible in the Police Data Act when it comes to the analysis of the data, as the scope of the Police Data Act is personal data and not so much regulating the analysis and use of group data or statistical data. Stevens et al. make a similar argument in their paper on preventive policing, where they argue that there is a tension between the use of article 8 Police Data Act as a basis for data processing for preventative purposes, while article 8 Police Data Act assumes the data pertain to an identifiable individual.[1219] The regulatory framework for risk profiling leaves a gap here and should also contain provisions on the use of data that does not pertain to identifiable individuals, both in the Police Data Act and in the CCP.

The EncroChat case law demonstrates the importance of criteria that form a regulatory framework to determine under which conditions to collect data on a large scale, to make concrete how proportionality in such cases can be safeguarded. Another example of safeguards in proportionality can be found in data protection in case law of the CJEU on data retention, such as in Digital Rights Ireland. The CJEU in Digital Rights Ireland determined that a blanket provision for data retention was not in line with the fundamental rights protection of articles 7 and 8 of the Charter, as requirements and safeguards such as on access and authorization were lacking.[1220] The same argumentation can be applied to police data collection for the creation of risk profiles: it concerns a vast collection of data, also of many individuals that are ultimately not suspects (such as phone contacts of suspects), or data that reveals aspects of their life not relevant to the criminal investigation.

The use of tools such as Hansken shows how easily data can be compiled and analyzed in one go, creating significantly less work for investigative officers. The Koops Committee in their analysis of the current regulatory framework remarks that in the past, investigations involving data, such as smartphone data, were implicitly regulated by the limited knowledge and expertise available, but that such implicit limitations are

1218 Stevens, L., Hirsch Ballin, M., Galic, M., Buisman, S., Groothoff, B., Hamelzky, Y., & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2021(4), p. 237.

1219 Stevens, L., Hirsch Ballin, M., Galic, M., Buisman, S., Groothoff, B., Hamelzky, Y., & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2021(4), p. 237.

1220 CJEU, Digital Rights Ireland, 8 April 2014, ECLI:EU:C:2014:238.

disappearing through automation.[1221] The Koops Committee recommends to create proportionality requirements in concrete guidelines for digital investigations and to pay attention to the Police Data Act for drafting rules on the process of combining data from multiple investigations.[1222] Scholars such as Galič and Schermer turn to ECtHR jurisprudence on bulk-data collection to show how under national law, such as Dutch criminal procedural law, there might not yet be clear regulation of such powers, especially concerning data analysis that follows after the initial reception, while there is new case law on the European level that can give guidance to national courts on which safeguards to implement.[1223]

Not only is the question which criteria to apply, the question for risk profiling is also who is to apply these criteria and perform a proportionality test. In the EncroChat case it was deemed sufficient that the investigatory judge gave the authorization. For risk profiling there are several authorization scenarios depending on the privacy infringement: there is the public prosecutor, the investigative judge and the trial judge. However, as discussed at multiple points earlier in this chapter, in many instances the deployment of a measure will not be assessed by the trial judge, as not all investigations lead to prosecution let alone to a trial.[1224] I would therefore argue that a strong proportionality test should be conducted on the level of the public prosecutor or the investigatory judge.

6.6.1.3 A legal basis for bulk-data collection?

A related question is what the specific legal basis is for the gathering and analysis of bulk data, more specifically to first gather and analyze large volumes of data and from that analysis distill a reasonable suspicion against specific individuals; instead of the traditional other way around where there is first a suspect and then data about that suspect is gathered and analyzed. In the cases that followed from the EncroChat investigation, there was confusion about the legal basis from all sides: the defense claimed that there was no legal basis for the analysis of the data; the public prosecution argued that there was no specific legal base for the receiving of and searching of data

---

1221 Koops Committee, Regulering van opsporingsbevoegdheden in een digitale omgeving (Commissie modernisering opsporingsonderzoek in het digitale tijdperk), June 2018, p. 15.

1222 Koops Committee, Regulering van opsporingsbevoegdheden in een digitale omgeving (Commissie modernisering opsporingsonderzoek in het digitale tijdperk), June 2018, p. 15.

1223 Galič, M. (2022), 'Bulkbevoegdheden en strafrechtelijk onderzoek: wat de jurisprudentie van het EHRM ons kan leren over de normering van grootschalige data-analyse', *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 8(2), pp. 130-137; Schermer, B. W., & Galič, M. (2022). Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen? *Nederlands Tijdschrift voor Strafrecht*, 3(3), 167-177. [2022/38].https://doi.org/10.5553/NTS/266665532022003003006.

1224 See also: Koops, B. J. (2009). Technology and the crime society: rethinking legal protection. *Law, Innovation and Technology*, 1(1), 93-124

received from the French police, but that none was needed; while ultimately in one of the cases the court ruled that article 126uba CCP contains the legal basis for such bulk gathering and analysis of data through hacking a crypto server.[1225] In another case following from the EncroChat investigation, a different criminal court similarly ruled on article 126uba CCP as the legal basis for collection and analysis of bulk data through police hacking.[1226]

Seeing these two cases in combination a few points can be made. First of all, the courts reason that article 126uba CCP is the applicable legal basis in this type of case. In the context of an investigation into organized crime, article 126uba CCP creates the power for the public prosecutor to hack an automated device (such as a computer or smartphone), after an authorization by the investigative judge, and to investigate the data, such as to determine characteristics of the user of the device, e.g. identity or location, and record these. Another aspect of article 126uba CCP is that this so called hacking competency can also be used to execute a warrant to secretly record telecommunications data (art. 126t CCP) from a suspect of organized crime. According to both courts in the referred to EncroChat cases, this hacking and recording of telecommunications data is what factually happened, even though the French police were the ones to hack the EncroChat server. The fact that the French police performed the hack does, in the court's opinion, not mean that the activities that follow after that hack, the recording and searching of the data, cannot be based on the hacking competency. The reasoning is that article 126uba CCP has allowed more than what the Dutch police have factually accomplished in this case, namely it allows hacking, recording, storing and searching, so article 126uba CCP certainly allows for doing less as well (i.e. not performing the hack but only the other activities).[1227]

Concretely for risk profiling, this means that there is not a specific separate legal basis for the data analysis itself for such scenarios: the power to analyse the data is read into another investigatory power that allows a certain type of collection of data. While exceptional, it is possible for the investigatory judge to make explicit safeguards for the search process in the authorization, as was demonstrated in EncroChat cases. However, the safeguards then can differ on a case per case basis. A lack of specific legal basis for investigatory actions would create a tension with article 1 CCP, which contains the principle of legality and determines that all actions of criminal prosecution, including police powers, have to be foreseen by law. Foreseeability is not

[1225] District Court (criminal law) Amsterdam 17 March 2022, ECLI:NL:RBAMS:2022:1273, para. 3.5.
[1226] District Court (criminal law) Noord-Holland 4 May 2022, ECLI:NL:RBNHO:2022:3899, para. 3.7.
[1227] See for a detailed explanation: District Court (criminal law) Amsterdam 17 March 2022, ECLI:NL:RBAMS:2022:1273, para. 3.5.

merely a criterion of criminal procedural law to ensure for example the presumption of innocence and the right to fair trial; it is a crucial requirement of various fundamental rights. Foreseeability is equally important when it comes to the fundamental rights of privacy and data protection. If police powers pose an infringement to the right to privacy or the right to data protection, there needs to be a foreseeable legal basis. In this way police powers are not just regulated by criminal procedural law but also by other fundamental rights and there is an important interplay between the different frameworks. For this reason, basing police powers on case law and taking a case-by-case approach is not desirable. The EncroChat case law demonstrates this difficulty, as the public prosecutor did not deem it necessary in the first place to request an order from the investigative judge for analysing the data.

6.6.1.4 Oversight on large scale data collection

For cases that do not lead to a trial, because the prosecution of an individual is not taken further, or data is analyzed about an individual but they are not prosecuted at all, there is no safeguard of the trial judge reviewing the broad powers of data collection and analysis. It is therefore paramount to think of innovative ways of oversight and checks and balances that are more attuned to practices of large-scale data analysis.

When taking the Dutch criminal justice system as an example, it can be lauded that there are clear steps being taken to achieve such new checks and balances. One such way is in the internal organizational division of tasks and oversight. For example, in the EncroChat investigation there was a division in technical staff handling the data and staff working on the investigatory team. Such a distribution of tasks can limit the chances of fishing expeditions or function creep occurring. A second step is in creating additional layers of internal and external oversight. This is a development that may be taking place in practice, but it is difficult to get full insight in this from an external perspective. Therefore it is hard to conclude whether sufficient safeguards have been successfully established on this point. For example, in the EncroChat investigation, the exact working of the JIT does not become clear; also in the court cases that followed afterwards, the process and supervision remains opaque to safeguard the evidence and efficiency of future investigations.[1228]

Nonetheless, interesting guiding points can be found in the Dutch policy debate. For example, the Council of State, in its advisory role on legislation regarding powers such as police hacking, has in the past stated that structural system oversight is required on the lawful use of investigatory powers using ICT in cases that have not been assessed

[1228] This opacity is point of discussion in many of the cases, as I will discuss in section 6.6.3.

by a criminal trial judge.[1229] System oversight in this sense refers to a specific type of oversight within governmental actors that uses the idea of self-regulating systems within an organization, where activities of the actor under supervision are aimed at enhancing the quality and legal compliance of their work.[1230] While this refers more to internal oversight, which borders on self-regulation, similar arguments can be made for independent external oversight. In a report from 2022, the Attorney General (*Procureur-Generaal*, PG) to the Dutch Supreme Court, for example, underlined the conclusion that there is a need for more oversight in cases where data analysis is at the core of the investigation.[1231] The PG points out the supervisory tasks of the Inspectorate of Justice and Security and the supervisory tasks of the Dutch Data Protection Authority (DPA) as authorities that might be able to take up part of this role.[1232] At the same time the PG report also pointed out that the competency of the DPA only extends to the processing of personal data and that the system supervision of the Inspectorate of Justice and Security only sees to police activities, excluding the Public Prosecution Service.[1233] The PG suggests that it can offer complementary supervision on the investigatory competencies of the Public Prosecution in limited, themed, trajectories.[1234] While these are all good suggestions and developments, it remains to be seen how these new forms of supervision will be picked up in practice.

1229 Kamerstukken II 2015/16, 34 372, no. 4 (Advies RvS), p. 6-7.

1230 J. Helderman & M.E. Honingh, Systeemtoezicht. Een onderzoek naar de condities en werking van systeemtoezicht in zes sectoren, Den Haag: WODC 2009.

1231 Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available in Dutch: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf, p. 6.

1232 Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available in Dutch: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf, p. 6.

1233 Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available in Dutch: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf, p. 6.

1234 Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available in Dutch: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf, p. 6.

6.6.2 Regulation of risk profiles and the interplay between different legal frameworks: the CCP and Police Data Act

The Police Data Act together with the Judicial Data and Criminal Records Act and Police Data Decree is one framework for police data processing, which is mainly relevant for determining the purpose of the data processing and setting conditions which data can be matched and which data can be accessed by which actors. The other framework for police data processing is the CCP together with the Police Act to regulate the competencies to gather data. Thus, due to the difference in objective, there are two different legal frameworks relevant to the profiling process. Because of the separate frameworks, the challenge is to have an adequate, well-functioning interplay between the two.

One of the challenges for the interplay is how possible violations of legal requirements for the gathering or analysis of the data are treated. Herein lies a problematic aspect: violations of the Police Data Act are not always examined by the judge in a criminal trial. Why this is the case and why this is an issue can be illustrated once again by the case law of the EncroChat investigation. In the trials of individuals following the EncroChat police investigation, one of the points put forward by the defense was that there had been violations of the Police Data Act in the process and that this should be addressed by the court in the context of the right to a fair trial. More specifically, the argument was put forward that the defense could not assess whether the EncroChat data were processed in accordance with the Police Data Act as the files to perform this assessment were not shared with the defense. According to the public prosecutor the defense did not have a relevant interest in having access to these files and stated: "*after all, the Police Data Act cannot be regarded as such a provision under criminal law that a violation thereof constitutes a procedural defect as referred to in art. 359a CCP, let alone to a violation of art. 6 ECHR*".[1235] The court agreed with this reasoning by the public prosecutor: in an earlier assessment, a court had already ruled that the Police Data Act is not an important criminal procedural law regulation,[1236] and for that reason the court ruled that the defense has no interest in the court assessing whether the requirements of the Police Data Act were met. According to the court, such an assessment is not relevant for the questions the court has to answer during the criminal trial, nor for a question whether there is a fair trial under article 6 ECHR.[1237] There could be some misconception on what 'relevant' means in this perspective: it could be interpreted as the court stating that the right to privacy as protected under the Police Data Act is not relevant enough, or a breach thereof not serious enough to perform an assessment.

[1235] District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584, r.o. 2.1; translation by the author.

[1236] See District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584, r.o. 2.1, for more explanation on this.

[1237] District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584, r.o. 2.1.

That is in my opinion not the case: the court is merely pointing towards the separation between the Police Data Act and the CCP.

It is strange that the trial judge does not see it as their task to assess the data analysis; it is an artificial separation to view the collection and analysis of data completely separately. The criminal trial judge only reviews the gathering of the data[1238] but apparently has no competency to assess lawfulness of the subsequent use of those data in the phase of data analysis under data protection law, while in reality the analysis of the data itself has a major impact on the criminal investigation and the prosecution. It is therefore an artificial distinction to see the collection and analysis of data as completely separate activities and to view the analysis of data in the criminal investigation as an activity under data protection law without implications for the law regulating the criminal investigation. If I take the EncroChat case as an example again, the CCP regulates how the communications data and smartphone data can be gathered (through a hack, decryption order after seizure of the phone, etc.). The analysis of the data using Hansken to make connections in the network of the suspect, link search terms together, or create a profile of a suspect or group of suspects, is regulated through the Police Data Act, which determines which data can be compared with which other data and who has access to which data for analysis. Then, afterwards, when the data analysis is used as evidence in the criminal trial, the judge only reviews the competency to gather the data in the first place and the use of the outcome of the analysis as evidence (for example whether the profile created reasonable suspicion so that the individual could be arrested or their house could be searched). The DPA has independent oversight on the analysis phase as it is deemed a piece of data protection regulation. This, however, creates an awkward and fragmented reality, as the collection, analysis and use of data are supervised by different independent authorities. It is also raises the question whether the DPA has sufficient insight into and the means to assess data analysis in every criminal investigation. Some scholars put forward that in practice violations of the Police Data Act hardly receive attention from the Dutch DPA.[1239] The same scholars argue that while in large-scale data collection, such as in the EncroChat cases, where data are collected of all the users of the communication service, it is not self-evident that all these data should be allowed to be used for data analysis in the future for various criminal investigations.[1240]

1238 At the same time, the courts in the EncroChat cases were also limited in their assessment of the data collection as the data originated from a hack performed by the French police, and the principle of trust hinders a full assessment of the actions by the French police.

1239 Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02, p. 89.

1240 Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02, p. 89.

Following the EncroChat case law, such analysis would be possible after permission from the Public Prosecutor.[1241] I think this is too low a threshold, which is problematic in the light of data protection case law such as the data retention case law; as discussed previously in this chapter, one of the prominent points of said case law was exactly the large scale storage of data that also pertains to those not suspected of serious crime.

I would therefore argue that data analysis criteria need to be included in the CCP, if not through official integration in the law, then through integration in police practices implemtenting the CCP. In this manner the data analysis will be included in the assessment of powers conducted by the Public Prosecution Service and investigatory judge and ultimately also by the trial judge, creating one comprehensive framework of legal protection. Not only does this create a better interplay between criminal procedural law and data protection law, it also removes legal uncertainty. In the future, criminal justice actors will more frequently face questions as to how the risk profiling process is regulated, and a compartmentalized legal approach creates the risk that these questions fall through the cracks of legal assessment and legal protection. For example, are errors in risk profiles a question of problems in the criminal investigation or of data protection law? Are they not rather both? If inaccurate data is for example classified as a Police Data Act violation, this would lead to questions what the consequences of that should be for the criminal investigation. Fragmentation in the regulation also leads to legal uncertainty over the competency of the criminal trial judge and of the DPA to take action.

As the CCP regulates investigatory powers, providing a legal basis for the privacy interference they pose, it is important that the CCP follows the case law of the right to privacy to create appropriate safeguards in line with the right to privacy. To create a legal basis for a privacy interference so that the interference is in accordance with the law, three conditions need to be met, following the case law on article 8(2) ECHR: accessibility of the law, foreseeability of the law, and a certain quality of the law.[1242] Other scholars have reviewed this case law extensively, for a summary of the main points I rely on the analysis of Oerlemans and Galič here.[1243] Accessibility of the law refers to the law providing an adequate indication of which rules and procedures apply;

1241 See also Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02, p. 89.

1242 See e.g., ECtHR 4 May 2000, ECLI:CE:ECHR:2000:0504JUD002834195, appl. no. 28341/95, para. 52 (*Rotaru v. Romania*) and ECtHR 1 July 2008, ECLI:CE:ECHR: 2008:0701JUD005824300, appl. no. 58243/00, para. 59 (*Liberty and Others v. the United Kingdom*).

1243 Oerlemans, J-J., & Galič, M. (2021). Cybercrime investigations. In *W. Van der Wagen, J-J. Oerlemans, & M. Weulen Kranenbarg (Eds.), Essentials in cybercrime: A criminological overview for education and practice* (pp. 197-254). Eleven Publishers / Boom Juridische Uitgevers, p. 198-203.

foreseeability of the law refers to clarity in the scope of the competency created and the way in which the investigative measure is exercised in practice; and a certain quality of the law sees to the level of detail of the regulations and the minimum procedural safeguards that must be present.[1244] It is commonly accepted that the more serious the privacy interference is, the higher level of procedural safeguards is required. This aspect I already discussed in section 6.2.3 and is thus an aspect of regulation that is followed in the CCP and Police Act. It is interesting however to briefly revisit this requirement to illustrate the need for more interplay between the CCP and the Police Data Act, or more broadly speaking, between criminal procedural law and fundamental rights of privacy and data protection.

Oerlemans presented this structure of an increase in legal safeguards along the increase in gravity of the privacy interference in a scale figure, as displayed in figure 4.

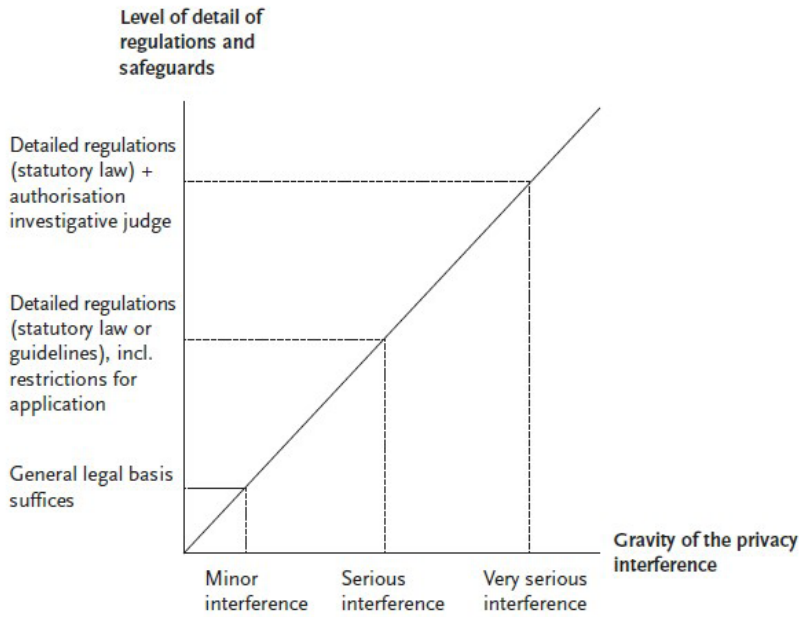

Figure 4. Oerlemans's scale of level of detail of regulations and safeguards and the gravity of the privacy interference.[1245]

[1244] Oerlemans, J-J., & Galič, M. (2021). Cybercrime investigations. In *W. Van der Wagen, J-J. Oerlemans, & M. Weulen Kranenbarg (Eds.), Essentials in cybercrime: A criminological overview for education and practice* (pp. 197-254). Eleven Publishers / Boom Juridische Uitgevers, p. 199 & 200.

[1245] Oerlemans, *Investigating cybercrime* (Dissertation) 2017, ISBN 9789085551096 p. 91.

In the report on the modernization of the CCP, the Koops Committee engages with this figure and propose the idea of systematicness, as explained in section 6.2.3. However, the legal basis in both the figure of Oerlemans and the criterion of systematicness sees to the authorization solely. As I explained in section 6.6.1.3, oversight is indeed an important aspect of data collection and analysis. Nonetheless the requirement of authorization does not in itself create cohesion between the criminal investigation and fundamental rights such as data protection and privacy. The CCP does not in detail regulate how large-scale data should be treated or analyzed; this happens on a case by case basis dependent on the order of a public prosecutor or investigatory judge. That is not very accessible or foreseeable. Nor is the fragmented oversight between the trial judge and DPA a very strong level of supervision as required for such bulk operations.

6.6.3. Regulation of risk profiles and the right to fair trial

The use of risk profiles by law enforcement also raises questions about whether such practices are in line with the right to fair trial. It can be argued that use of algorithmic systems requires a different approach to regulating criminal procedure, because of transparency and understandability of the investigation, to safeguard the equality of arms, even for algorithmic tools that 'only' offer support and do not create risk assessments.[1246] The fundamental right is laid down in article 6 ECHR, which entails that, when faced with a criminal charge, everyone is entitled to 'a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law'. Article 6 ECHR includes a couple of rights that should at the least be granted to the individual in question: the presumption of innocence; the right to be informed of the nature and cause of the accusation against him; the right to have adequate time and facilities for the preparation of his defence; the right to legal assistance; the right to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him; and the right to an interpreter when necessary. Contrary to what the name might suggest, the right to fair trial does not solely mean assessment of compliance with article 6 ECHR of the criminal trial following criminal investigations, the assessment also includes the pre-trial phase of criminal proceedings.[1247]

While for the more traditional, less data-driven, ways of evidence collection, such as witness statements, there exists a large body of case law on article 6 ECHR to detail which requirements flow from the right to fair trial, such detailed requirements

[1246] M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BSb* 2021/2, p. 41.

[1247] See e.g. ECtHR, *Alexandru-Radu Luca v. Romania* 2022, para. 63; European Court of Human Rights, Guide on Article 6 of the European Convention on Human Rights, available at: https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf, p. 7.

do not exist for large scale data analysis as foundational evidence as is used in risk profiling.[1248] For risk profiling the main element of importance is the transparency of the data collection, analysis and use. That is why the right of the defendant to have adequate time and facilities to prepare a defense is so important here. Being able to prepare a defense also entails having the necessary information to do so. This ability is reflected in the concept of equality of arms, which is an inherent feature of any fair trial. The equality of arms requires that each party is given a reasonable opportunity to present their case, under conditions that do not place them at a disadvantage vis-à-vis the opponent.[1249] It is noteworthy here to realize that while the equality of arms demands that information relevant to the case is shared with the defense, in the Dutch system of criminal prosecution it is the public prosecutor who determines which information is relevant and thus made available. The initiative and assessment of what is relevant thus rests on the side of the prosecution.

Returning to the example of risk profiling from EncroChat case law, an issue that became apparent is how opaque the collection, selection and analysis of data points can be to the defense. In order to prepare a proper defence, I would think knowledge is at least required on: the legal basis used to collect data, including the factors substantiating a reasonable suspicion; how data were selected to be used in data analysis, for example which search keywords were selected as part of the risk profile; how the data analysis was conducted, for example how an automated search tool such as Hansken was deployed, or how the outcome of data analysis led to an authorization to use an investigatory power. The defence in the EncroChat cases argued similarly that they needed to be able to assess the legality of the data collection, the validity of the reasonable suspicion and the data analysis that led to the collection of the gathering of further evidence.[1250] Van Toor and Oerlemans analysed the EncroChat case law extensively and put forward that the defence argued in the various cases that they need access to the EncroChat data collected, from a point of view of the right to a fair trial, for three purposes: first, to review the integrity of the data; second, to review the reliability of the data, in particular because all EncroChat messages are sent under

1248 M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BSb* 2021/2, p. 42.

1249 European Court of Human Rights, Guide on Article 6 of the European Convention on Human Rights, available at: https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf, p. 34.

1250 See e.g. District Court Rotterdam 11 October 2021, ECLI:NL:RBROT:2021:9906, para. 6.5.8 and District Court Amsterdam 16 July 2021, ECLI:NL:RBAMS:2021:3707.

pseudonyms; and third, to determine whether any exculpatory evidence can be found in the data.[1251]

The approach the public prosecution chose to take was an interesting one. The defense was offered an opportunity to come to the Netherlands Forensic Institute premises and re-create searches in Hansken to assess the reproducibility of the police queries, in addition to receiving a cd with data.[1252] However, the defence in that case still argued they were not given sufficient time or means to investigate the data used as evidence against the suspect, in particular to be able to construct an alternative scenario to the events as presented by the public prosecution.[1253] A general problem is thus that the automated analysis and decision-making are not always understandable for the defense. Nonetheless, giving access to the system to conduct searches in combination with the requirements posed by the investigatory judge in the authorization for the data collection, form important equality of arms safeguards. A good example of this from the EncroChat cases is the requirement that search terms have to be approved ex-ante by the investigatory judge in combination with giving the defence the opportunity to conduct the same search in the database. Ultimately, the police practices stood the test by the court. This is actually the most clear in a case regarding the take down of Ennetcom, an operation very similar to that of EncroChat. The District Court of Amsterdam ruled there that the results obtained from Hansken were not unreliable, that the procedures had been sufficiently controllable by the defence, and that the use of such tools does not require any additional legal provisions.[1254]

Since the French police originally performed the hack and collected the data and shared those with the Dutch police, the principle of trust applies and impedes a full assessment by Dutch courts of the data collection. However, the principle of trust does not apply to subsequent processing of the data such as analysis.[1255] Thus, the assessment of the compliance with criminal procedural safeguards has been predominantly focused on the authorization by the investigatory judge, as the earliest point of the hacking operation that can be fully assessed by Dutch courts. Therefore

---

1251 Oerlemans, J.J., & van Toor, D.A.G. (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective, *European Journal of Crime, Criminal Law and Criminal Justice*, 30(3-4), p. 321. doi: https://doi.org/10.1163/15718174-bja10037.

1252 See also Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02, p. 87.

1253 See also Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02, p. 87.

1254 District Court Amsterdam, 19 April 2018, ECLI: Netherlands:RBAMS:2018:2504.

1255 Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02, p. 86; District Court Midden-Nederland, 16 September 2021, ECLI:NL:RBMNE:2021:4480, para. 4.1.3.

information about the authorization provided and the process leading up to it has been made public throughout the case law, which is a positive development from a point of view of equality of arms. The EncroChat case law in that way was the driving force in making information about the previously secret operation public, by the myriad of questions posed by the defence on the (sometimes implicit) basis of article 6 ECHR.[1256]

One important aspect to distinguish in risk profiling is between different types of data: there are those data that are originally collected to find patterns and correlations of interest to the police, there are data that point into a certain direction (for example a group or a risk profile of an individual yet to be identified), and then there are data specifically about an identified suspect to be used as evidence later in prosecution and trial. It is important to distinguish between these types of data which narrow in on the suspect, as they start from relatively untargeted and move to evidence in the individual investigation at hand. The question is how the right to a fair trial regulates information provision and data access to these different types: is there from a point of view of article 6 ECHR a difference in which data should be shared with the defence to achieve equality of arms or not? In principle all these data fall within the scope of the right to a fair trial, as the protection of article 6 ECHR also includes all procedures leading up to the trial. At the same time, the public prosecution can make arguments as to why full access to the data would not be possible, for example to safeguard other criminal investigations. This point was also illustrated in the EncroChat cases, where the court had to assess which data was relevant to the defence. Galič provides a partial answer to the question painted above. In her extensive research on access to information under article 6 ECHR case law, she proposes similarly to distinguish between three datasets: the first, full, data set; the secondary data set, which is a result that originates from the first searches done by the prosecution on the full data set; and the tertiary data set, which contains the data deemed relevant by the prosecution from that secondary data set for the investigation at hand. Galič concludes that based on the ECtHR case law, the full data set is of enough relevance to the defence to require at least indirect access such as involvement of the defence in the search terms used on a dataset. The defence should be provided full access to the secondary data set. Both are needed to allow the defence to search for counter evidence, which is crucial to the equality of arms.[1257]

1256 Oerlemans, J.J., & van Toor, D.A.G. (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective, *European Journal of Crime, Criminal Law and Criminal Justice*, 30(3-4), p. 315. doi: https://doi.org/10.1163/15718174-bja10037.

1257 M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BSb* 2021/2, p. 41-49.

Originally, some scholars criticized the availabilities and argued more action is necessary to comply with the equality of arms.[1258] For example, Oerlemans and Schermer recommended a data-room should be set up for the defence[1259], while later the defence was given the opportunity to search in Hansken; and scholars such as Galič point towards ECtHR jurisprudence to argue that the public prosecution should involve the defence in selecting secondary datasets.[1260] I would think that with the current developments in encouraging the defence to conduct research in tools such as Hansken, and perhaps continuing those possibilities more extensively, while combined with strict ex-ante regulation to prevent fishing expeditions, there is already much progress in Dutch criminal procedural law to ensure a fair trial when it comes to the use of risk profiles.

6.7 Conclusion

This chapter first described the Dutch criminal procedural law in relation to risk profiling. The concept of the criminal investigation is a key concept for such legislation and has a broad scope; many police activities for risk profiling can be deemed to be within its scope. As the concept kept expanding over the years, and preventive police actions become more common, it is likely that new forms of risk profiling will also fall within the scope of the criminal investigation. On the one hand, a broad interpretation of the concept of criminal investigation is desirable from the perspective of fundamental rights, as it carries with it important safeguards. On the other hand, the constant expansion of the concept of criminal investigation also brings a risk of legitimizing police powers that are increasingly pre-emptive, posing fundamental rights issues that way.

While the concept of criminal investigation might be broad, not all police activities used for risk profiling are rooted in their own specific legal basis. In the Netherlands, the system of light infringements to the right to privacy emerged as a concept to determine when investigatory powers for the collection of data can be used without a

---

1258 D.N. de Jonge & S.L.J. Janssen, 'Eindelijk toegang tot datasets. (Erg) langzaam maar zeker naar een nieuw normaal', *NJB* 2021, afl. 34, p. 2793-2799.

1259 B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3.

1260 M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BSb* 2021/2, p. 46-47; See for a similair argument: S.G.A.M. Adams, 'Vertrouwen is goed, maar controle is beter. De interpretatie van het interstatelijke vertrouwensbeginsel door Nederlandse feitenrechter bij samenwerking tussen EVRM-lidstaten in het kader van internationale digitale rechtshulp in strafzaken en het beginsel van equality of arms', *DD* 2021/74.

specific legal basis, relying on the competence of the general policing task, or when the infringement is too serious requiring its own specific legal basis with accompanying safeguards. Interestingly, the system of light infringements was developed through case law; during the writing of this dissertation the modernization bill for the CCP was proposed, which will anchored it in a more formal sense in the legislation.

The EncroChat investigations and subsequent case law demonstrate four interesting points when it comes to the regulation of risk profiling. First, operations of risk profiling are initially targeted at suspicious groups or criminal organizations, rather than at individuals. This factor makes it important to regulate proportionality checks and balances and to require substantiation on the selection of the groups for targeting. Second, the analysis of data rapidly increases in importance, especially using automated tools such as Hansken. At the same time there are no specific requirements for data analysis in this regard in the current law, although there is a form of regulation through case law and there will be slightly more attention for this issue under the new upcoming law. Third, in the EncroChat cases a crucial role was played by the investigatory judge to fill in the gaps left by the lack of a specific legal basis for the data collection and for data analysis in this type of bulk-data investigations. This is quite a unique phenomenon and it can be encouraged that such safeguards are further developed in case law and laid down in legislation. Fourth, the EncroChat cases demonstrated the importance of the right to fair trial and how meaningful insights can be provided to the defense in criminal investigations with a strong emphasis on data analysis.

Apart from the risk profiling in EncroChat, I used the example of the OxRec tool to further explain how risk assessment functions in decision-making for probation and sentencing. Here risk profiling seems to be taking, until now at least, a more advisory role in probation reports; there is no full automated decision-making as meant in the standard of data protection law. Nonetheless, rules on instruments such as OxRec are already in place through the niche framework of the probation authorities. To which extent internal guidelines there also govern the data analysis within OxRec is difficult to judge from the outside.

Next to the CCP and legislation regulating the activities of the probation authorities, this chapter also discussed the Police Data Act and the related acts, namely the Judicial Data and Criminal Records Act and the Police Data Decree. These pieces of legislation pertaining to the processing of data in the criminal justice sector focus, most notably, on purpose limitation in that they limit the data collection and use to a specific policing task, as well as containing storage limitations, authorization requirements,

and requirements for data collected for which purpose can be compared with data collected for another purpose. One notable gap, when it concerns the regulation of risk profiling, is that none of these instruments give clarity on the legal status of the profile itself.

While the legal framework discussed in this chapter regulates the investigatory police powers to a certain extent, there emerged also some gaps in the legislation. First of all, when it comes to relatively new policing purposes such as disruption as a policing strategy, the regulation does not seem to take into account such practices. Second, in large scale data collection, especially targeted at risk groups rather than individuals, safeguards are lacking in the CCP itself to limit the scope of the collection, and more prominently, data analysis. Third, there is no specific legal basis in the CCP for many instances of large scale data analysis or the use of automated searches. Fourth, there are gaps in oversight as some parts of the early stage of the criminal investigation are not overseen by a judge, in data analysis falls in-between the cracks of oversight exercised by the trial judge and the DPA.

In the next chapter I will delve further into what these gaps mean exactly for risk profiling and how regulation could be improved.

Chapter 7

Concluding chapter

In this concluding chapter of the dissertation, the key points of the dissertation are presented, the main research question is answered, and recommendations are presented. The chapter is structured along three parts. Section 7.1 focuses on answering the main research question, through briefly reflecting on the main concepts and findings of the dissertation. Section 7.2 combines the insights from the different chapters to analyze the regulation of risk profiling by national law enforcement actors, discussing how the different regulatory frameworks manage to regulate risk profiling from the perspective of protecting fundamental rights of those individuals and groups that are subject to risk profiling, as well as gaps identified in this fundamental rights protection. Section 3 contains the recommendations and reflections on how to move forward from a regulatory point of view to offer more complete fundamental rights protection to individuals and groups subject to law enforcement risk profiling.

7.1 The research question and main contributions of the dissertation

The main research question of this dissertation is:

How does the regulatory framework comprising of European data protection law, European non-discrimination law and Dutch criminal procedural law, regulate risk profiling conducted by national law enforcement actors and to what extent does it provide adequate fundamental rights protection to those subject to the risk profiling?

As explained in the introduction chapter of this dissertation, this research took the perspective and methodology of legal doctrinal analysis of the protection of the fundamental rights of those subjected to risk profiling. In order to answer this question, the research first analysed what risk profiling is and how it is used, in chapter 2; next, in chapter 3, the dissertation discussed which fundamental rights challenges risk profiling raises; and lastly, in chapters 4-6, how each legal field (European data protection law, European non-discrimination law and Dutch national criminal procedural law) regulates risk profiling or to which extent the regulation addresses the challenges of risk profiling from a fundamental rights point of view. The following subsections reflect on each of these three parts of the dissertation.

7.1.1 Defining risk profiling

The overarching topic of this dissertation is risk profiling. To scope that discussion, the research explored the concept of risk profiling as such and in that manner added to the academic discourse as there was no clear description of risk profiling yet. I proposed a working definition of risk profiling based on an assessment of technical literature on profiling, legal literature on profiling, literature on risk (and risk theories), and legal policy documents on profiling and automated decision-making. According to the working definition of this dissertation, risk profiling in criminal justice is: the *categorizing or ranking* of individuals or groups, sometimes *including automated decision making*, *using correlations and probabilities* drawn from combined and/or aggregated data, to *infer information used to evaluate or predict behavior* in relation to the level of risk that is posed to the protection of interests and rights safeguarded by criminal law.

Delineating the concept of risk profiling allowed for the exploration of each of the working definition's components in detail throughout the dissertation and allows for the use of the concept of risk profiling in further research. Using the concept of risk profiling enables the discussion to go beyond the profiling discussions that have already been going on for the past years. While there have been many useful discussions on the concept of risk as such or on a risk-based society,[1261] such discussions are based on varying arguments and aimed at different challenges according to the actors and sector specific factors involved. This dissertation has illustrated that the notion of risk in criminal justice has a distinct meaning; the research demonstrated that there is a unique mix in the combination of taking a risk averse approach to criminal justice and a profiling approach relying on generalizations and groupings. Such an approach focuses on correlations and patterns, using statistical or group data. As a consequence, although the focus on the individual is key to both data protection and criminal procedural law, the proposed approach moves away from notions such as identified (or identifiable) individuals. The level of aggregation and abstraction achieved in risk profiling facilitates the detection of patterns, used towards the aim of short term decision-making as well as long term estimates of behaviour of individuals and groups. It is also an approach that requires large, varied volumes of data. This approach of risk profiling that focuses on trends in behaviour, groupings of behaviour, future behaviour, and on the way in which different personal characteristics and factors combine, based on large scale data, is a practice that differs from traditional approaches to policing and criminal justice, where the emphasis has been traditionally on reactive approaches and on the individual.

[1261] Bernstein, P. L. *Against The Gods - The Remarkable Story of Risk*. New York: John Wiley & Sons Inc., 1996, and, Gellert, R. (2017). *Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk*. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

This dissertation brought the discussions on 'profiling', 'risk' and 'risk profiling' together through the fundamental rights lens, to assess the adequacy of current legal frameworks in regulating risk profiling activities from a fundamental rights protection perspective. At the same time this research is not solely relevant to risk profiling: the research findings are relevant for the broader technological- and societal development of the use of a data- and AI-driven approach in law enforcement. In that sense this research offers an illustration of the fundamental rights challenges of law enforcement's increasingly data-driven approach to offer points for discussion and analysis.

7.1.2 Regulation of risk profiling

An important contribution of the dissertation is the approach of the object of study from three legal frameworks: European data protection legislation, European non-discrimination law, and Dutch criminal procedural law. For the latter the focus was on national law, as the European law leaves it up to the discretion of member states to draft their own legislation for regulating the powers of criminal justice actors. In the regulation of risk profiling conducted by national law enforcement actors, these three legal fields play an equally important yet fundamentally different role. In approaching the regulatory analysis from three different perspectives, the research was able to draw conclusions about the requirements and safeguards from each of the three fields in detail, while also seeing the complete picture of how different legal fields can interact or leave gaps in fundamental rights protection. On the one hand, focusing on multiple legal frameworks in one dissertation makes it difficult to achieve the same level of detail as when focusing on only one legal framework. On the other hand, this limitation is outweighed by the merit of this approach, as there is no work of research yet that approaches the regulation of profiling from data protection law, non-discrimination law, and criminal procedural law, at the same time.

While there is scholarship on profiling and each of the three fields of law discussed in this dissertation individually, and some scholarship on data protection law together with non-discrimination law or data protection law together with criminal procedural law, those combined perspectives remain few and there is no scholarship looking at profiling or other large-scale data collection in criminal justice from all three fields of law combined. Issues of profiling have long been a data protection debate, creating the risk that we only look through that lens and make data protection the catch all legislation for all problematic aspects of profiling. Algorithmic profiling gains more attention in non-discrimination law, but it is still a relatively new field. The criminal procedural law perspective on automated analysis and data comparison is also a relatively new discussion. Not only is alignment in application of the legal frameworks important, also in legal research there needs to be more emphasis on research that

transcends a legal field to offer meaningful reflections on current profiling and future AI developments in the area of criminal justice.

European data protection legislation (both on the EU and CoE level) has been a prominent field of law for the regulation of profiling for years, with provisions on automated decision-making and profiling and even specific rules for profiling in the law enforcement sector under the LED. Data protection law applies to all processing of personal data, and thus to risk profiling where personal data are involved. Data protection law regulates profiling mostly through the data protection principles, of which fairness, data minimization and purpose limitation are the most relevant for profiling, as well as through provisions on automated decision-making and profiling. However, while specifically regulating the activity of profiling, it does so from the perspective of the fundamental right to data protection, which comes with its limitations and gaps, most notably in its relation to identifiable and identified individuals as well as its focus on regulating data collection and profile application. Undoubtedly, issues arise from the actual focus on personal data, while profiling also relies to a large extent on non-personal data; personal data is strongly related to the individual while profiling places importance on groups. It can also be argued that while data protection law applies to collection, analysis and use of the data in profiling, in practice there might be overemphasis on regulation of data collection and the regulation of data analysis could be improved.[1262] Despite these limitations, the thesis focuses on the rules relating to the processing of personal data and in particular the ones of special relevance to profiling, as still a large part of data used in profiling will qualify as personal data and many risk profiles in the law enforcement context will be applied to individuals.

Non-discrimination law is focused on only one aspect of the profiling process, namely the application of the profile, meaning the differential treatment of those subjected to the application of a risk profile. While the case law from the CJEU and ECtHR in this domain is often not concerning risk profiling or other forms of data-driven profiling, it has increasingly over the years developed concepts and benchmarks that can be applied to law enforcement risk profiling. For example, the idea of discrimination by association could be applied in the case law of the courts to profiling and the interpretation given by the ECtHR to the criterium of the objective justification can be used to require law enforcement to provide some transparency of risk profiling deemed unlawfully discriminatory by those subjected to it.[1263] At the same time, the field of non-discrimination law sometimes also falls short in adequately protecting against

[1262] See sections 7.2.1 and 7.2.2.

[1263] See chapter 5, sections 5.4.2.3 and 5.4.4 respectively.

the fundamental rights risks of profiling, most notably when profiling concerns new, unforeseen, or opaque, groupings. The case law from the CJEU and ECtHR shows willingness to be flexible with the protected grounds laid down in articles 21 CFREU and 14 ECHR by interpreting the existing numeration of grounds in a non-exhaustive manner. Nonetheless, the approach of requiring an explanation of which ground would be at stake still possibly complicates those subjected to risk profiling from seeking an effective remedy. The CJEU and ECtHR still have some way to go in assessing complicated cases of intersectionality when risk profiles are the result of a myriad of data points pointing to different possible protected grounds, combined with opacity hindering an assessment of whether there could be unlawful discrimination before reaching the step of substantiating an objective justification.[1264]

Lastly, criminal procedural law is the legal framework specifically attuned to the unique characteristics of the law enforcement sector, with its most prominent requirements being the opacity of police practices due to security reasons or reasons of safeguarding the criminal investigation, a strong power imbalance between the different actors (individual suspects vs. police or public prosecution), and a possible broad competence to gather and use data based on national legislation providing exceptions to, for example, data protection rights or privacy safeguards. At the same time the criminal procedural legal framework is a multi-faceted, complicated legal domain. First of all, it is regulated on the national level instead of European level, requiring an assessment of national law and its exemptions to laws such as the LED in the data protection domain. Second, at least in the Netherlands, the national jurisdiction analyzed in this research, criminal procedural law has multiple functions. On the one hand, criminal procedural law safeguards fundamental rights pertaining to criminal investigations and trials, such as the presumption of innocence and the right to fair trial; on the other hand, it is an instrument of legitimizing and restricting police powers to gather data. At the same time it is a field of law containing specific provisions stemming from EU data protection law, the Dutch Police Data Act and the Dutch Judicial Data and Criminal Records Act on the authorization to store, access, and analyze data. And lastly, it simultaneously also regulates the right to privacy, as every investigatory power used by police contains a balance in itself between the right to privacy and the importance of the societal interest of the criminal investigation. In addition, chapter 6 of this dissertation showed that specific pieces of legislation outside of the Code of Criminal Procedure, such as laws regulating the probation authorities, are of relevance as well when it comes to a risk profiling tool such as OxRec. Thus, criminal procedural law regulates risk profiling from different angles and takes into account different interests. Perhaps unsurprisingly for such a multifaceted legal domain, this research

[1264] See chapter 5, section 5.4.2.1.

has shown several gaps in adequate fundamental rights protection. First of all, when it comes to relatively new policing purposes such as disruption as a policing strategy, the regulation does not seem to take into account such practices. Second, in large scale data collection, especially targeted at risk groups rather than individuals, safeguards are lacking in the CCP itself to limit the scope of the collection, and more prominently, to regulate data analysis. Third, there is no specific legal basis in the CCP for many instances of large scale data analysis or the use of automated searches. Fourth, there are gaps in oversight as some parts of the early stage of the criminal investigation are not overseen by a judge, and data analysis seems to fall in-between oversight exercised by the judge and the DPA.

7.1.3 Examples of risk profiling

An analysis of legislation from a solely scholarly or theoretical point of view does not present a comprehensive overview of the adequacy of regulation; a view of practices completes the picture. In this dissertation several examples of risk profiling from practice were used to illustrate the uses and challenges of risk profiling in different stages of the criminal justice chain and for different policing purposes.

The example of CAS was introduced along with the example of PredPol software to show risk based policing that is targeted at locations, while the example of the Chicago SSL heatlist showed a form of risk based predictive policing targeted at individuals. The example of SyRI illustrated how risk profiles are deployed to detect which individuals are at high risk of committing fraud and how in that way risk profiles can be the starting point for a criminal investigation. The EncroChat investigations were used as an example of the role of large scale, untargeted, data-collection and automated data analysis to find suspects. The example of COMPAS from the USA shows how risk profiles can be used in assisting in and influencing of criminal justice decisions such as parole or prison sentencing. And lastly, OxRec was used as an example similar to COMPAS to explain the use of risk profiles in probation decisions for a European jurisdiction.

The example used in this research demonstrated different difficulties in the use of risk profiling. Hotspot policing tools such as CAS and PredPol receive criticism from scientists for their use of biased data and dangers of creating self-fulfilling prophecies and wrong feedback loops, which have their impacts on the right to non-discrimination and can exacerbate stigmatization of socially disadvantaged groups. The SyRI program received a lot of negative press attention and the legislation providing the basis for its use was struck down by the Dutch District Court of The Hague. SyRI was a problematic program from a fundamental rights perspective, mainly because of its problems with proportionality (in terms of the right to privacy) and opacity. The EncroChat

investigations conducted by the Dutch police were scrutinized by several Dutch courts and, in contrast to the use of SyRI, stood the fundamental rights test. Nonetheless, the discussions between the defense teams of suspects subjected to risk profiling in EncroChat investigations and the public prosecution on the legitimacy of the data collection and analysis, together with the reflections from the investigative judges from the warrants, and the considerations by the courts showed serious concerns over the legitimacy and proportionality of large scale data collection, over the legal basis that could be specific enough to cover such a privacy infringement, over the right to fair trial when it comes to automated data analysis and comparison and opacity of such systems. Both COMPAS and OxRec illustrated challenges of bias and discrimination in using historic police data and group profiles together with systems trained on biased data containing over-representation of data of vulnerable minorities, and the risks of automation bias.

The use of these illustrations demonstrated that the use of risk profiling has an impact on multiple fundamental rights, most prominently on the rights to data protection and privacy, the right to non-discrimination and the right to fair trial. Simultaneously, the issues with the examples from practice demonstrated that risk profiling is a current societal challenge that remains unsolved. This is most notably clear in the ruling of the Dutch District Court of The Hague on the unlawfulness of the legal basis for SyRI over privacy concerns, the fair trial concerns raised about COMPAS in the *Loomis v. Winsconsin* case and the concerns to safeguarding the rights to privacy and fair trial raised in the EncroChat court cases. Over the course of writing this dissertation, on multiple occasions, the Dutch Tax Authority was the object of journalistic inquiries and investigation by the Dutch DPA for problematic and at times unlawful aspects of risk profiling of citizens, related to criteria of nationality. Although the Tax Authority is predominantly not a law enforcement institution, this situation highlights the complexity of risk profiling systems and balancing the efficiency that these systems aim at with interests protected by fundamental rights. All these examples demonstrate that in practice risk profiling creates risks of violations of fundamental rights, raising questions about the adequacy or clarity of underlying legislation. The examples underpinned the choice for the legal frameworks that were analysed in this dissertation and were used throughout to illustrate the regulation of risk profiling.

7.1.4 Challenges of risk profiling

Chapter 3 of this dissertation examined the challenges raised by law enforcement risk profiling in-depth while also creating a categorization of challenges. The categories followed along the steps of the risk profiling process, ranging from challenges in principles that underly systems and connect to the design of systems, to the step of

input of data, to the step of data analysis, to ultimately the application phase. This categorization along different stages of the risk profiling process follows the division into the stages of data collection, data analysis and use of data, as proposed in earlier research by the author[1265], but adds as a 'pre-stage' that of the overarching principles and system design in which the data will later be fed. Within those chronological steps following the profiling process, the categories of challenges that I formed flowed from the challenges as described in the practical examples of risk profiling as well as from the literature studies on profiling and data-driven policing. The categories derived from both the examples and the literature were as following: fairness, bias, probabilistic systems, opacity, discrimination, privacy, and lastly due process. This conceptualization of the challenges was used later in the dissertation to assess the adequacy of the protection of the legal frameworks, but also offers a theoretical framework for other scholars to discuss fundamental rights challenges of systems of risk profiling, or of very similar data-driven or AI-driven systems.

Here, these challenges as identified in chapter 3, are re-visited to summarize how the legal frameworks of data protection law, non-discrimination law, and criminal procedural law, as analyzed in this dissertation, relate to the different challenges of risk profiling. First, each of the three legal frameworks is discussed in their relation to the challenges in section 7.1.4.1. Second, in section 7.1.4.2, conclusions are drawn about how these challenges are reflected in legislation on the whole, viewing the three legal frameworks together, focusing in particular on the different phases of risk profiling.

7.1.4.1 How the challenges of risk profiling relate to data protection law, non-discrimination law, and criminal procedural law

Starting off with data protection law, it can be concluded data protection law regulates multiple challenges. The data protection legislation aims to address issues of fairness in different ways. One way is through the general objective of data protection law; Bygrave and Tzanou for example argue that the objective of data protection legislation is to ensure fairness in the processing of data and to some extent in the outcomes of the processing.[1266] In addition, fairness is safeguarded through the main principles found in data protection legislation, whether it concerns CoE or EU legislation, such

---

[1265] van der Sloot, B., & van Schendel, S. Tien voorstellen voor aanpassingen aan het Nederlands procesrecht in het licht van Big Data. *Computerrecht*, 2020(1), 4-13; van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302.

[1266] See section 4.1; L.A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International: The Hague/London/New York 2002) 2; M. Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

as purpose limitation, data quality, data security, transparency of processing and accountability.[1267] Lastly, the provisions on profiling and automated decision-making can be viewed as fairness requirements in themselves. Data protection law connects fairness to transparency, by requiring the provision of information about profiling and automated decision-making from a point of view that profiling can only be fair if enough information is provided about the processing. There is a tension with fairness because the criminal investigation is by nature such an opaque process. At the same time there is a limitation in achieving fairness in that fair processing not only requires transparency, but for profiling also has implications for the data analysis, such as which characteristics it is fair to base categorization on. The latter says something about the treatment of people and which characteristics such treatment should or should not be based on. This is a question that it is more suited to be regulated through non-discrimination law rather than data protection law. Data protection law does not contain provisions specific for bias, but bias can be seen as being regulated through the principles of fair personal data processing and accurate personal data processing combined. Data protection law does not contain provisions specific to probabilistic systems, the only way this aspect is reflected is through the principle of accuracy. Although the CoE Profiling Recommendation and LED talk about distinguishing between facts and personal assessment, they leave unclear the position of correlations and categorizations within profiling. According to the principle of accuracy inaccurate factual information should be corrected, but information in profiles might be factual in each individual data point but still paint a distorted picture. There is a difference between factuality and relevance, meaning that some correlations might be factually correct but not relevant or causal, leading to risks of wrong categorization or wrong decisions. Data protection law assumes a simplified version of reality, as it does not acknowledge such differences nor does it have provisions on profiling, categorization, or predictive analytics. There is a gap here in data protection law in regulating profiling challenges related to probabilities. When it comes to privacy challenges of profiling, data protection law regulates the informational privacy aspects, in particular by limiting the collection of personal data by requiring a specific purpose and processing ground for each processing activity. However, at the same time this protection is limited to the informational privacy of identifiable individuals and, apart from the purpose, says little about the use of such data. Due process is regulated when it concerns violations of data protection norms, such as the data protection principles or article 11 LED, as individuals can lodge a complaint with a supervisory authority, have an effective judicial remedy against a binding decision by a supervisory authority, and have an effective judicial remedy against a controller or processor.

[1267] M. Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

Non-discrimination law regulates issues relating to fairness, opacity, discrimination and due process. Fairness and discrimination are closely related in this context. Non-discrimination law aims for a fair treatment, which is to not be discriminated against based on protected characteristics, ensuring an equal treatment for equal cases. Non-discrimination law requires a treatment or action, mere bias is thus not necessarily regulated by non-discrimination law if it is not followed by any action, such as a decision, application of a profile or designing a policy or law. In that sense there is an important role for data protection legislation to counter bias. Non-discrimination law can be seen as regulating transparency aspects of profiling as well: as risk profiling relies on group data and statistical data for categorization, law enforcement actors will have to demonstrate an objective justification for indirect discrimination, requiring that they submit data proving such an objective reason. At the same time one can wonder to what extent such an objectifiable approach aligns with fairness in a broader perspective, seeing fairness as more than just non-discriminatory treatment: that a policy or decision is rooted in facts or data does not mean it is a decision considered to be based on fair factors. Due process for risk profiling by Dutch law enforcement authorities is offered through oversight by the Netherlands Institute for Human Rights and established complaint mechanisms, as well as the possibility to launch complaints before the ECtHR against the state after exhausting national remedies.

Criminal procedural law mainly concerns itself with the challenge of privacy and the challenge of due process. Privacy challenges are regulated in the balancing between creating competencies for data collection by the police and providing a legal basis for an interference to the right to privacy of the individual whose data are collected. Due process is regulated through the right to a fair trial and related safeguards on the level of national law. This due process, however, is limited to the scope of the criminal trial.

7.1.4.2 The challenges of risk profiling along the phases of risk profiling

In drawing conclusions in chapter 3[1268], the hypothesis was presented that the challenges with risk profiling originate predominantly early on in the profiling process. In the chapters following, I did not find counter evidence to suggest that the hypothesis was erroneous. Some challenges such as discrimination, may only become apparent when profiles are applied to individuals or groups, but that does not entail that the issues originate at that point in time. I refer to this point to raise two arguments. First, many challenges that risk profiling creates will originate early in the process of risk profiling, namely while the data are being collected or the system is designed (such as programming the AI). At the same time, data protection law and criminal procedural law, do regulate the early parts of the risk profiling, for example in limiting the data

[1268] See chapter 3, section 3.9.

collection and scoping the data collection to a specific purpose. This is thus a positive aspect of the regulatory approach in addressing issues of risk profiling. However, secondly, still examples persist of negative effects of risk profiling, as demonstrated in examples such as COMPAS or SyRI, and examples of uncertainty, such as illustrated in the EncroChat case law. These illustrations raise the question whether the regulatory framework is then truly successful in regulating the challenges originating from system design and data collection. More specifically put, it is questionable whether the law sufficiently mitigates these challenges.

7.2 The issues in current legal protection

It can be concluded that risk profiling is perhaps not a technological process or practice regulated as such. Rather risk profiling illustrates the problems the fundamental rights framework has to address when it comes to several aspects of current and future law enforcement practices, such as: the use of AI; a data-driven or data-centered way of working; categorizing, labeling and ranking of individuals and groups; bulk data collection; automated analysis and correlation recognition; and working with information inference or profiles as digital images of a more complicated reality. Because technological change happens so fast, it is not surprising that specific practices such as risk profiling are not regulated as such. However, states claiming a pioneer role in the development of new technologies bear a special responsibility for striking the right balance between the use of modern scientific techniques in the criminal justice system and important private-life interests.[1269] Therefore, it can be argued that it is crucial to ensure a high level of fundamental rights protection, as the consequences of criminal investigation and prosecution for individuals are significant, as well as the societal impacts of policing strategies.

Turning towards the Dutch context, it is clear that the Dutch legislator has not kept up with regulating AI developments, looking at the piecemeal regulation of digital investigation methods and lack of specific regulation on digital sentencing tools. This lack of regulation leads to gaps in fundamental rights protection, fragmented regulation, or legal uncertainty in ad hoc regulation through case law. Throughout the period in which research was conducted for this dissertation, the Dutch legislator has made crucial progress in creating a more comprehensive framework for regulation of digital investigation methods through the modernization of the CCP: the Modernization bill aims to create a more comprehensive regulation to replace the piecemeal regulation of digital investigation methods and will introduce ways

[1269] *S. and Marper v. the United Kingdom* (Applications nos. 30562/04 and 30566/04), para 112.

to integrate checks and balances for expected privacy intrusions for some powers. This is a step in the right direction from a point of view of minimizing fragmentation and legal uncertainty. Unfortunately, this is still a draft bill and the process will take some years before the new legislation comes into force. Keeping in mind the examples of risk profiling from the USA, discussed in chapter 2, we can expect challenges comparable to those in the USA to become increasingly prominent in the EU as well, as the technology for data analysis progresses. Profiling already posed problems to the regulatory framework from a perspective of protecting fundamental rights, as portrayed in profiling discussions on the right to privacy and data protection from the early 2000s and 2010s, but many of these problems have remained unresolved and have only become more complex as the technology and data landscape increase in complexity.

A lot of challenges discussed in this dissertation are not necessarily unique to risk profiling, but are challenges that we are faced with increasingly with any kind of automation or use of AI. For example, fairness and opacity of scoring, opacity of machine learning, the fairness or unfairness of non-distributive group profiling, or including group factors in individual decision-making are difficult issues that expand beyond risk profiling. Risk profiling is a practice that involves many issues combined, and especially in the law enforcement context, which is marked by opacity and with serious consequences for unfairness, constitutes a practice that deserves attention in academic research and attention from regulators. Critically exploring the regulation of risk profiling allows addressing these broader issues. For example, under data protection law there are crucial safeguards when it comes to profiling such as fairness and transparency. There is a mutual relation between fairness and transparency which becomes unbalanced if not enough transparency can be provided, for example to evaluate if there was differential treatment. The problem is that whether enough information is provided to data subjects, to exercise data subject rights and to assess whether there is a possible violation of their fundamental rights, is a complex question to answer which depends on the specific implementation of the LED in the law of Member States as well as the way information is provided in practice.[1270] Another example is the use of groupings and group profiles in the law enforcement domain, such as in risk based sentencing tools, which are applied to individuals without always taking note of the group dimension. Thus, there is a need for a regulatory framework that tackles the problems specific to risk profiling in the law enforcement sector.

[1270] See the elaborate study of Vogiatzoglou et al., which describes through empirical research the complexities of exercising the right of access under the LED: P. Vogiatzoglou; K. Quezada Tavarez; S. Fantin; P. Dewitte, "From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 11, no. 3 (2020): pp. 274- 302.

Below, the main findings of the research are presented, in the form of a discussion of the most problematic aspects of risk profiling vis-à-vis the current regulatory framework of fundamental rights as analyzed in this dissertation.

7.2.1 Conflicts in the legal framework in regulating data analysis in profiling

As mentioned already in section 7.1.2, one of the ways in which the regulatory framework struggles to fully regulate risk profiling is centered in the analysis that takes place in risk profiling processes. This problem is twofold: risk profiling relies for an important part on non-personal data; and the analysis stage is an opaque and complicated part of the risk profiling process, meaning that while data protection in theory applies to analysis as a processing activity as well, in reality the legislation is difficult to apply to data analysis in practice.

Data protection law is only applicable to the processing of personal data; other data being processed in the context of profiling such as statistical data, anonymous data and aggregated data fall outside of the scope of this field of law. At the same time, the latter types of data are increasingly prominent in profiling and increasingly difficult to distinguish from personal data. The focus of data protection law on identifiability makes sense when the majority of data processing concerns either individual specific data collection, or statistical data analysis (for example for the development of tools and models or for national government policies).[1271] But for profiling which is a mixture of these two types of processing, a distinction between personal and non-personal data becomes more complicated for two main reasons. First, it is increasingly easy to infer specific information about identifiable individuals from aggregated data, statistical data or anonymous data, especially when combining datasets through evolving technological capacities, or to re-identify individuals in anonymous data.[1272] As a consequence different types of data become more fluid, blurring the boundaries between personal and non-personal data, raising questions on the scope of data protection law when it comes to regulating a practice such as profiling.[1273] Second, data collection has moved from focusing on individual data to focussing on aggregated data,

---

[1271] van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT, p. 110. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y.

[1272] See for example: European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide (2018). doi:10.2811/73473.

[1273] For more on this discussion see: van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y.

group profiles, and patterns, which can even be used for decisions that affect people as part of a group or category.[1274] On the one hand it can be argued that the importance of data traditionally considered non-personal thus increases, creating the necessity for other legal frameworks to regulate some aspects of collection, analysis and use of such data. The use of such types of data can allow people to be profiled in actionable ways without being personally or individually identified.[1275] On the other hand it can also be argued that this means that the scope of data protection law just expands, as data in which can individuals cannot be identified as such, but are still *applied to* individuals then falls under the data protection framework.[1276] The remaining question is what the status is of data that are not personal and are arguably not applied to individuals, but for example to groups. Apart from profiles focusing on areas, such as hotspot policing, there do not seem to be clear examples yet of where risk profiles in the law enforcement context are used without being related to individuals.

The data protection legal framework strongly regulates the collection of data, which precedes the construction of profiles in the profiling process, and contains specific provisions on profiling and automated decision-making that are focused on the application of profiles as well as the purpose limitation which prevents issues in re-use

1274 These conclusions follow from the entire report: 'van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y', but in particular p.110.

1275 See for example: Strandburg, K. (2014). Monitoring, datafication and consent: legal approaches to privacy in the big data context. In: *Lane, J., Stodden, V., Bender, S., Nissenbaum, H. (Eds.). (2014). Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge University Press; Barocas, S., Nissenbaum, H. (2014) Big data's end run around anonymity and consent. In: *Lane, J., Stodden, V., Bender, S., Nissenbaum, H. (Eds.). (2014) Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge University Press; van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT, p. 110. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y.

1276 van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT, p. 110. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y.

of personal data.[1277] As data protection law regulates all processing activities pertaining to personal data, it also regulates the steps of the profiling process in-between the data collection and application of profiles, being the data analysis. However, the data analysis does not seem to receive enough attention under data protection law in the form of provisions that would be explicitly about the analysis. Data protection law sets conditions and safeguards to control power over data, as it says something about the conditions under which data can be gathered or under which conditions profiling is allowed. In addition, the data protection principles, such as purpose limitation and data minimization, can be effective in scoping the collection of data and shape the analysis of data that way. Nonetheless, the provisions are more suited to steer the collection and use of data and do not for example specifically determine which tools can be used in analysis, nor steer the process of inferring data explicitly, nor determine which statistical methods can be used, nor determine how data mining or AI can be used. As there is increasingly more data collected over the years, the regulation of data collection is put under strain.[1278] This raises questions as to how effective the regulation of data collection is for practices such as profiling, which is a process relying on large scale data and also non-personal data.

7.2.2 The role of groups in profiling

One major gap in the fundamental rights protection analyzed in this dissertation concerns the role of groups in risk profiling. Groups play a role in risk profiling on several levels. First of all, there are groups formed by categorization. Those groups can correlate to characteristics that people are traditionally used to being grouped by, for example age, but there can also be new unexpected groupings that people are unaware

---

1277 van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT, p. 28. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y. For a similar argument of data protection law focusing on data collection through the core principle of data minimization, see: Hoboken, J. van (2016) 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and U.S. Frameworks for Personal Data Processing', pp. 231-259 in: *B. van der Sloot, D. Broeders and E. Schrijvers (eds.) Exploring the Boundaries of Big Data*, WRR-Verkenning 32, Amsterdam: Amsterdam University Press, p. 234. For a criticism on the effectiveness of the regulation of data collection, see: E.J. Koops, The trouble with European data protection law, *International Data Privacy Law*, Volume 4, Issue 4, November 2014, available at: https://doi.org/10.1093/idpl/ipu023, p. 253.

1278 van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT, p. 16-17. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y; Bert-Jaap Koops, The trouble with European data protection law, *International Data Privacy Law*, Volume 4, Issue 4, November 2014, available at: https://doi.org/10.1093/idpl/ipu023, p. 253.

of or are not sure about the consequences of that grouping; examples of the latter could be grouping people by the color of the car that they drive, grouping people who drink plant based milk, or in the criminal justice sector, grouping people who are friends with person x or who rent holiday homes in winter. Of course these are very simplified examples, but the idea is that people will not understand why such a factor would be the classification factor for a group they are in or what the consequence is of that grouping. Because these can be unexpected new groupings, it is usually not clear what the impact of the classification would be or what the interest is of the group that needs legal protection. The use of profiles also means that information about categories or groups becomes the most prominent data, sometimes more so than personal data of an individual, allowing for predictions and decisions at a group level while the legislation focuses on the individual level.[1279] The merit of the use of profiles is not so much the identification of characteristics of individuals but rather the comparison with other individuals in the dataset.[1280] For example, the knowledge of interest is what makes one individual more likely to commit a certain type of crime compared to another, more so than identifying the individual characteristics of a person. I would argue that while in practice it is still difficult to find examples of law enforcement decisions or law enforcement policy that solely pertain to the group level or rather cause harm by pertaining to the group level, that does not mean the point of treating individuals based on the group they are algorithmically placed in, rather than on their individual merit or in reference to their individual characteristics, does not create a tension with the idea behind fundamental rights of treating individuals based on their own merits or flaws.[1281]

A second way in which groupings play a role in risk profiles is in the use of group data for the creation of a profile, while the application of the profile concerns an individual. The data protection framework focuses on the individual application (and data collection) but leaves the analysis phase where groupings are created either out of scope, when those data are non-personal, or up to the general data protection principles; there are no specific provisions on the role or influence of group data in later use pertaining to individuals. This is most clearly observed in article 11 LED and article 22 GDPR on automated decision-making including profiling, which only concern individual decision-making as the result of such profiling.

1279 Mittelstadt, B. From Individual to Group Privacy in Big Data Analytics. *Philos. Technol.* 30, 475–494 (2017). https://doi.org/10.1007/s13347-017-0253-7, p. 476.

1280 Edwards and Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1, p. 35-36.

1281 See also chapter 5, section 5.4.1.

The different distinctions made in the profiling process further illustrate this point, as described in chapter 2.[1282] The application of profiles is often indirect; for example, risk profiles in programs such as COMPAS or OxRec are very reliant on group data. There are no provisions found in either data protection legislation or legislation in the criminal justice sector regulating such tools that take specific account of this fact; for example, data protection legislation assumes data processing about an individual relies on data concerning that individual, while decision-making might also include data not about the individual in question. There seems to be a legal fiction in data protection legislation, such as the LED and the GDPR, that data applied to a certain individual are data originally pertaining to that data subject, while that is not always the case: for example, instruments such as the LED and GDPR grant rights to data subjects to leverage control over their data and decrease the power asymmetry over data between data controller and data subject; while at the same time this only gives the data subject little influence over the profiling process, as the creation of categories and the placement of an individual in a specific category is dependent on a myriad of factors beyond the personal data of that specific data subject. It can be argued that the application of a profile to an individual gives the data subjects' rights concerning the outcome of the data analysis, namely the profile and the application of the profile to them. Data protection law applies to all processing activities pertaining to personal data, so also to analysis, but at the same time does not contain explicit provisions about activities of analysis, such as categorization. A similar problem is present in non-discrimination law, where on the one hand the goal of non-discrimination law is to show the difference in treatment between individuals based on group characteristics, but on the other hand the legal framework does not seem to accommodate that with risk profiling not all the data is known to the people in question. It can be difficult to prove discrimination by law enforcement, which requires statistical data individuals might not have access to. At the same time individuals might not be aware they are in a certain group or what the meaning of the categorization is. As explained in chapter 5, in the case law of the ECtHR it is demonstrated that the court is willing to accommodate individuals when it comes to opacity or lack of access in working with hypotheses or assumptions that states have to disprove. Nonetheless the new categorizations that come from algorithmic profiling challenge existing non-discrimination law.

It can be concluded that all three of the regulatory frameworks researched (European data protection law, European non-discrimination law and Dutch criminal procedural law), seem to grapple with the group dimension of profiling with three common threads, as explained above: no specific regulation of (new and unclear) classifications,

---

[1282] See chapter 2, section 2.3.4.

no regulation of group data, and no recourse for individuals when it concerns issues that do not have clear individual harm nor recourse for groups.

Traditionally the fundamental rights framework is very much focused on individuals, especially the fundamental rights of data protection and privacy and criminal procedural rights. The safeguards for profiling are linked to individual decision-making[1283] and criminal procedural rights apply solely to the individual level as well. Non-discrimination law handles the protection of groups better, since in its essence it is about comparing people or treating people based on a (shared) characteristic. At the same time, non-discrimination law grapples with decisions based on new classifications, which do not correspond to the protected characteristics enumerated under non-discrimination law such as nationality or gender; for example, algorithms might classify people according to the neigbourhood they live in, according to their social connections, or a combination of various seemingly fragmented factors such as someone's profession, their age, their social media profile and which languages they speak.

The profiling aspects that are further removed from individual decision-making or application remain underregulated either because the legal framework has issues quantifying and qualifying the harm, or because the legal framework does not take into account any effects that go beyond the individual interest in the application of a profile to that specific individual. Both leave open issues of structural bias or errors in profiles on the level of the categorization itself and leave marginalized groups open to new or exacerbated discrimination or stigmatization.

7.2.3 Lack of connection and alignment of regulatory frameworks

The three legal frameworks together suffer from issues of insufficient connection and alignment. The benefit of having separate frameworks is that each one can offer the necessary specialization and can more easily be adapted than a holistic framework. However, this regulation strategy only offers comprehensive fundamental rights protection if the different frameworks align, leaving no gaps. There are a few illustrations apparent from this dissertation where gaps arise. This problem of lack of connection was most obviously demonstrated in chapter 6, for example in the case of the EncroChat investigations. The criminal trial court is hesitant to include fundamental right interests such as privacy, data protection and non-discrimination in its assessment of the concrete case at hand. Rather the courts focus on the legality of police practices from criminal procedural rules, such as authorization for evidence collection or storing of evidence, from the perspective of the criminal procedural code

[1283] See chapter 4, section 4.3.3.

and article 6 ECHR, not testing the data protection requirements from the Dutch Police Data Act. In the laws themselves there is also no clear alignment of different frameworks, such as criminal procedural law and data protection law. In addition, in practice, the Dutch CCP and Dutch Police Data Act are viewed as different fields of law, connections between the two normative frameworks when it comes to data and profiling are missing.[1284] Ultimately this means that the legal framework struggles to offer safeguards at all points where it is necessary for large-scale data collection and analysis. The lack of alignment creates a risk that there is no attention or scrutiny for the risk process as a whole, which has consequences for the oversight.[1285] In addition there is no coherent approach to how profiles themselves should be viewed, in terms of data processing under the Police Data Act for example, where neither data protection law or criminal procedural law provides a clear answer. Another example is the focus on early stages of the criminal investigation when it comes to data collection activities, while procedural safeguards might be placed later in the criminal investigation process or assessment by a trial judge is not present for all data processing; better alignment between data protection law and criminal procedural law could for example be viewed in terms of criminal procedural law being more attuned in terms of safeguards to where in the criminal investigation the important data processing is taking place.

7.2.4 Fragmented oversight

Similar to the challenge of fragmentation in the regulation, there is a fragmentation in the oversight on national law enforcement actors when it comes to risk profiling. The oversight here works on three different levels: there is internal oversight, for example in rules and guidelines within the Public Prosecution Authority and semi-internal through the use of investigatory judges; there is oversight within the criminal justice sector but outside of the chain of command, namely the independent trial judge on the national level as well as on the European level when for example the ECtHR assess compliance of national laws with article 6 ECHR; and there is external oversight by the national DPA and The Netherlands Institute for Human Rights for compliance of law enforcement actions and criminal procedural law with regulation concerning data protection and non-discrimination respectively. The example of EncroChat investigations in chapter 6 made clear that in practice these three levels are not aligned. Internally there is not enough attention for fundamental rights interests such as privacy, data-protection and non-discrimination, plus the oversight is fragmented as every investigatory judge could set different standards in warrants for large-scale data collection and automated-data analysis; and the oversight by the trial judge only

[1284] Hirsch Ballin, M., & Oerlemans, J. J. Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden. *Delikt en Delinkwent*, 2023(1), 18-38.

[1285] This is discussed in the next section, section 7.2.4.

focuses on the criminal procedural rights (of defense) and article 6 ECHR, expecting the DPA to keep oversight on data protection safeguards and requirements and to oversee data analysis. Nonetheless the data collection, analysis and data use, as well as the values protected by data protection law, non-discrimination law, and criminal procedural law, are not that separated in reality, creating artificial separations in oversight. In principle, this fragmentation could to some extent be addressed by strong oversight by the DPA, since data protection law applies to the data collection, analysis and data use. However, the national DPAs are often understaffed or dealing with very opaque and complex law enforcement systems, hampering effective oversight.

7.2.5 Clashes between different interests

There is also a fundamental rights issue that is perhaps not so much of a gap but more of a conflict: at times the interests protected by the three different legal frameworks can clash and limit full protection.

One way in which this is clear, is the legal protection offered by European non-discrimination law to specific group characteristics and the strict regime under data protection law for special categories of data. From the data protection point of view the requirements are to limit the use of special categories of data (such as ethnicity, sexuality, religion) and from the non-discrimination point of view the perspective is to refuse differential treatment without objective justification based on such categories. The literature study of chapter 2 and the legal analysis and literature study of chapter 4, together with the practical examples of COMPAS and OxRec, make clear that this approach can often have the directly opposite effect and enable indirect discrimination. In many cases, sensitive factors, such as ethnicity, should be explicitly taken into account to mitigate harmful effects, which the laws of data protection can inherently forbid. I would argue that not allowing the use of special categories of data according to data protection law does not solve problems of discrimination, but instead either leads to the use of proxies (such as the infamous example of using zipcodes as a proxy for ethnicity or nationality) which can cause hidden discrimination or unfair treatment, or to limiting of measures that can counter bias and discrimination. Data protection law should not focus on categorically, apart from some exceptions, limiting the processing of special categories of data, but rather setting specific conditions and requirements which enable a fair use of such data to prevent the use of proxies aiming to bypass regulation of special categories of data and to prevent errors and discrimination stemming from a lack of data processing relating to sensitive characteristics of individuals.

Another instance in which a clash of interests happens is in the tradeoff between accuracy and informational privacy that takes place in a lot of profiling processes. It is possible that the rationale of data protection law of limiting the collection of data is at odds with the inherent way in which profiling works. For example, for profiles to be accurate, and individuals thus being treated on the basis of accurate information, data *minimumization* might be required rather than data minimization.[1286] Data minimumization refers to a minimum level of data that is necessary to achieve accuracy as well as fairness, especially for non-distributive profiles, where the context is so important. To do justice to the specific circumstances of cases at hand a contextual approach to profiling is necessary.[1287] Such a contextual approach is reminiscent of Nissenbaum's seminal theory of contextual integrity. According to Nissenbaum's theory, privacy can only be achieved through an appropriate flow of information; that information flow requires contextual information taking into account the data subject, the sender, the recipient and the information type.[1288] The idea of contextual factors is crucial to risk profiling, going beyond the dichotomy between accuracy on the one hand and informational privacy and data minimization on the other hand. The importance of context brings different values together. In risk profiling, data are sometimes used for categorizations and assessment for other purposes or in other contexts than the original data collection. In addition, by combining data points to make up one category, the variety of data points alter the context. In a grouping or in the total risk profile data are thus ascribed new meaning, as profiling focuses on deriving new information from already existing data. A lack of contextual factors and too much focus on data minimization thus risks inaccuracies.

7.3 Moving towards more comprehensive fundamental rights protection

After having discussed the main conclusions of the dissertation in section 7.2, pertaining to which problems exist in the regulation of risk profiling, section

---

1286 Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR, p. 26; For a similar argument, see: van der Sloot, B. (2012). From Data Minimization to Data Minimummization. In B. Custers, T. Calders, B. Schermer & T. Zarsky (eds.), 'Discrimination and Privacy in the Information Society', Springer, Heidelberg 2012, p. 273-287.

1287 S. van Schendel, Data used in governmental automated decision-making & profiling: towards more practical protection, (Accepted/In press) The boundaries of data: Technical, practical and regulatory perspectives. van der Sloot, B. & van Schendel, S. (eds.). Amsterdam: Amsterdam University Press.

1288 Nissenbaum, H. (2020). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press; Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 79, 119.

7.3 describes possible solutions. In view of the gaps and conflicts, I propose recommendations along five different, but sometimes interconnected, lines: regulation of data analysis, regulation that goes beyond the individual interest, more focus on regulation of contextuality, strengthened oversight on large scale data collection and analysis, and more practical alignment of different regulatory frameworks. Each of these is explained below.

7.3.1 Stronger regulation of data analysis

Already with the peak in the hype of the topic of big data analytics in scientific research in 2015 and 2016, many scholars pointed out the inherent tension between regulating the collection of data from a point of view of minimization and purpose specification and limitation versus the large, varied, and sometimes unbridled collection of data for big data analytics.[1289] Thus far, the focus of this debate has very much been on the data collection, as the collection of data can be an interference to the right to privacy in itself. In addition, limiting or at least steering the collection of data through strict rules on purpose prevents the combining of data from various sources without a clear purpose and the creation of profiles based on those correlations. However, limiting the collection of data is only one part of the picture, it says little about the way in which the data are used. Several scholars have made arguments in favor of focusing more on the regulation of the use of data,[1290] or in favor of moving away from the notion of the purpose of the collection and further processing being the key to data protection.[1291]

To mitigate issues that arise during the analysis phase of profiling, it is important to create provisions that see specifically to that phase. The data protection framework seems the most suitable legal field to regulate data analysis, since it is so strongly

[1289] WRR, Big Data and Security Policies: Serving Security, Protecting Freedom, Policy brief 6, 2017, p. 19, available at: https://english.wrr.nl/binaries/wrr-eng/documenten/policy-briefs/2017/01/31/big-data-and-security-policies-serving-security-protecting-freedom/WRR_PB6_BigDataAndSecurityPolicies.pdf.

[1290] For example: Hoboken, J. van (2016) 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and U.S. Frameworks for Personal Data Processing', pp. 231-259 in: *B. van der Sloot, D. Broeders and E. Schrijvers (eds.) Exploring the Boundaries of Big Data*, WRR-Verkenning 32, Amsterdam: Amsterdam University Press; Koops, B.J. (2013) 'On decision transparency, or how to enhance data protection after the computational turn', pp. 196-220 in: *M. Hildebrandt and K. de Vries (eds.) Privacy, due process and the computational turn*, Abingdon: Routledge; Sloot, B. van der (2016) 'The Individual in the Big Data Era: Moving towards an Agent based Privacy Paradigm', pp. 177- 203 in: *B. van der Sloot, D. Broeders and E. Schrijvers (eds.) Exploring the Boundaries of Big Data*, WRR-Verkenning 32, Amsterdam: Amsterdam University Press; Moerel, E.M.L. and Prins, J.E.J., Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data.

[1291] Moerel, E.M.L. and Prins, J.E.J., Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016). Available at: http://dx.doi.org/10.2139/ssrn.2784123, p. 7.

connected to data itself. The data protection principles apply to data analysis, as they apply to any form of processing. However, since there are still challenges of bias and opacity in existing risk profiling systems, the principle of fair processing does not appear to be functioning so well; for example, literature on bias in police data shows substantial problems in this regard, yet police data are an important source of data for risk profiles.[1292] In the law enforcement sector there is some opacity related to criminal investigations, the principle of transparent processing does not appear in the LED. I would propose there should be a provision that stipulates what information should be provided to data subjects in terms of analysis, with a special sub paragraph stipulating information to be provided in case of profiling. Such information should at least specify the categorization used as well as the type of AI or software used. Such a provision would not be an information right, which has to be exercised by the data subject, but rather an information obligation for controllers. However, it is important to acknowledge that there can be practical barriers to implementing such an obligation, resembling the issues discussed in for example the right to an explanation debate under the GDPR[1293] and encountered in the exercise of data subjects' rights under the LED[1294], such as how to interpret such an obligation practice and how to ensure that law enforcement actors have the time and means to provide all the relevant information.

Second, I would propose a provision that says something about standards or requirements for data analysis in general, which are also useful outside of the scope of risk profiling. While there is the general principle of accuracy in processing of personal data, profiles remain an instrument of probability, having risks of errors even though the input data itself were correct. Inspiration could be sought with existing niche standards for data analysis, such as those contained in the Code of Practice for European Statistics.[1295] Principles that could be interesting for risk profiling include, for example, the principle that the statistical methodology used must be independent, objective and reliable, that organizations must regularly monitor compliance with these principles, where necessary with the help of external experts, and that not only the statistical methodology used must be made public, but also the data sources and the method of data collection. If an error has been discovered in the methodology or

---

1292 See chapter 3, section 3.3.

1293 See chapter 4, section 4.3.4.

1294 See for example: P. Vogiatzoglou; K. Quezada Tavarez; S. Fantin; P. Dewitte, "From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 11, no. 3 (2020): 274-302.

1295 Praktijkcode voor Europese statistieken: voor de nationale statistische autoriteiten en Eurostat, Comité voor het Europees statistisch systeem, 16 November 2017, available at: https://ec.europa.eu/eurostat/documents/4031688/9394211/KS-02-18-142-NL-N.pdf/580e523c-85a4-406d-9ad2-9a78f5820fc6.

statistical outcome within the big data context, then this should be made public and the main statistical outputs should be checked regularly, for example for biases.[1296] Preferably, data analysis in law enforcement should be done on the basis of the same procedures, in order to guarantee that standard terms, definitions, classifications and other standards are used in the same way everywhere. Finally, it could be stipulated that persons in charge of data analysis within an organization should be trained to do so and that there is a dividing line between the departments in charge of statistical analysis and the law enforcement officers involved in conducting criminal investigations, in order to prevent undue influence.[1297] This final point seems to be applied to some extent in the practice of Dutch criminal investigations, where there is a separation between technical experts performing the data analysis and investigative officers working on the case receiving the outcomes of data analysis from technical colleagues. Although we see some examples of this practice in the EncroChat investigations, it would be clearer and stronger if this separation in roles was regulated, most logically in the Police Data Act and Police Data Decree. So far these instruments stipulate which investigative officers have access to which data, but do not clearly regulate separations of different roles or tasks. Related interesting provisions would be provisions that connect consequences to the labels or categories of victims, witnesses, suspects and offenders. While these distinctions are fluid and not always interesting to make,[1298] it is important that the fluidity and grey areas are taken into account in the data analysis and demand precaution where the data in particular does not pertain to suspects.

Data protection law in its scope is limited to the processing of personal data; however, many processes in risk profiling are not so much about personal data, they are about large amounts of aggregated data. Whether or not a piece of data was personal data in the collection phase becomes increasingly irrelevant when in the analysis phase, data are aggregated and are no longer personal data. In the long run, this may create a legal loophole, as non-personal data can also be used to make decisions that have a major impact on the lives of citizens.[1299] A statistical profile of the security risks within a neighborhood that is used to make decisions, such as when and where to deploy police patrols, does not necessarily contain personal data as such, but can have a major

---

1296 van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302;

1297 van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302;

1298 See chapter 6, section 6.5.2.

1299 van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302; see also van der Sloot, B., & van Schendel, S. (2019). De Modernisering van het Nederlands Procesrecht in het licht van Big Data. Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving. TILT/WODC, Tilburg, p. 9.

impact on those living in the neighborhood. Data increasingly shift between being personal or non-personal and between for example falling in special categories of data or not; a set of special category personal data can be aggregated in a split second and used for a statistical profile, then enriched with another dataset so that personal data is processed again, and then anonymized again. With regard to the analysis phase of profiling, in which the data is processed at a highly aggregated level and algorithms find statistical correlations and general patterns, there does not seem to be much regulation in place, while errors are made especially in this phase.[1300] Although working with large data-sets, from which statistical relationships are distilled, the common statistical methodology, standards and principles are not regulated. This adversely affects the quality of for example predictions and can result in law enforcement policy choices being based on incorrect assumptions;[1301] or when there is a bias in a dataset, algorithm or group profile, as a result of which decisions are taken, this can lead to discrimination or errors. For example, if the police database systematically contains more data about violations of the law by people with a migration background, the predictive algorithm will recommend the police to increase their surveillance in neighborhoods where many people with a migration background live, resulting in even more registrations of people with a migration background.[1302] Creating legal provisions on specific parts of the analytical process, such as provisions on statistical methods, on categorization, on inferences or on the use of AI can contribute to accuracy and reduction of bias.

As explained throughout this dissertation, the aspect of automated decision-making of profiling is regulated under data protection law with specific safeguards, such as human intervention. The human intervention pertains to an end result of the profiling process, namely the application of a profile in the form of a decision. However, I would argue that means a human decision-maker has meaningful influence over

1300 van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302; see also van der Sloot, B., & van Schendel, S. (2019). De Modernisering van het Nederlands Procesrecht in het licht van Big Data. Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving. TILT/WODC, Tilburg, p. 9.

1301 van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302; see also van der Sloot, B., & van Schendel, S. (2019). De Modernisering van het Nederlands Procesrecht in het licht van Big Data. Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving. TILT/WODC, Tilburg, p. 9.

1302 van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302; see also van der Sloot, B., & van Schendel, S. (2019). De Modernisering van het Nederlands Procesrecht in het licht van Big Data. Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving. TILT/WODC, Tilburg, p. 9.

the application of the profile; it does not necessarily pertain to the process prior to the application, namely the data analysis. It would be better from a fundamental rights perspective, or at least clearer, if under data protection law there was a clear separation between profiling and automated decision-making, containing two different provisions. The current provisions of article 11 LED and article 22 GDPR could, in a changed form, pertain solely to automated decision-making, focusing on the application of automated analysis to data subjects in the form of decisions and directing safeguards to that aim, such as human intervention; there could then be a separate provision on profiling focusing for example on inferences and categorization.

7.3.2 Regulation of profiling beyond the individual[1303]

Profiles often involve some component of aggregation: data from individuals are combined to detect patterns and correlations. Together, these correlations can form a profile that represents an idea of a specific individual, such as a profile reflecting a group of individuals with a shared interest or shared behaviour. Thus, this kind of profile is about a group of individuals who share data points rather than about one specific individual. For group profiles, there is an assumption that the creation and use of them is less harmful than profiles about specific individuals: the legal framework tends to offer protection only if the profile is applied to an individual or if the profile is comprised of traits of specific (identified or identifiable) individuals. For example, in data protection law safeguards are attached to the use of profiles and decision-making only on the individual level. Article 22 of the GDPR and article 11 of the LED both limit automated decision-making and profiling but only when it comes to a decision concerning a data subject, thus an individual.

The headings of article 22 GDPR and article 11 LED make clear that both provisions apply only to decisions about individuals. The text of the provisions further emphasises this by mentioning the data subject in singular form. The scope of the LED and GDPR applying only to the processing of personal data and the focus on natural persons demonstrates that these instruments are tailored to the individual. Over the years, there have been increasingly more discussions about the strong individual emphasis

[1303] Parts of this subsection are based on: (Accepted/In press) S. van Schendel, Data used in governmental automated decision-making and profiling: towards more practical protection. In: *The boundaries of data: Technical, practical and regulatory perspectives*. van der Sloot, B. & van Schendel, S. (eds.). Amsterdam: Amsterdam University Press, 2023.

of data protection legislation at the expense of attention for groups and collectives.[1304] This point of criticism on instruments like the GDPR and the LED becomes painfully clear in connection to profiling. While the protection offered by data protection law, such as in article 22 GDPR and article 11 LED, focuses on the individual, algorithmic harms in profiling arise from how systems classify or compare groups, creating a mismatch between profiling practices and the legal safeguards. Some scholars argue that this issue with groups versus individuals has been an issue in data protection and privacy legislation for some time,[1305] and that the issue remains underexplored in the context of automated decision-making and explanations.[1306] The creation of groups and categories means that profiling practices can have risks or harmful effects that go beyond the individual or are not even applicable to the individual level. This concern also applies to automated decision making, where scenarios are possible in which a decision has an effect that goes beyond the individual and, therefore, article 22 GDPR or article 11 LED apply to one individual while the actual scope of the decision is much broader. Collective decisions affecting multiple individuals or groups can, for example, be based on the shared characteristic of living in a certain area, such as is the case with automated decisions taken by the police to increase police surveillance in a certain geographical area, affecting all data subjects living in it.[1307]

Although the scope of the LED and GDPR pertains to personal data and thus natural persons, that does not mean that data protection instruments of the future should not protect collectives of data subjects. A clear example where data protection law does take the collective dimension into account is through the right to representation. Article 55 LED grants data subjects the right to mandate a not-for-profit body, organization or association to lodge a complaint on his or her behalf and to exercise the right to lodge a complaint with a supervisory authority, the right to an effective judicial remedy against a supervisory authority and the right to an effective judicial remedy against a

---

1304 See for example: A. Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, *Computer Law & Security Review*, Volume 32, Issue 2, 2016, Pages 238-255, https://doi.org/10.1016/j.clsr.2016.01.014; L. Taylor, L. Floridi, and B. Van der Sloot, eds. *Group privacy: New challenges of data technologies*. Philosophical Studies series, vol. 126. Springer, 2017.

1305 P. De Hert & V. Papakonstantinou, Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review* 40 (2021); L. Taylor, L. Floridi & B. van der Sloot (eds), *Group Privacy. New challenges of data technologies*, Philosophical Studies series, vol 126, Springer, 2017, p. 238.

1306 L. Edwards and M. Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1, p. 22.

1307 Brkan, M. (2019). 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond', pp. 91-121 in *International Journal of Law and Information Technology*, 27, doi: 10.1093/ijlit/eay017, p. 100.

controller or processor, on his or her behalf. Article 80 GDPR bestows a similar right to representation for the GDPR regime. While the right to representation is rather about a bundling of individual interests of the different data subjects rather than the interest of a group as such, it still demonstrates the possibility of a shared interest or a harm that simultaneously concerns more than one data subject. If a categorization is discriminatory or incorrect in itself, the group of individuals forming that category might want to contest that on a group level rather than an individual level. It would be good to acknowledge, for example through EDPB guidelines, that the right to representation can also be used for data processing impacting groups; this protection can be linked to a group being a collection of data subjects to make it fit in the scope of data protection.

Under non-discrimination law, legal protection is already strongly connected to group protection. Under criminal procedural law, the oversight whether internally or through the trial judge is so far strongly focused on the individual dimension, as the criminal investigation and trial will focus on one individual (or one criminal organization). There is no acknowledgement yet under criminal procedural law of the interests of groups that stem from data analysis focused on groups, for example for users of a specific technology such as in the case of EncroChat. Through stronger regulation of data analysis as described above, this can also mitigate issues for groups that arise in the analysis phase, such as over-targeting of specific groups in police surveillance. The oversight discussed below should also be broader than individual cases, focusing on the bigger picture of large scale data collection and analysis such as risk profiling, which will automatically also mitigate negative effects on groups and protect group interests.

7.3.3 Regulation of contextuality[1308]

A variety of data are used in profiling and automated decision-making tools. These data range from non-personal data –such as aggregated data–, to static personal data –such as date of birth–, to dynamic personal data – such as behavioural data. The great variety of data underpinning automated decision-making and profiling begs the question if each data type is equally suited for the purpose of the decision-making or profiling in question. Because in risk profiles so many data sources are mixed and categorizations are made based on correlations rather than causal relations, context matters. Contextual information can reduce errors and bias and increase fairness and transparency.

[1308] This subsection is heavily based on: (Accepted/In press) S. van Schendel, Data used in governmental automated decision-making and profiling: towards more practical protection. In: *The boundaries of data: Technical, practical and regulatory perspectives*. van der Sloot, B. & van Schendel, S. (eds.). Amsterdam: Amsterdam University Press, 2023.

When data are collected, they are collected in a specific context, which is characterised by at least the following elements. First of all, there is usually a specific purpose for which the data are collected at that moment in time. Second, there is a specific perspective on the subject of the data. This is not to be confused with the data protection term, 'data subject', because outside of the scope of data protection law, the subject of the data can also be a group of individuals or a person that cannot be identified in said data. Third, there is a specific actor gathering the data, bringing its own perspective to the collection. The importance of these elements is illustrated below.

As described in this dissertation, profiling is focused on evaluating aspects, such as behaviour of people. To get to that point, one needs to take several steps, such as defining categories, labelling characteristics as belonging to specific categories and grouping individuals into the categories based on their apparent characteristics. In this sense, profiles are a type of image that can be used to identify and represent someone.[1309] Profiles carry an assumption that an individual has all the characteristics attributed to them in the profile, which is not problematic for distributive profiles but may be problematic for non-distributive ones. This assumption, together with the possibility of comparing different individuals and groups easily, enables mastering large quantities of data. Processing data in this way does not necessarily imply that the analysis results in meaningful information; correlations do not require a causal relationship between different characteristics, nor a meaningful relation between data points, which makes the assumption more problematic.

Thus, in profiles, there will be data points connected that originally belonged to different contexts. We can see an example of this in the case of SyRI. In some instances, data about water consumption and water billing were the main data in a risk profile on fraud in income compensation. The use of data in a different context than what they were originally gathered for raises issues from a privacy perspective. For example, people tend to have an expectation that data about their water usage will be used mainly for purposes like determining the water bill, efficiently running the drinking water system, fair dividing of drinking water or efficiently running the sewage system. Generally speaking, water data being used to determine instances of fraud is not what most people would expect. This is partially why projects like the Waterproof project under SyRI were received with such scepticism: people felt surveilled after it became publicly known that this kind of data was being used for these kinds of purposes.[1310] In the court case against the legislation that regulated the SyRI system, claims were put forward based on privacy

[1309] Hildebrandt M., Backhouse J. (2005), Descriptive analysis and inventory of profiling practices. In FIDIS Project Deliverable 7.2., p. 51, Available at: http://www.fidis.net.

[1310] District court The Hague 5 February 2020, ECLI:NL:RBDHA:2020:1878, para. 3.8.

violations and the chilling effects of data driven social welfare systems[1311], inter alia because people have a certain expectation what their data will be used for that does not align with the all the use in reality. The idea that people have a certain assumption about data collection within a particular context is not new. Nissenbaum raised awareness of this issue with her theory on contextual integrity, where privacy protection requires norms of specific contexts, stipulating that information gathering and dissemination has to be appropriate to the relevant context.[1312]

There is another part of contextualisation of data collection illustrated by SyRI: the data collected are gathered about a specific subject, namely groups in society that receive social benefits. This is a context that creates its own specific challenges that should be taken into account, as it includes a potentially vulnerable group within society.[1313]

The importance of being aware of all three aspects of context in which data are gathered are illustrated through the SyRI example: the purpose for which data are collected, the subjects about whom data are collected, and the perspective of the actor who is gathering the data; the collection of data about water use comes with the expectation of a certain purpose, but the use in reality can be different than expected given the role of the actor who uses the data, and the subject of the data can be an especially vulnerable individual -for example financially- creating distrust towards future data collection. It is important to align all three of these contextual aspects to prevent privacy, opacity, discrimination and stigmatisation problems. In practice, all factors of context matter.

When looking at the example of applications like OxRec, there is the additional complexity that comes with law enforcement data. Law enforcement data can be influenced by underreporting of crimes or by a focus on certain crimes or groups over others.[1314] Crime data are not real time data of actual crime; they simply reflect the

---

1311 District court The Hague 5 February 2020, ECLI:NL:RBDHA:2020:1878.

1312 See for example: H. Nissenbaum, Symposium, Privacy as Contextual Integrity, 79 *Wash. L. Rev.* 119 (2004). Available at: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.

1313 Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/HA ZA 18/388), available at: <https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf >.

1314 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366; E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

rate of crime that was caught or reported and recorded.[1315] Not only is crime data not a perfect mirror of crime occurring, but the police also make choices regarding their data, which influences the data through the way they observe, notice, act upon, collect, categorise and record it.[1316] At the same time, a system like OxRec is an important advisory tool in probation- and sentencing decisions.

Bias in data also plays a role in general in data. For example, factors such as postal code, gender, age, education level or income can be good predictors (for example to determine the likelihood that someone will commit crimes), but they can also be indicators for ethnic profiling.[1317] A similar problem is visible in profiling and automated decision-making in the context of social welfare systems, such as SyRI, where interventions can be location or neighbourhood based and thus indirectly target specific societal groups who become overrepresented in the system. For all data, it should be considered that they are gathered in a certain way and that data are always a representation of reality. To be sure, in governmental decision-making that is not automated, there is just as well bias in human thinking and decision-making. Nonetheless a crucial point is that the more data-driven systems become, the more difficult it is to disentangle the decision-making from the biased data, the more hidden the bias is and the more exacerbated the inequalities.

As data driven processes – such as profiling and automated decision-making – are so dependent on non-personal data – such as statistics and aggregated data – non-personal data play perhaps an equally important role as personal data. Arguably, aggregated data and statistics actually fuel the constructions of models and compilations of categories. Ultimately, this means that the use of non-personal data affects groups and individuals when profiles are applied to them or lead to decisions impacting them. The EU legislator has opted to only focus on the application of profiles on individuals with data protection legislation by focusing on human intervention as a safeguard and setting requirements for when profiling and automated decision-making can be deployed. However, in this approach the EU legislator leaves the door open for the gathering of statistical and aggregated data and for the creation of

---

1315 L. Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366; E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

1316 E. Joh, Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, vol. 26:287.

1317 Van Dijck, G. (2020). Algoritmische risicotaxatie van recidive. Over de Oxford Risk of Recidivism tool (OXREC), ongelijke behandeling en discriminatie in strafzaken. *Nederlands Juristenblad*, 95(25), 1784-1790; Richard S. Frase, 'What Explains Persistent Racial Disproportionality in Minnesota's Prison and Jail Populations?', *Crime and Justice: A Review of Research* 2009, p. 201-280.

profiles, while it remains an open question whether the collection of statistical and aggregated data that are later used for profiling and the creation of profiles are not a privacy and data protection risk as such.

Correlations and patterns also create new meaning, and thus seemingly insignificant personal data can become highly significant.[1318] The same is true for non-personal data: they can be deemed not to contain sensitive or important information but, if combined with other data, can actually reveal a lot of traits, behaviours and other valuable information, at which point data protection legislation and even data protection legislation on processing of special categories of data can become applicable. This raises questions for legislators how to protect individuals against privacy infringements caused by the generation of information in either unseen ways creating legal uncertainty about which legal provisions to apply or in ways that are not covered by existing data protection legislation and privacy safeguards.

In practice, it is difficult to draw strict boundaries between what data can or cannot be used in profiling and automated decision-making. Data can for example be assumed not to be sensitive while actually being much more sensitive than other types of personal data, especially in a specific context. A good example of this can be found in processes conducted by the Dutch Tax Administration that were deemed unlawful by the Dutch DPA. In July 2020, the Dutch DPA determined that the Benefits Office of the Dutch Tax Administration should not have processed the nationality -which was assumed not to be sensitive to the context- of childcare benefit applicants in the way it had been doing for years. According to the results of the DPA's investigation, this practice was unlawful and discriminatory.[1319] This example of using nationality as an important factor in a profile shows that the value and sensitivity of a type of data are very much dependent on their situation or context.

Therefore, I propose that a new data protection principle of contextuality could be adopted or could be added explicitly to for example the principle of accountability. This could focus on describing and logging of contextual factors and origins of data, which can be especially useful in the context of re-use of data.

1318 Hildebrandt, M. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

1319 See: Autoriteit Persoonsgegevens, 'Methods used by Dutch Tax Administration unlawful and discriminatory', 17 July 2020, available at: https://www.autoriteitpersoonsgegevens.nl/en/current/methods-used-by-dutch-tax-administration-unlawful-and-discriminatory.

7.3.4 Stronger regulation of oversight

There are several actors involved in the risk profiling process in criminal justice with different responsibilities. There is the police, who collect, analyze and use the data; the public prosecution, where the public prosecutor or assistant public prosecutor can give authorization for the deployment of investigative powers through which data are gathered; the investigatory judge, who needs to give authorization for police powers when there is a serious expected interference to the right to privacy; the trial judge, who in retrospect assesses whether the investigation, prosecution and trial are in line with criminal procedural law; the DPA, who oversees compliance with the Police Data Act and the Judicial Data and Criminal Records Act; and there is the Netherlands Institute for Human Rights that oversees compliance with non-discrimination law for Dutch law enforcement.

There are a couple of points to make as to why the current forms of oversight do not function adequately for risk profiling and how these issues could be solved. First of all, there is a gap in oversight when it comes to the role of the judge in the criminal trial. Many activities involve data processing but will not lead to prosecution of a specific suspect, or to a trial of a suspect. These parts of the data collection, analysis and use will not be assessed by the trial judge. Related to that point, there can also be data processing activities, such as initial data collection or gathering of intelligence not with the purpose of taking decisions for the prosecution process, and thus these activities are seen as out of the scope of the criminal investigation.[1320]

A second point is the lack of consequences when the judge does rule on privacy infringements. Some scholars propose that when the activities are within the ambit of the criminal investigation and thus within the competency of the judge to assess, the judge is reluctant to attach consequences to violations of rights of the defendant.[1321] Schermer and others propose that the interest of truth finding seems to get preference over the interest of sanctioning police violating procedural rules,

---

[1320] Hirsch Ballin, M., & Oerlemans, J. J. (2023). Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden. *Delikt en Delinkwent*, 2023(1), p. 33; see also: Eeden, C.A.J. van den, Berkel, J.J. van, Lankhaar, C.C., Poot, C.J. de, Opsporen, vervolgen en tegenhouden van cybercriminaliteit, WODC, Cahiers 2021-23, available at: http://hdl.handle.net/20.500.12832/3114.

[1321] Schermer, B. W. (2022). De gespannen relatie tussen privacy en cybercrime. Inaugural lecture, Universiteit Leiden, 7 November 2022. Retrieved from https://hdl.handle.net/1887/3484256, p. 11; See also: Kuiper, R. (2014). Vormfouten, juridische consequenties van vormverzuimen in strafzaken, dissertatie Radboud Universiteit Nijmegen; Nan, J. S., Bektesevic, D. (2017), Structurele vormverzuimen: een structureel probleem?, in: DD 2017/22; Samadi, M. (2020), Normering en toezicht in de opsporing Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen, dissertatie Universiteit Leiden.

which has consequences for the attitude of police and the public prosecution regarding such procedural rules.[1322] I agree and would add that the reluctance displayed by some judges in the EncroChat cases to assess compliance by the police with rules on data analysis further demonstrates that it will be rare to find serious consequences attached to infringements to the right to privacy.[1323]

A third point is the gap between the CCP and the Police Data Act.[1324] Because the Police Data Act is considered a piece of data protection legislation, it is not considered an ordinance of criminal procedural law, and thus not assessed by the judge in assessment of the powers used in the criminal investigation. The lack of interaction between the two legal frameworks thus has its consequences for the oversight as well.[1325]

Seeing that more oversight than is currently offered by the judge of the criminal trial is needed, the question is then where this function should be situated. It appears that currently oversight on large scale data operations in the law enforcement sector is not the priority of the Dutch DPA; looking into their most recent annual report, the emphasis of their oversight seems to be on European law enforcement data bases and data exchange.[1326] I propose oversight should rather be assigned to an actor that has a broader competency than the individualized criminal investigation (compared to the criminal trial judge), but with expertise specific to the law enforcement domain (compared to the DPA); to bestow an ideally situated actor with such oversight it would be recommended to create a new oversight body. Creating a new oversight body is also

1322 Schermer, B. W. (2022). De gespannen relatie tussen privacy en cybercrime. Inaugural lecture, Universiteit Leiden, 7 November 2022. Retrieved from https://hdl.handle.net/1887/3484256, p. 11; See also: Kuiper, R. (2014). Vormfouten, juridische consequenties van vormverzuimen in strafzaken, dissertatie Radboud Universiteit Nijmegen; Nan, J. S., Bektesevic, D. (2017), Structurele vormverzuimen: een structureel probleem?, in: *DD* 2017/22; Samadi, M. (2020), Normering en toezicht in de opsporing Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen, dissertatie Universiteit Leiden.

1323 District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584, para. 2.1.

1324 See for example chapter 6, sections 6.6.1.3 and 6.6.2.

1325 Hirsch Ballin, M., & Oerlemans, J. J. (2023). Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden. *Delikt en Delinkwent*, 2023(1), 18-38.

1326 Autoriteit Persoonsgegevens, Jaarverslag 2021, available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarverslag_ap_2021.pdf, p. 15 & 16; Of course this comes with the caveat that it is not fully certain to say what exactly the oversight of the DPA on law enforcement consitutes in practice based on publicly available information.

in line with the recommendation by the PG to the Dutch Supreme Court.[1327] I agree with the PG that there needs to be a body of oversight for large scale data collection, analysis, and use; this new oversight body would have two tasks. On the one hand oversee specific large scale operations, comparable to operations that happened in the past in taking down cryptophone networks, through ex ante permissions and continuous oversight. As well as having the power to inquire into specific investigations. On the other hand the oversight body would have a task to harmonize and give structure to processes of data collection, analysis and use, in general through the drafting of guidelines for police and the public prosecution and through audit procedures. I further propose that law enforcement actors such as police and public prosecution need to be transparent about their policies and decision-making at large, for example by publicly available guidelines that provide information about the use of large scale data and profiling as such. This does not address the group dimension of profiles as such but does help mitigate some of the problematic aspects of new categorizations, as well as assisting in complying with non-discrimination law and data protection principles. The oversight body could also assess such guidelines and protocols and oversee compliance.

An alternative option would have been to bestow the competency of such oversight to an already existing body that has field specific knowledge, broader than specific criminal investigations at hand; such a body is the Inspectorate of Justice and Security. There are two important qualifications that the Inspectorate of Justice and Security lacks though. The first caveat is that the systemic oversight of this body only sees to police activities, excluding the Public Prosecution Service.[1328] The second caveat is that traditionally fundamental rights law, such as article 5 ECHR, requires independent oversight. While a judge such as the investigatory judge could be argued to be independent enough due to its qualifications as a judge, it is unlikely that the Inspectorate of Justice and Security would be viewed as independent comparable to a judge under human rights law, as it is organizationally a part of the Ministry of Justice and Security.

[1327] Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available in Dutch: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf, p. 6; see also Hirsch Ballin, M., & Oerlemans, J. J. (2023). Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden. *Delikt en Delinkwent*, 2023(1), 18-38, who are also in favor of creating a new body of oversight.

[1328] Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available in Dutch: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf, p. 6.

7.3.5 Practical alignment of regulation

Rather than suggesting one all-encompassing law or an integration of elements of one law in another, which would create 'one super law' for risk profiling, I would propose more integration in practice through practical alignment of different legal frameworks. Practical alignment here refers to a process that is broader than adopting guidelines that give interpretation to the law, it also includes training and organizational measures to achieve a different mindset; especially given how procedural rules to protect privacy are often undervalued in criminal trials, as described above.[1329]

The problem with offering fundamental rights protection in the context of law enforcement profiling is not always the laws as such, but the lack of integration of different pieces of laws, which presents fragmentation and gaps in practice. This problem is best illustrated by the lack of interaction between the CCP and the Police Data Act. The criminal procedural framework sets the legal conditions for gathering data in terms of managing levels of privacy infringements, thus which powers can be used in the investigation of which types of crime and degree of suspicion and which authorization is required. The Police Data Act, which is a piece of data protection legislation, determines which data can be used for which policing purposes, which data can be compared, how data can be compared in an automated way, for how long data can be stored, and who has access to which data. In theory, if different pieces of law cover different parts of profiling, that should be sufficient if together those parts cover the entire process of profiling. However, in practice it is not adequate because of compartmentalized thinking; the CCP and Police Data Act are seen as different fields of law, striving to achieve different aims, rather than be seen as covering different stages of data processing (collection, analysis and use). It would be helpful if there were more guidelines within the police and public prosecution organization on safeguards in data analysis that pertain to the right to privacy, data protection and non-discrimination. More specifically, principles from data protection law, such as purpose limitation, proportionality, and human intervention in profiling and automated decision-making could be factors that deserve a more prominent place in data collection, analysis and use by the police, to ensure that the safeguards from data protection law are applied in practice.

1329 Schermer, B. W. (2022). De gespannen relatie tussen privacy en cybercrime. Inaugural lecture, Universiteit Leiden, 7 November 2022. Retrieved from https://hdl.handle.net/1887/3484256, p. 11; See also: Kuiper, R. (2014). Vormfouten, juridische consequenties van vormverzuimen in strafzaken, dissertatie Radboud Universiteit Nijmegen; Nan, J. S., Bektesevic, D. (2017), Structurele vormverzuimen: een structureel probleem?, in: *DD* 2017/22; Samadi, M. (2020), Normering en toezicht in de opsporing Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen, dissertatie Universiteit Leiden.

Practical alignment could also be used to bridge gaps in legislation. As concluded in chapter 6, a question that remains is how the result of data processing under article 8 of the Police Data Act should be treated; what legal status does the risk profile itself have? Article 8 of the Police Data Act does not stipulate that the results of the analysis, such as the profile, have to be deleted. The question of how to treat risk profiles as pieces of data that do not always have a clear connection yet to a criminal investigation, is a question that is situated in a boundary area between data protection legislation and criminal procedural legislation: as it concerns the processing basis for data it would most naturally appear to be a question that should be regulated under data protection legislation, but, as discussed in chapter 4 of this dissertation, the EU LED does not provide an answer. The national implementation of the Police Data Act similarly does not regulate what happens to the results of processing under article 8 of the Police Data Act. At the same time, because bases for processing police data are not regulated in the CCP, no answers can be found there. Guidelines on large scale data collection and analysis should also stipulate how data combinations that provide new information, such as profiles, should be treated. In addition, it would be helpful if the guidelines also stipulate how non-personal data, such as statistical data and group data are handled.

Figure 5 illustrates the interconnections between different recommendations, showing the existence of overlaps between the regulation of data analysis, oversight, and profiling beyond the individual interest, as well as the overlap between regulation contextuality and data analysis. As shown, the increase of regulation of data analysis impacts the other three recommendations as well. In this way there is a synergy between the different recommendations; they enable one another rather than conflict. Finally, the practical alignment of legal frameworks binds these different recommendations together to ensure the four recommendations align together in practice.

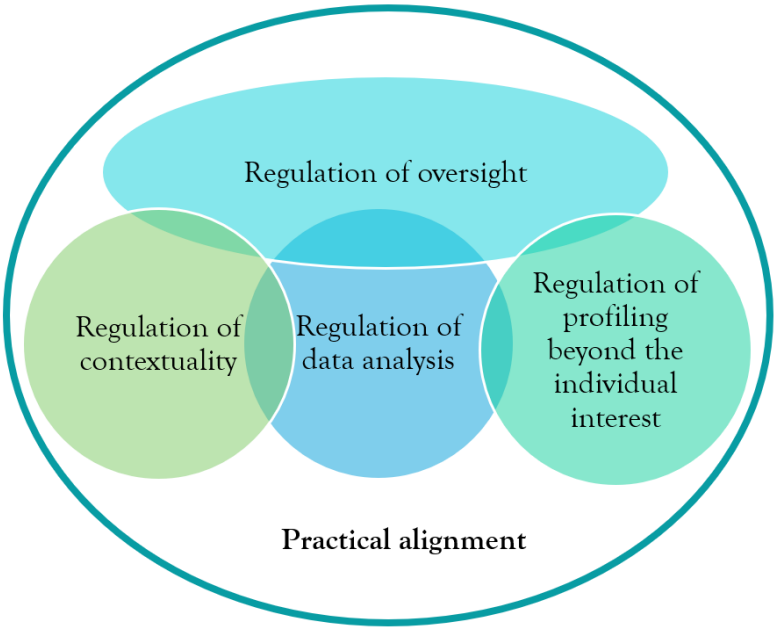

Figure 5. Regulation recommendation for more comprehensive fundamental rights protection.

7.4 Final remarks

This dissertation analyzed the regulation of risk profiling in European data protection law, European non-discrimination law and Dutch criminal procedural law. However over the course of the research for the dissertation, crucial legal developments took place: in EU data protection law, the LED and GDPR came into effect; Dutch criminal procedural law was, and still is, undergoing major reforms in its regulation of powers relevant to risk profiling; and the idea of an EU AI Act arose and is still undergoing development. These legal developments meant for EU data protection law that some pieces of the research on former legislation became less relevant and had to be replaced; for Dutch criminal procedural law that reference was necessary to the potential future legislation; and for the EU AI Act that this was an instrument unfortunately too late to take into account into the research, as the research was finalized in June 2022 while the AI Act was not far enough developed yet to predict what it would look like in the end for law enforcement risk profiling. To briefly reflect here on the latter, as it is currently being debated whether some forms of predictive AI might become prohibited for policing, it could appear at first glance that some applications of risk profiling

would be banned in the future if the legislation is adopted.[1330] However, this is not necessarily the case. As explained throughout the dissertation, many risk profiling systems are presented as advisory tools and not phrased in terms of predictive policing by law enforcement. It is very much the question whether they would meet the threshold of the proposed AI Act's prohibition. More specifically, looking at the text of the amendments made by the EU Parliament, the focus is on banning risk assessment. Amendment 224, introducing a new article 5 paragraph 1 (d)(a), states that it is prohibited:

> *"the placing on the market, putting into service or use of an AI system for making risk assessments of natural persons or groups thereof in order to assess the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal or administrative offence based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of natural persons".*[1331]

Two remarks can be made here. The first is that it will depend on the interpretation of 'AI system for making risk assessment' whether systems that advise in the decisions but do not qualify as automated decision-making fall within the scope of this prohibition. Second, systems mentioned in this prohibition that actually predict the occurrence of crime based on profiles are still quite futuristic; most systems make estimates based on group profiles but cannot be said to actually predict future crimes yet. While it thus very much depends on interpretation of such a provision to what extent different risk profiling activities are covered, it is a positive development from a fundamental rights perspective that there is attention from the EU legislators for the fundamental rights risks of the use of AI in risk assessment and police profiling systems. Such an overarching act, bridging different legal domains, is a step in the direction of alignment of legislation on data protection, non-discrimination, and criminal procedure.

1330 On 11 May 2023 the European Parliament voted on the text of the AI Act, including an amendment that prohibits the use of AI in certain predictive policing systems. See: https://www.europarl.europa.eu/committees/en/artificial-intelligence-act/product-details/20230417CDT11481.

1331 Report on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts 22.5.2023 - (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), available at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_EN.html.

7

Bibliography

Case law

European Court of Human Rights

ECtHR, *Abdu v. Bulgaria*, 2014
ECtHR, *Abdulaziz, Cabales and Balkandali v United Kingdom* 1985.
ECtHR, *Adzhigitova and Others v. Russia*, 2021
ECtHR, *Alajos Kiss v Hungary* 2010.
ECtHR, *Alexandru-Radu Luca v. Romania* 2022.
ECtHR, *Andrejeva v. Latvia* [GC], 2009.
ECtHR, *Anguelova v. Bulgaria*.
ECtHR, *Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxemburg*, application no. 29121/95, 29 June 1999.
ECtHR, *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007.
ECtHR, *B.S. v. Spain*, 2012
ECtHR, *Bekos and Koutropoulos v. Greece*, 2005
ECtHR, *Belgian linguistic case*, 1968.
ECtHR, *Belli and Arquier-Martinez v. Switzerland*, 2018.
ECtHR, *Biao v. Denmark* (Grand Chamber), No. 38590/10, 24 May 2016.
ECtHR, *Big Brother Watch and Others v The United Kingdom* App nos. 58170/13, 62322/14 and 24960/15, 2018.
ECtHR, *Burden v. the United Kingdom* [GC], 2008.
ECtHR, *Carson and Others v. The United Kingdom* App no 42184/05, 2010.
ECtHR, *Chassagnou and Others v. France* [GC], 1999.
ECtHR, *Cînța v. Romania*, 2020.
ECtHR, *Clift v The United Kingdom* App no 7205/07, 2010.
ECtHR, *Cyprus v Turkey* 2001.
ECtHR, *D.H. and Others v. the Czech Republic* [GC], 2007.
ECtHR, *Di Trizio v. Switzerland*, 2016, para. 86.
ECtHR, *EB v France* (2008) 47 EHRR 21.
ECtHR, *Engel and Others v The Netherlands* 1976.
ECtHR, *Fabian v Hungary*, App no 78117/13, 2017.
ECtHR, *Fedorchenko and Lozenko v. Ukraine*, 2012
ECtHR, *Glor v Switzerland* 2009.
ECtHR, *Guberina v. Croatia*, 2016.
ECtHR, *Hoffmann v Austria* 1993.
ECtHR, *Hoogendijk v. the Netherlands*, 2005.
ECtHR, *Hugh Jordan v. the United Kingdom*, 2001.
ECtHR, *Khamtokhu and Aksenchik v. Russia* [GC], 2017.
ECtHR, *Khelili v. Switzerland* (application no. 16188/07) 18 October 2011.
ECtHR, *Kiyutin v Russia* 2011.

ECtHR, *Kjeldsen, Busk Madsen and Pedersen v Denmark* Series 1976.
ECtHR, *Klass and Others v. Germany* (Application no. 5029/71) 6 September 1978.
ECtHR, *Konstantin Markin v. Russia* [GC], 2012.
ECtHR, *Lawlor v. UK*, application no. 12763/87, 14 July 1988.
ECtHR, *Leander v. Sweden*, 1987.
ECtHR, *Liberty and Others v. the United Kingdom*, 1 July 2008, appl. no. 58243/00.
ECtHR, *Lingurar v. Romania* (Application No. 48474/14), 16 April 2019.
ECtHR, *Lupeni Greek Catholic Parish and Others v Romania* App no 76943/11 (Grand Chamber), 2016.
ECtHR, *Makhashevy v. Russia*, 2012
ECtHR, *Makuchyan and Minasyan v. Azerbaijan and Hungary*, 2020.
ECtHR, *Malone v. the United Kingdom*, (Application no. 8691/79), 2 August 1984.
ECtHR, *Mamatas and Others v. Greece*, 2016.
ECtHR, *Milanovic´ v Serbia* 2010.
ECtHR, *Moldovan and Others v. Romania* (no. 2), 2005
ECtHR, *Molla Sali v. Greece* [GC], 2018.
ECtHR, *Nachova and Others v. Bulgaria* [GC], 2005
ECtHR, *Opuz v. Turkey*, application no. 33401/02, 9 June 2009.
ECtHR, *Oršuš and Others v. Croatia* [GC], 2010.
ECtHR *Roman Zakharov v. Russia* 4 (Application no. 47143/06) December 2015.
ECtHR, *Rotaru v Romania* (Application no. 28341/95) 4 May 2000.
ECtHR, *S. and Marper v. United Kingdom* (Applications nos. 30562/04 and 30566/04) 4 December 2008.
ECtHR, *Salman v. Turkey* [GC], 2000.
ECtHR, *Sampanis and Others v. Greece*, 2008.
ECtHR, *Schalk and Kopf v. Austria*, 2010.
ECtHR, *Šečić v. Croatia*, 2007
ECtHR, *Sejdić and Finci v. Bosnia and Herzegovina* [GC], 2009.
ECtHR, *Škorjanec v. Croatia*, 2017.
ECtHR, *Stec and Others v. the United Kingdom* [GC], 2006.
ECtHR, *Stoica v. Romania*, 2008
ECtHR, *Stummer v. Austria* [GC], 2011.
ECtHR *Szabó and Vissy v. Hungary* (Application no. 37138/14) 12 January 2016.
ECtHR, *Tauira and others v. France,* application no. 28204/95, 04 December 1995.
ECtHR, *Timishev v Russia* ECtHR (2nd section), App Nos 55762/00 and 55974/00, judgment of 13 December 2005.
ECtHR, *Turan Cakir v. Belgium*, 2009
ECtHR, *Valenzuela Contreras v. Spain*, 1998.
ECtHR, *Weber and Saravia v. Germany*, 2006.
ECtHR, *Weller v. Hungary*, 2009.

European Court of Justice

CJEU (Grand Chamber) of 31 January 2006, *Commission of the European Communities v Kingdom of Spain*, ECLI:EU:C:2006:74.
CJEU, *Coleman v Attridge Law* 17 July 2008, C-303/06, ECLI:EU:C:2008:415.
CJEU (Grand Chamber) of 16 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, ECLI:EU:C:2008:724.
CJEU, C-293/12 and C-594/12, *Digital Rights Ireland*, 8 April 2014.
CJEU,C-83/14, Judgment ECLI:EU:C:2015:480, 16 July 2015, *CHEZ Razpredelenie Bulgaria*, para 129.
CJEU, Judgment of the Court (First Chamber) of 24 November 2016, *David L. Parris v Trinity College Dublin and Others*, Case C-443/15.

National case law – Germany

Bundesverfassungsgericht, Decision of 4 April 2006 (1BvR 518/02) (2006) 59 Neue Juristische Wochenschrift 1939.

National case law - The Netherlands

College voor de Rechten van de Mens, 22 July 2013, judgment 2013-94.
Supreme Court, 4 March 2014, ECLI:NL:HR:2014:477.
Supreme Court, 1 July 2014, ECLI:NL:HR:2014:1562.
Centrale Raad van Beroep, 21 November 2017, ECLI:NL:CRVB:2017:4068.
District Court Amsterdam, 19 April 2018, ECLI:NL:RBAMS:2018:2504.
District Court The Hague, 5 February 2020, ECLI:NL:RBDHA:2020:865/ ECLI:NL:RBDHA:2020:1878.
District Court Rotterdam, 24 June 2021, ECLI:NL:RBROT:2021:6050.
District Court Rotterdam, 25 June 2021, ECLI:NL:RBROT:2021:6113.
District Court Amsterdam 16 July 2021, ECLI:NL:RBAMS:2021:3707.
District Court Midden-Nederland, 16 September 2021, ECLI:NL:RBMNE:2021:4480.
District Court The Hague, 22 September 2021, ECLI:NL:RBDHA:2021:10283.
District Court Rotterdam 11 October 2021, ECLI:NL:RBROT:2021:9906.
District Court Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584.
District Court Limburg, 26 January 2022, ECLI:NL:RBLIM:2022:571.
District Court Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1273.
District Court Rotterdam, 11 April 2022, ECLI:NL:RBROT:2022:2809.
District Court Midden-Nederland, 12 April 2022, ECLI:NL:RBMNE:2022:1389.
District Court Limburg 26 April 2022, ECLI:NL:RBLIM:2022:3227.
District Court, Noord-Holland 4 May 2022, ECLI:NL:RBNHO:2022:3833.

District Court (criminal law) Noord-Holland 4 May 2022, ECLI:NL:RBNHO:2022:3899.
District Court Amsterdam, 11 May 2022, ECLI:NL:RBAMS:2022:2384.
District Court The Hague 12 May 2022 ECLI:NL:RBDHA:2022:4504.
District Court The Hague, 14 June 2022, ECLI:NL:RBDHA:2022:5762.

National case law – USA

Loomis vs Wisconsin case *(Loomis v. Wisconsin, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017)*

Legislation & parliamentary documents

Council of Europe

Committee of Ministers explanatory memorandum, to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

Convention 108+ Explanatory Memorandum, available at: https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, No. 108.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, L 350/60.

Council of Europe, June 2018, *Convention 108+. Convention for the protection of individuals with regard to the processing of personal data*. Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

Council of Europe, October 2011, The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 and explanatory memorandum. Available at: https://rm.coe.int/16807096c3.

Council of Europe: European Commission Against Racism and Intolerance (ECRI), ECRI General Policy Recommendation N°11 on Combating racism and racial discrimination in policing, Adopted by ECRI on 29 June 2007, 4 October 2007, CRI(2007)39, https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/recommendation-no.11.

Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223, Strasbourg, 10.10.2018.

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223, Strasbourg, 10/10/2018.

Protocol no. 12. to the Convention for the protection of human rights and fundamental freedoms, Rome, 4.XI.2000, No. 177.

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

European Union

Charter of Fundamental Rights of the European Union (2016) Official Journal C202, 7 June, pp. 389-405.

Commission Communication on the application of Directive 2000/43/EC (COM (2006) 643)

Commission Communication on the protection of individuals in relation to the processing of personal data in the community and information security, COM(90) 314 final SYN 287 and 288, Brussels, 13 September 1990.

Commission Recommendation 92/131/EEC on the protection of the dignity of women and men at work, Council declaration on the implementation of the Commission Recommendation on the protection of the dignity of women and men at work (19 December 1991)

Council Directive 79/7/EEC on the progressive implementation of the principle of equal treatment for men and women in matters of social security (19 December 1978).

Council of Europe, 'Explanatory Report to the Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 XI. 2000)' <https://rm.coe.int/16800cce48>.

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

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, L 281/31.

Employment Equality Directive (2000/78/EC)

Equal Treatment Directive (recast) 2006/54/EC (5 July 2006).

European Parliament Resolution 2010/C 16 E/08.

Gender Goods and Services Directive (2004/113/EC).

JHA Council of 28 and 29 November 2002, Council of the EU doc 14817/02 (press 875), Annex II, 21.

Proposal for a Regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final - 2012/0011 (COD).

Racial Equality Directive (2000/43/EC).

Recast Gender Equality Directive (2006/54/EC).

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

Report on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts 22.5.2023 - (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), available at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_EN.html.

Dutch law

Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), available at: https://wetten.overheid.nl/BWBR0041426/2019-03-01.

Draft bill 'Wetsvoorstel Wetboek van Strafvordering', 30 July 2020, available at: https://www.rijksoverheid.nl/documenten/publicaties/2020/07/30/ambtelijke-versie-juli-2020-wetsvoorstel-wetboek-van-strafvordering.

Kamerstukken II 1996/97, 25 403, no. 3.
Kamerstukken II 2004/05, 30164, no. 3.
Kamerstukken II 2005/06, 30327, no. 3 (explanatory memorandum).
Kamerstukken II 2015/16, 34 372, no. 3.
Kamerstukken II 2015/16, 34 372, no. 4 (Advies RvS)

Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, July 2020.

Politiewet 2012, legislation no. BWBR0031788, available at: https://wetten.overheid.nl/BWBR0031788/2023-01-01.

Reclasseringsregeling 1995, no. 455985/94/6:
https://wetten.overheid.nl/BWBR0007120/2019-06-26.

Rijksbegroting 2020 Justitie en Veiligheid (Kamerstukken II 2019/20, 35300-VI, no. 2)

Tweede Kamer der Staten-Generaal 2017–2018, 34 889, no. 3.

Tweede Kamer, 2017–2018, 34889, no. 3.

Tweede Kamer, 2020-2021, 35869, no. 2, 'Wijziging van het Wetboek van Strafvordering ter bevordering van innovatie van verschillende onderwerpen in het kader van de modernisering van het Wetboek van Strafvordering (Innovatiewet Strafvordering)'.

Tweede Kamer, 2020-2021, 35869, no. 3, explanatory memorandum.

Uitvoeringsregeling reclassering 2005, no. DDS 5378751: https://wetten.overheid.nl/BWBR0019016/2005-11-25.

Wet justitiële en strafvorderlijke gegevens, legislation no. BWBR0014194, available at: https://wetten.overheid.nl/BWBR0014194/2022-07-01.

Wet politiegegevens, legislation no. BWBR0022463, available at: https://wetten.overheid.nl/BWBR0022463/2022-10-01.

Wetboek van Strafvordering, available in Dutch at: https://wetten.overheid.nl/BWBR0001903/2023-01-01.

Wetboek van Strafvordering, legislation no. BWBR0001903, available at: https://wetten.overheid.nl/BWBR0001903/2023-01-01.

Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Tweede Kamer 1996-1997, 25403, no. 3.

Literature and similair sources

Adams, S.G.A.M., 'Vertrouwen is goed, maar controle is beter. De interpretatie van het interstatelijke vertrouwensbeginsel door Nederlandse feitenrechter bij samenwerking tussen EVRM-lidstaten in het kader van internationale digitale rechtshulp in strafzaken en het beginsel van equality of arms', *DD* 2021/74.

Allo, P., "The Epistemology of Non-distributive Profiles." *Philosophy & Technology*, vol. 33, no. 3, Sept. 2020.

Alonso Blas, D., First Pillar and Third Pillar: Need for a Common Approach on Data Protection. In: S. *Gutwirth et al. (eds.), Reinventing Data Protection?* Springer 2009.

Alpaydin, E., *Machine Learning*. Cambridge: MIT Press, 2016.

Ananny, M., and Crawford, K., 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability', *New Media & Society* 20, no. 3 (1 March 2018): 973–89, available at: https://doi.org/10.1177/1461444816676645.

Andrejevic, M., To Preempt a Thief, *International Journal of Communication* 11(2017).

Angèle, C., Rosenblat, A., and Boyd, D., "Courts and Predictive Algorithms". Data & Civil Rights: a new era of policing and justice. October 27, 2015. https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf.

Angwin, J., J. Larson, S. Mattu, and L. Kirchner. "Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks." ProPublica. May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Aradau, C., L. Lobo-Guerrero, and R. van Munster. "Security, Technologies of Risk and the Political: Guest Editors' Introduction". *Security Dialogue* 39, no. 2–3 (April 2008): 147-154. https://doi.org/10.1177/0967010608089159.

Arnardóttir, O.M., 'Multidimensional Equality from Within: Themes from the European Convention on Human Rights', in: *Schiek and Chege (eds), European Union Non-Discrimination Law: Comparative Perspectives on Multidimensional Equality Law* (London: Routledge-Cavendish, 2009) 53 at 60–1.

Arnardóttir, O.M., 'Non-discrimination in International and European Law: Towards Substantive Models' (2007) 25 *Nordic Journal of Human Rights* 140 at 146–9.

Arnardóttir, O.M., 'Vulnerability under Article 14 of the European Convention on Human Rights' (2017) Vol. 4 *Oslo Law Review* 150.

Arnardóttir, O.M., "The differences that make a difference: recent developments on the discrimination grounds and the margin of appreciation under Article 14 of the European Convention on Human Rights." *Human Rights Law Review* 14, no. 4 (2014).

Article 29 Data Protection Working Party, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, WP233, 01 December 2015.

Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 17/EN WP 258.

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01.

Autoriteit Persoonsgegevens, 'Jaarverslag 2021', available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarverslag_ap_2021.pdf.

Autoriteit Persoonsgegevens, Report 17 July 2020. *Belastingdienst/Toeslagen. De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag*. Available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_belastingdienst_kinderopvangtoeslag.pdf.

Baker A. & Phillipson G. (2011) Policing, profiling and discrimination law: US and European approaches compared, *Journal of Global Ethics*, 7:1, 105-124, DOI: 10.1080/17449626.2011.556142.

Balayn A. and Gürses S., "Beyond Debiasing: Regulating AI and its Inequalities", EDRi September 2021, available at: https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf.

Bamforth, N., Malik, M., and O'Cinneide, C., *Discrimination Law: Theory and Context* (Sweet & Maxwell 2008) 73.

Barocas, S., and Selbst, A., "Big data's disparate impact" *California Law Review* vol. 104 no. 3 pp. 671-729, June 2016 [online] Available: https://ssrn.com/abstract=2477899.

Barocas, S., Nissenbaum, H. (2014) Big data's end run around anonymity and consent. In: *Lane, J., Stodden, V., Bender, S., Nissenbaum, H. (Eds.). (2014) Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge University Press.

Barrett, L., "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border," *New York University Review of Law & Social Change* 41, no. 3 (2017): 327-366.

Bauman, Bigo, Esteves, Guild, Jabri, Lyon, and Walker. "After Snowden: Rethinking the impact of surveillance." *International political sociology* 8, no. 2 (2014): 121-144.

Bayamlıoglu, E., The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", *Regulation & Governance* (2021) doi:10.1111/rego.12391.

Bennet Moses, L. and Chan, J. (2014) 'Using Big Data For Legal and Law Enforcement Decisions: Testing The New Tools', *University of New South Wales Law Journal* 37(2).

Bennett Moses, L., & Chan, J., Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 2018, vol. 28, no. 7, 806–822, https://doi.org/10.1080/10439463.2016.1253695.

Benoît-Rohmer, F. "Lessons from the recent case law of the EU Court of Justice on the principle of non-discrimination." In: *The Principle of Equality in EU Law*, pp. 151-166. Springer, Cham, 2017.

Berk, R., *Machine learning risk assessments in criminal justice settings*, Springer 2019.

Bernstein, P.L. *Against The Gods - The Remarkable Story of Risk*. New York: John Wiley & Sons Inc., 1996, p. 77.

Bijlsma, J., Bex, F., & Meynen, G., Artificiële intelligentie en risicotaxatie: Drie kernvragen voor strafrechtjuristen. *Nederlands Juristenblad* 2019, issue 44, p. 2778- 3319.

Binns, R. (2020, January). On the apparent conflict between individual and group fairness. In Proceedings of the 2020 conference on fairness, accountability, and transparency (pp. 514-524).

Binns, R. and Veale, M., 'Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR', *International Data Privacy Law*, Vol. 11, No. 4, 2021.

Binns, R., Fairness in Machine Learning: Lessons from Political Philosophy, Proceedings of Machine Learning Research 81:1-11, 2018, Conference on Fairness, Accountability, and Transparency 2018.

Borgers, M. J. (2015). De normering van 'lichte' opsporingshandelingen. *Delikt en Delinkwent*, 2015(15), 143-155.

Borgers, M.J., 'Het gemoderniseerde Wetboek van Strafvordering: beginselen en uitgangspunten', *RM Themis* 2017-6, no. 6.

Borking, J., M. Artz, and L. van Almelo, *Gouden bergen van gegevens. Over datawarehousing, datamining en privacy*. Achtergrondstudies en verkenningen 10, Den Haag: Registratiekamer, 1998.

Bosco, F., Creemers, N., Ferraris, V., Guagnin, D., and Koops, E.J. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities". In: *Reforming European Data Protection Law. Law, Governance and Technology Series*, vol 20. Edited by Serge Gutwirth, Ronald Leenes, and Paul de Hert, 3-33. Dordrecht: Springer, 2015.

Brayne, S., Rosenblat, A., and Boyd, D. "Predictive Policing". Data & Civil Rights: a new era of policing and justice. October 27, 2015. https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf.

Brewczyńska, M. (2022). A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation. *In: E. Kosta, R. Leenes, & I. Kamara (Eds.), Research handbook on EU data protection law* (pp. 91-114). (Research Handbooks in European Law series). Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781800371682.00013.

Brkan, M. and Bonnet, G., Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. European *Journal of Risk Regulation*, 11 (2019), pp. 18–50 doi:10.1017/err.2020.10.

Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International journal of law and information technology*, 27(2), 91-121. doi: 10.1093/ijlit/eay017.

Broeders, Schrijvers, Hirsch Ballin, WRR-Policy Brief: Big Data and Security Policies: Serving Security, Protecting Freedom, The Hague 2017, https://www.wrr.nl/publicaties/policy-briefs/2017/01/31/big-data-and-security-policies-serving-security-protecting-freedom.

Burrell, J. "How the machine 'thinks': Understanding opacity in machine learning algorithms". *Big Data & Society*, 3 no. 1 (June 2016): 1-12. https://doi.org/10.1177/2053951715622512.

Bygrave, L., Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling'(2001). *Computer Law & Security Report*, 17.

Bygrave, L., *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International: The Hague/London/New York 2002) 2.

Bygrave, L., Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions. University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2020-35. [Version 1.1; final version to be published in Ienca et al. (Eds.), Cambridge Handbook of Life Sciences, Information Technology and Human Rights (forthcoming)].

Bygrave, L., "Core principles of data protection" (2001) 7(9) *Privacy Law and Policy Reporter* 169.

Bygrave, The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review*, October 2020, https://doi.org/10.1016/j.clsr.2020.105460.

Calders T. & Verwer S. "Three naive Bayes approaches for discrimination-free classification." *Data Mining and Knowledge Discovery* 21, no. 2 (2010): 277-292.

Calders T. & Žliobaitė I.. "Why unbiased computational processes can lead to discriminative decision procedures." In: *Discrimination and privacy in the information society*, pp. 43-57. Springer, Berlin, Heidelberg, 2013.

Citron, D.K. (2008) 'Technological Due Process', *Washington University Law Review* 85: 1249-1313.

Citron, D.K. and Pasquale F. "The Scored Society: Due Process for Automated Predictions". *Washington Law Review* 89, no. 1 (March 2014): 1-34.

Clarke, R., Introduction to Dataveillance and Information Privacy, and Definitions of Terms (1997, revised 2016), <http://www.rogerclarke.com/DV/Intro.html>.

Clarke, R. "Profiling: A Hidden Challenge to the Regulation of Data Surveillance". *Journal of Law, Information and Science* 4, no. 2 (1993): 403-419.

Clifford, D., & Ausloos, J., Data Protection and the Role of Fairness, *Yearbook of European Law*, Vol. 37, No. 1 (2018), pp. 130–187, doi:10.1093/yel/yey004.

Cocx, T. *Algorithmic tools for data-oriented law enforcement (diss.)*. Leiden: University of Leiden, 2009, ISBN 9789090248059.

Corea, F. *An Introduction to Data: Everything You Need to Know About AI, Big Data and Data Science*. Springer, 2019.

Corstens, G. J. M., & Borgers, M. J. (2014). *Het Nederlands strafprocesrecht* (8th edition).

Corstens, G.J.M., & Borgers, M.J., *Het Nederlands strafprocesrecht*, Kluwer, Deventer 2011.

Crawford, K., & Schultz, J., Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, vol. 55, issue 1, *Boston College Law Review* 2014.

Crenshaw, K., 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics' (1989) *University of Chicago Legal Forum* 139 at 166–7.

Cukier, K. & V. Mayer-Schönberger, V., The Rise of Big Data: How It's Changing the Way We Think About the World, *Foreign Affairs*, Vol. 92, No. 3 (2013), p. 29.

Custers B.H.M. (2004), *The Power of Knowledge: Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Tilburg: Wolf Legal Publishers, ISBN: 90-5850-085-3.

Custers, B.H.M., Data Mining and Group Profiling on the Internet (2001). Custers B.H.M. (2001), Data Mining and Group Profiling on the Internet. In: *Vedder A (red.) Ethics and the Internet*. Antwerpen: Intersentia. 87-104, 2001.

Custers, B.H.M., Risicogericht toezicht, profiling en Big Data, *Tijdschrift voor Toezicht* 2014 (5) 3.

Custers, B.H.M., 'Effects of Unreliable Group Profiling by Means of Data Mining' in: *G Grieser, Y Tanaka and A Yamamoto (eds), Lecture Notes in Artificial Intelligence*, Proceedings of the 6th International Conference on Discovery Science (DS 2003) Sapporo, Japan vol 2843 (Springer 2003) 290-295.

Custers, B.H.M., Risk Profiling of Money Laundering and Terrorism Funding; Practical Problems of Current Information Strategies. In: *Proceedings of the 9th International Conference on Enterprise Information Systems* 2007.

Custers, B.H.M., "Data Dilemmas in the Information Society: Introduction and Overview". In:

Custers, Bart. "Data mining and Profiling in Big Data". In: *The SAGE Encyclopedia of Surveillance, Security and Privacy*, edited by Bruce A. Arrigo, 277-279. Thousand Oaks, California: Sage Publications, 2018.

Dalla Corte, L., On proportionality in the data protection jurisprudence of the CJEU, *International Data Privacy Law*, 2022, Vol. 12, No. 4.

Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big data & society*, 4(2), 2053951717726554.

Das, A., & Schuilenburg, M. (2018). Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht. *Strafblad*, 2018(4), 19-26.

De Goede, N., De Graaf, B., Sentencing risk: Temporality and precaution in terrorism trials, *International Political Sociology* 7 (3), 313-331.

De Goede, M., Simon, S., and Hoijtink, M. "Performing preemption." *Security Dialogue* 45, no. 5 (2014): 411-422.

De Hert, P., & Lammerant, H., 'Predictive profiling and its legal limits: effectiveness gone forever?', in: B. van der Sloot, D. Broeders & E. Schrijvers (eds.), *Exploring the Boundaries of Big Data*, The Hague: WRR 2016.

De Hert P., & V. Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and analsyis', *Computers & Law Magazine of SCL* 2012, vol. 22, issue 6.

De Hert, P., & Sajfert, J. (2021). The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680.

De Hert, P., & Sajfert, J., Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review* 40 (2021),Available at SSRN 4016491.

De Hert, P; Huisman, W; Vis, W. Intelligence led policing ontleed, *Tijdschrift voor Criminologie*; The Hague Vol. 48, Iss. 4, (Dec 2005): 5.

De Hert, P., V., Papakonstantinou & C. Riehle, Data protection in the third pillar: cautious pessimism, in: *Martin, Maik (ed.), Crime, Rights and the EU: cautious pessimism*. Justice, London (2008).

De Jonge, D.N., & Janssen, S.L.J., 'Eindelijk toegang tot datasets. (Erg) langzaam maar zeker naar een nieuw normaal', *NJB* 2021, afl. 34, p. 2793-2799.

De Poorter, J., & Goossens, J., Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad* 2019/2777, p. 3305.

De Schutter, O., 'Three Models of Equality and European Anti-Discrimination Law' (2006) 57 *Northern Ireland Legal Quarterly* 1.

De Schutter, O., and J. Ringelheim. "Ethnic profiling: A rising challenge for European Human Rights law." *The Modern Law Review* 71, no. 3 (2008): 358-384.

De Terwangne, C., (2014) The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data, International Review of Law, *Computers & Technology*, 28:2, 118-130, DOI:10.1080/13600869.2013.801588.

De Vries, M., J. Bijlsma, A.R. Mackor, F. Bex, and G. Meynen. "AI-risicotaxatie: nieuwe kansen en risico's voor statistische voorspellingen van recidive." *Strafblad* 2021, no. 2 (2021): 58-66.

Diakopoulos N., 'Accountability in Algorithmic Decision Making', Communications of the ACM (Vol. 59, No 2, 2016).

Dimitrova, D., and P. De Hert. "The right of access under the police directive: small steps forward." In: *Annual Privacy Forum*, pp. 111-130. Springer, Cham, 2018.

Dinant, J., Lazaro, C., Poullet, Y., Lefever, N., Rouvroy, A.: Application of Convention 108 to the profiling mechanism Some ideas for the future work of the consultative committee, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-Pd) 24th meeting 13-14 March 2008 Strasbourg, G01 (TPD), Secretariat document prepared by the Council of Europe Directorate General of Human Rights and Legal Affairs, Strasbourg, 11 January 2008 T-PD(2008)01. Available at: https://rm.coe.int/16806840b9.

Domingos, P. (2015). *The master algorithm: How the quest for the ultimate learning machine will remake our world*. Basic Books.

Dressel, J., and Farid, H., The accuracy, fairness, and limits of predicting recidivism, *Science Advances* 2018;4: eaao5580 17 January 2018.

Eckes C, *EU Counter-Terrorist Policies and Fundamental Rights: The Case of Individual Sanctions* (OUP 2009).

EDPS, Opinion of the European Data Protection Supervisor 2009/C 276/02.

Edwards L. and Veale M., "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, vol 16, issue 1.

Edwards, L., Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective, 1 *European Data Protection Law Review* 28, 28–58 (2016).

Eeden, C.A.J. van den, Berkel, J.J. van, Lankhaar, C.C., Poot, C.J. de, Opsporen, vervolgen en tegenhouden van cybercriminaliteit, WODC, Cahiers 2021-23, available at: http://hdl.handle.net/20.500.12832/3114.

Eklund, H. & Kilpatrick, C., Article 21 EU charter of fundamental rights, European University Institute: Academy of European Law, AEL working Paper 2021/01, ISSN 1831-4066, available at: https://hdl.handle.net/1814/71418.

Ensign, D., S. A. Friedler, S. Neville, C. Scheidegger, and S. Venkatasubramanian. 2017. Runaway Feedback Loops in Predictive Policing. Paper prepared for the first conference on Fairness, Accountability, and Transparency in Machine Learning, New York University, New York, February 2018. http://arxiv.org/abs/1706.09847.

EPDS, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019. Available at: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf.

Ericson, R.V., & Haggerty, E., *Policing the Risk Society*, Clarendon Press 1997.

European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, updated on 31 August 2021, available at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

European Court of Human Rights, Guide on Article 6 of the European Convention on Human Rights, available at: https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf.

European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law*. Luxembourg: Publications Office of the European Union, 2018. doi:10.2811/792676.

European Union Agency for Fundamental Rights, Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. Luxembourg: Publications Office of the European Union, 2010. doi:10.2811/40252.

Eurostat, 'Praktijkcode voor Europese statistieken: voor de nationale statistische autoriteiten en Eurostat', Comité voor het Europees statistisch systeem, 16 November 2017, available at: https://ec.europa.eu/eurostat/documents/4031688/9394211/KS-02-18-142-NL-N.pdf/580e523c-85a4-406d-9ad2-9a78f5820fc6.

Fayyad U., Piatetsky-Shapiro G., Smyth P. (1996) From Data Mining to Knowledge Discovery: an Overview, *In Fayyad U, Piatetsky-Shapiro G, Smyth P, Uthurusamy R. (eds) Advances in Knowledge Discovery and Data Mining*. AAAI Press / MIT Press, Cambridge.

Feeley, M. M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, 30(4), 449-474.

Ferguson, A. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.

Ferguson, A.G., 'Policing Predictive Policing' (2017) 94 *Wash U L Rev* 1109.

Ferraris et al., *Working Paper Defining profiling*, PROFILING, UNICRI, available at: http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf.

Ferraris, V., Bosco, F., Cafiero, G., D'Angelo, E., & Suloyeva, Y. (2013). Defining profiling. Available at SSRN 2366564.

Ferrer, X., Van Nuenen, T., Such, J.M., Coté, M., and Criado, N., "Bias and Discrimination in AI: A Cross-Disciplinary Perspective," in *IEEE Technology and Society Magazine*, vol. 40, no. 2, pp. 72-80, June 2021, doi: 10.1109/MTS.2021.3056293.

Finck, M., & Biega, A. J. (2021). Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. *Technology and Regulation*, 2021.

Flores, A.W., Bechtel, K., Lowenkamp, C.T., "False Positives, False Negatives, and False Analyses: A Rejoinder to Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks," *Federal Probation* 80, no. 2 (September 2016): 38-46.

Foqué, R., & Hart, A.C., *Instrumentaliteit en rechtsbescherming*, Gouda Quint-Kluwer Rechtswetenschappen, Arnhem-Antwerpen 1990.

Fox, E. W. (2015). Estimation and Inference for Self-Exciting Point Processes with Applications to Social Networks and Earthquake Seismology. *UCLA*. ProQuest ID: Fox_ucla_0031D_13456. Merritt ID: ark:/13030/m5md16wm. Available at https://escholarship.org/uc/item/5cm7g4jp.

Frase, R.S., 'What Explains Persistent Racial Disproportionality in Minnesota's Prison and Jail Populations?', *Crime and Justice: A Review of Research* 2009, p. 201-280.

Fredman, S., 'Double Trouble: Multiple Discrimination and EU Law' (2005) 2 *European Anti- Discrimination Law Review* 13 at 16.

Fredman, S., 'Emerging from the Shadows: Substantive Equality and Article 14 of the European Convention on Human Rights' (2016) Vol. 16 *Human Rights Law Review* 273.

Fredman, S., 'Providing Equality: Substantive Equality and the Positive Duty to Provide' (2005) 21 *South African Journal on Human Rights* 163.

Fredman, S., *Discrimination Law*, Oxford University Press, 2011. 9780199584437.

Fredman, S., Substantive equality revisited, *International Journal of Constitutional Law*, Volume 14, Issue 3, July 2016, Pages 712–738, https://doi.org/10.1093/icon/mow043.

Friedler, S.A., C. Scheidegger, S. Venkatasubramanian, S. Choudhary, E.P. Hamilton, and D. Roth. 2018. A Comparative Study of Fairness-Enhancing Interventions in Machine Learning. FAT*19 Proceedings of the Conference on Fairness, Accountability and Transparency, 329-338. Atlanta, GA. January 29-31, 2018. http://arxiv.org/abs/1802.04422.

Friedman, B and Nissenbaum, H (1996) 'Bias in Computer Systems', *ACM Transactions on Information Systems* 14(3), p. 330-347.

Fuster G., Gutwirth S., Erika E. (June 2010), Profiling in the European Union: A high-risk practice. INEX Policy Brief, no. 10.

Galič, M. (2022), 'Bulkbevoegdheden en strafrechtelijk onderzoek: wat de jurisprudentie van het EHRM ons kan leren over de normering van grootschalige data-analyse', *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 8(2), p. 130-137.

Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, 40, 1-13. [105486]. https://doi.org/10.1016/j.clsr.2020.105486.

Galič, M., 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BSb* 2021/2.

Gellert, R. (2017). Understanding the risk based approach to data protection: An analysis of the links between law, regulation, and risk. [Doctoral Thesis, Vrije Universiteit Brussel – LSTS].

Gellert, R., de Vries, K., de Hert, P., Gutwirth, S. (2013). A Comparative Analysis of Anti-Discrimination and Data Protection Legislations. In: *Custers, B., Calders, T., Schermer, B., Zarsky, T. (eds) Discrimination and Privacy in the Information Society*. Studies in Applied Philosophy, Epistemology and Rational Ethics, vol 3. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-30487-3_4.

Geraghty, K.A., Woodhams, J., The predictive validity of risk assessment tools for female offenders: A systematic review. *Aggress. Violent Behav*. 21, 25 (2015).

Gerards J. & R. Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law. European Commission, Luxembourg: Publications Office of the European Union, 2021.

Gerards, J. H. (2005). Art. 14 Discriminatieverbod. In: *A. W. Heringa, J. Schokkenbroek, & V. der J. Velde (Eds.), EVRM Rechtspraak en Commentaar*. SDU uitgevers BV. Retrieved from https://hdl.handle.net/1887/3913.

Gerards, J., 'The Discrimination Grounds of Article 14 of the European Convention on Human Rights' (2013) 13 *Human Rights Law Review* 99.

Gerards, J., Pluralism, Deference and the Margin of Appreciation Doctrine, 17 *Eur. L.J.* 80, 102 (2011).

González Fuster, G., 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights', European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 656.295, 2020.

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

Goodman B. and S. Flaxman, European Union Regulations on Algorithmic Decision-making and a "Right to Explanation", *AI magazine*, 38(3), 50-57, arXiv:1606.08813.

Goodman, B., 'A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection', 2016, 29th conference on neural information processing systems (NIPS 2016), Barcelona. NIPS foundation.

Graef, I., Clifford, D., and Valcke, P., Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, 2018, Vol. 8, No. 3.

Greenawalt, K., 'How Empty is the Idea of Equality?' (1983) 83 *Columbia Law Review* 1167.

Groenhart, Lexplicatie, commentaar op regeling Besluit politiegegevens.

Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 8 Wpg (1 July 2022).

Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 9 Wpg (1 July 2022).

Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 10 Wpg (1 July 2022).

Groenhart, T&C Privacy- en gegevensbeschermingsrecht, commentaar op art. 11 Wpg (1 July 2022).

Groenhuijsen, M. S., & Knigge, G. (Eds.) (2001). Het vooronderzoek in strafzaken. Tweede interimrapport onderzoeksproject Strafvordering 2001. Gouda Quint.

Gutwirth, S., and De Hert, P., "Regulating profiling in a democratic constitutional state." *In: Profiling the European citizen*, pp. 271-302. Springer, Dordrecht, 2008.

Gutwirth, S. and De Hert, P. (2007). "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power." In: *Erik Claes, Antony Duff, and Serge Gutwirth., eds., Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia. pp. 61-104.

Hannett, S., 'Equality at the Intersections: The Legislative and Judicial Failure to Tackle Multiple Discrimination' (2003) 23 *Oxford Journal of Legal Studies* 65 at 69–70.

Harcourt B.E., 'Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally', 71.4 *University of Chicago Law Review* (2004).

Harcourt, B.E., *Against Prediction Profiling, Policing, and Punishing in an Actuarial Age*, The University of Chicago Press 2007.

Harcourt, B.E., Muslim profiles post-9/11: Is racial profiling an effective counter-terrorist measure and does it violate the right to be free from discrimination? In: *Goold BJ and Lazarus L (eds) Security and Human Rights*. Oxford and Portland, OR: Hart Publishing, 2017, pp. 73–98.

Harcourt, B.E., Risk as a proxy for race. John M. Olin Law & Economics Working Paper no. 535, (2d series), Public Law and Legal Theory Working Paper no. 323, September 2001. Available at: https://ssrn.com/abstract=1677654.

Harris, D.A., *Profiles in Injustice - Why Racial Profiling Cannot Work* (New York: The New Press, 2002) 16-18.

Helderman, J., & Honingh, M.E., Systeemtoezicht. Een onderzoek naar de condities en werking van systeemtoezicht in zes sectoren, Den Haag: WODC 2009.

Hildebrandt & Gutwirth, General Introduction and Overview. *In: M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

Hildebrandt M. (2006), Profiling: from Data to Knowledge. The challenges of a crucial technology, in DuD *Datenschutz und Datensicherheit*, 30(9), pp. 548-552.

Hildebrandt M., Backhouse J. (2005), Descriptive analysis and inventory of profiling practices. In FIDIS Project Deliverable 7.2., available at: http://www.fidis.net.

Hildebrandt, M. "Discrimination, Data-driven AI Systems and Practical Reason." *European Data Protection Law Review* 7 (2021): 358-366.

Hildebrandt, M. (2009). Who is profiling who? Invisible visibility. In *Reinventing data protection?* (pp. 239-252). Springer, Dordrecht.

Hildebrandt, M., & Koops, E.J., The Challenges of Ambient Law and Legal Protection in the Profiling Era, (2010) *Modern Law Review* 73(3) 428-460.

Hildebrandt, M., 'The Dawn of a Critical Transparency Right for the Profiling Era', p. 56, 2012, In: Bus, J. (ed.), *Digital Enlightenment Yearbook* 2012, pp. 41-56, available at: https://repository.ubn.ru.nl/handle/2066/94126.

Hildebrandt, M., Data-Driven Prediction of Judgment. Law's New Mode of Existence? (2019). OUP Collected Courses Volume EUI Summer-school, 2019. Available at: http://dx.doi.org/10.2139/ssrn.3548504.

Hildebrandt, M., Defining Profiling: A New Type of Knowledge?. In: *Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth*, Springer 2008.

Hildebrandt, M., *Smart technologies and the end(s) of law: novel entanglements of law and technology* (Edward Elgar 2015).

Hildebrandt, M., and S. Gutwirth. *Profiling the European citizen*. Dordrecht: Springer, 2008.

Hildebrandt, M.. "Profiles and correlatable humans." *Who Owns Knowledge? Knowledge and the Law* (2008): 265-84.

Hildebrandt, M., Profiling and AmI. *In: K. Rannenberg, D. Royer, A. Deuker, The Future of Identity in the Information Society. Challenges and Opportunities*. Springer 2009.

Hill, R.K., 'What an algorithm is', *Philosophy and Technology* 2015, 29, 1.

Hirsch Ballin, E. (2020). *Advanced introduction to legal research methods*. Elgar Advanced Introductions, p. 55-57.

Hirsch Ballin, M. F. H. (2012). Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States. T.M.C. Asser Press / Springer.

Hirsch Ballin, M., & Galič, M. (2021). Digital investigation powers and privacy: Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure. *Boom Strafblad*, 2(4).

Hirsch Ballin, M.F.H. & Oerlemans, J.J., 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijke optreden', *DD* 2023/2.

Hoboken, J. van (2016) 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and U.S. Frameworks for Personal Data Processing', pp. 231-259 in: *B. van der Sloot, D. Broeders and E. Schrijvers (eds.) Exploring the Boundaries of Big Data*, WRR-Verkenning 32, Amsterdam: Amsterdam University Press.

Hudson, B. (2005) Secrets of Self: Punishment and the Right to Privacy, in: E. *Claes & A. Duff (Eds) Privacy and the Criminal Law* (Antwerp Oxford, Intersentia).

Hustinx, P., "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", available at: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en.

Jaquet-Chiffelle, D.O., Direct and Indirect Profiling in the Light of Virtual Persons, p. 40. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives.* Springer 2008.

Jasserand, C., Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, *Computer Law & Security Review*, Volume 34, Issue 1, 2018, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.08.002.

Jefferson, B.J. 2017. Digitize and Punish: Computerized Crime Mapping and Racialized Carceral Power in Chicago. Environment and Planning D: Society and Space 35 (5): 775–96; Lum, Kristian, and William Isaac. 2016. To Predict and Serve? *Significance* 13 (5): 14–19.

Joh, E., Feeding the Machine: Policing, Crime Data, & Algorithms, *William & Mary bill of rights journal*, Vol. 26:287.

Kamarinou, D. and Millard, C. and Singh, J., Machine Learning with Personal Data (November 7, 2016). *Queen Mary School of Law Legal Studies Research Paper* No. 247/2016, Available at SSRN: https://ssrn.com/abstract=2865811.

Kaminski M., and Malgieri, G., Multi-layered Explanations from Algorithmic Impact Assessments in the GDPR, ACM, ISBN 978-1-4503-6936-7/20/02, https://doi.org/10.1145/3351095.3372875.

Kaminski, M., The Right to Explanation, Explained. U of Colorado Law Legal Studies Research Paper No. 18-24, *Berkeley Technology Law Journal*, Vol. 34, No. 1, 2019, Available at SSRN: https://ssrn.com/abstract=3196985.

Kamiran, F., & Žliobaitė, I. (2013). Explainable and non-explainable discrimination in classification. In: *Discrimination and Privacy in the Information Society* (pp. 155-170). Springer, Berlin, Heidelberg.

Kantardzic, M. (2011). *Data mining: concepts, models, methods, and algorithms*. John Wiley & Sons.

Kemshall, H., *Understanding risk in criminal justice*, Crime and Justice Series, Open University Press UK, 2003.

Kestemont, L. (2018). *Handbook on legal methodology: from objective to method*. Intersentia.

Kierkegaard et al., 30 years on – The review of the Council of Europe Data Protection Convention 108, *Computer Law & Security Review* 27 (2011) 223-231.

Kilpatrick, C. "Non-Discrimination." In: *The EU Charter of Fundamental Rights: A Commentary*. Ed. Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward. London: Hart Publishing, 2014. 579–604. Bloomsbury Collections. Web. 24 Jul. 2018. <http://dx.doi.org/10.5040/9781849468350.ch-024>.

Kimber, C.J.M., 'Equality or Self-Determination', in: *Gearty and Tomkins (eds), Understanding Human Rights* (London: Mansell, 1996) 266.

Kitchin, R., (2013) 'Big Data and human geography: Opportunities, challenges and risks', *Dialogues in Human Geography*, 3(3), p. 262-267.

Kleinberg, J., Mullainathan, S., & Raghavan, M. (2016). Inherent trade-offs in the fair determination of risk scores. arXiv preprint arXiv:1609.05807.

Koops Committee, Regulering van opsporingsbevoegdheden in een digitale omgeving (Commissie modernisering opsporingsonderzoek in het digitale tijdperk), June 2018.

Koops, E.J. (2013) 'On decision transparency, or how to enhance data protection after the computational turn', pp. 196-220 in: *M. Hildebrandt and K. de Vries (eds.) Privacy, due process and the computational turn*, Abingdon: Routledge.

Koops, E.J., Criminal investigation and privacy in Dutch law, TILT Law & Technology Working Paper Series, version 1.0, September 2016, available at http://ssrn.com/abstract=2837483.

Koops, E.J., Newell, B.C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M., 'A Typology of Privacy' (2017) 38 *U Pa J Int'l L* 483.

Koops, E.J., Technology and the Crime Society: Rethinking Legal Protection, (2009) 1 *Law Innovation and Technology*, p. 93-124.

Koops, E.J., The trouble with European data protection law, *International Data Privacy Law*, Volume 4, Issue 4, November 2014, available at: https://doi.org/10.1093/idpl/ipu023.

Koops, E.J., Some Reflections on Profiling, Power Shifts and Protection Paradigms, p. 326-337. In: *M. Hildebrandt & S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer 2008.

Kosta, E., Coudert, F., Dumortier, J., Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive, (2007) *International Review of Law Computers & Technology*, volume 21, no. 3.

Kosta, E., Surveilling Masses and Unveiling Human Rights - Uneasy Choices for the Strasbourg Court, Tilburg Law School Research Paper No. 2018-10, Available at SSRN: https://ssrn.com/abstract=3167723.

Kranzberg, M. (1986) Technology and History: 'Kranzberg's Laws', *Technology and Culture*, 27, pp. 544-560.

Kuiper, R. (2014). *Vormfouten, juridische consequenties van vormverzuimen in strafzaken*, dissertatie Radboud Universiteit Nijmegen.

Kuner, C., Svantesson, D.J.B., Cate, F.H., Lynskey, O., and Millard, C., Machine learning with personal data: is data protection law smart enough to meet the challenge? *International Data Privacy Law*, 2017, Vol. 7, No. 1.

Le Métayer, D., Le Clainche, J. (2012). From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles. In: *Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (eds) European Data Protection: In Good Health?* Springer, Dordrecht. https://doi.org/10.1007/978-94-007-2903-2_15.

Leese, M., The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue* 2014, Vol. 45(5) 494–511. https://doi.org/10.1177/0967010614544204.

Leiser, M. and Custers, B., The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, *European Data Protection Law Review* 2019, Vol. 5, nr. 3, doi:10.21552/edpl/2019/3/10.

Lepri, B., Oliver, N., Letouz, E., Pentland, A., Vinck, P., Fair, Transparent, and Accountable Algorithmic Decision-making Processes The Premise, the Proposed Solutions, and the Open Challenges. *Philos. Technol*. (2018) 31:611 –627. DOI 10.1007/s13347-017-0279-x.

Lessig, L. (1999a) *Code and other laws of cyberspace* (New York, Basic Books).

Lipton, Z. (2016) The Mythos of Model Interpretability, ICML Workshop on Human Interpretability in Machine Learning. (WHI 2016), New York. Available from URL: https://arxiv.org/pdf/1606.03490.pdf.

Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), 162-176.

Lyon, D. "Sorting for Suspects." *Arena Magazine* 70 (2004): 26-28.

Maas, M., Legters, E., & Fazel, S., Professional en risicotaxatieinstrument hand in hand: Hoe de reclassering risico's inschat. *Nederlands Juristenblad*, 17 July 2020, issue. 28 pp. 2055-2600.

Malgieri G. and Comande G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, 2017, Vol. 7, No. 4.

Mali, C. Bronkhorst-Giesen, M. den Hengst, Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot. Politie Academie, February 2017, available at: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93263.PDF.

Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719895805.

Mantelero, A., 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in: *Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) https://doi.org/10.1007/978-3-319-46608-8_8.

Mantelero, A., Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, *Computer Law & Security Review*, Volume 32, Issue 2, April 2016, P. 238-255.

Marks, A., Bowling, B., & Keenan, C., Automatic justice? Technology, Crime and Social Control. In: *R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology*, OUP 2017.

Marquenie, T., The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security Review* 33 (2017) 324-340.

Marx G.T. & Reichman N. (1984) 'Routinising the Discovery of Secrets' *Am. Behav. Scientist* 27,4 (Mar/Apr 1984) 423-452.

Mayer-Schönberger, V., and Padova, Y., 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation' (2016) 17 *The Columbia Science and Technology Law Review* 315, 317.

McCrudden, C., and Prechal, S., 'The Concepts of Equality and Non-Discrimination Inn Europe: A Practical Approach' (2009) European Network of Legal Experts in the Field of Gender Equality 21.

McCulloch J. & Wilson D., *Pre-crime: Pre-emption, precaution and the future*. Routledge Frontiers of Criminal Justice, Routledge: New York 2017.

McGarry J, 'Named, Shamed, and Defamed by the Police' (2011) 5 *Policing* 219.

Mendoza, I., & Bygrave, L. A. (2017). The right not to be subject to automated decisions based on profiling. In *EU Internet Law* (pp. 77-98). Springer, Cham.

Mittelstadt et al., 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* (July–December 2016), pp. 1–21.

Mittelstadt, B, Allo, P, Taddeo, M, Wachter, S and Floridi, L (2016) 'The ethics of algorithms: Mapping the debate', *Big Data Society,* July-December, p. 1-21.

Mittelstadt, B. "From individual to group privacy in big data analytics." *Philosophy & Technology* 30, no. 4 (2017): 475-494. https://doi.org/10.1007/s13347-017-0253-7.

Moeckli et al (eds.) *International Human Rights Law*, Oxford University Press 2018, 0198767234.

Moeckli, D., 'Discrimination Profiles: Law Enforcement After 9/11 and 7/7' (2005) 5 *European Human Rights Law Review* 517.

Moeckli, D., 'Terrorist profiling and the importance of a proactive approach to human rights protection' (16 December 2006), available at the Social Science Research Network (SSRN): http://ssrn.com/abstract=952163.

Moerel, E.M.L. and Prins, J.E.J., Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016). Available at: http://dx.doi.org/10.2139/ssrn.2784123.

Mohler, G.O., et al., 2011. Self-exciting point process modeling of crime. *Journal of the American statistical association*, 106 (493), 100–108. doi: 10.1198/jasa.2011.ap09546.

Muir, E. "The Added Value of the EU Charter of Fundamental Rights: at the Intersection of Legal Systems." Jean Monnet Working Paper 15/20, (2020).

Muir, E. "The Essence of the Fundamental Right to Equal Treatment: Back to the Origins." *German Law Journal* 20, no. 6 (2019): 817-839.

Nan, J. S., Bektesevic, D. (2017), Structurele vormverzuimen: een structureel probleem?, in: DD 2017/22.

Naudts, L. (2019). Criminal Profiling and Non-Discrimination: On Firm Grounds for the Digital Era?. Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. Cambridge, Antwerp, Chicago: Intersentia, 63-96.

Naudts, L., 'How Machine Learning Generates Unfair Inequalities and How Data Protection Instruments May Help in Mitigating Them', in: *Ronald Leenes and others (eds) in, Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2019) ch 3.

Neuvonen, PJ. "'Inequality in equality'in the European Union equality directives: A friend or a foe of more systematized relationships between the protected grounds?." *International Journal of Discrimination and the Law* 15, no. 4 (2015): 222-240.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 79, 119.

Nissenbaum, H. (2020). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

O' Neil C., *Weapons of Math Destruction*, Crown publishers 2016, ISBN 0553418815.

O'Connell, R., 'Cinderella comes to the Ball: Art 14 and the right to non-discrimination in the ECHR' (2009) 29 *Legal Studies* 211 at 228.

O'Cinneide, C. "The uncertain foundations of contemporary anti-discrimination law." *International Journal of Discrimination and the Law* 11, no. 1-2 (2011): 7-28.

Oerlemans, J.J., *Investigating cybercrime* (Dissertation) 2017, ISBN 9789085551096.

Oerlemans, J. J. (2017). *Normering van digitale opsporingsmethoden*. Nederlandse Defensie Academie, ISBN 9789088920691.

Oerlemans, J. J., & Wegberg, R. S. van. (2019). Opsporing en bestrijding van online drugsmarkten. *Strafblad*, 17(5), 25-31. Retrieved from https://hdl.handle.net/1887/83008.

Oerlemans, J.J., & van Toor, D.A.G. (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective, *European Journal of Crime, Criminal Law and Criminal Justice*, 30(3-4). doi: https://doi.org/10.1163/15718174-bja10037.

Oerlemans, J-J., & Galič, M. (2021). Cybercrime investigations. In *W. Van der Wagen, J-J. Oerlemans, & M. Weulen Kranenbarg (Eds.), Essentials in cybercrime: A criminological overview for education and practice* (pp. 197-254). Eleven Publishers / Boom Juridische Uitgevers.

Oswald M., Grace, J., Urwin, S., & Barnes, G.C., (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, 27:2, 223-250, DOI: 10.1080/13600834.2018.1458455.

Packer, H., *The Limits of the Criminal Sanction*, Stanford University Press 1968.

Pap L.A., 'Profiling, Data Mining and Law Enforcement: Definitions' (2009) 50 *Annales U Sci Budapestinensis Rolando Eotvos Nominatae* 277.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Polson N. and J. Scott, *AIQ: How Artificial Intelligence Works and How We Can Harness its Power for a Better World* (London: Bantam Press, 2018).

Prins, J.E.J., & Moerel, L. (2015). On the death of the purpose limitation principle. International Association of Privacy Professionals. Available at: https://privacyassociation.org/news/a/on-the-death-of-purpose-limitation/.

Prins, J.E.J., & Roest, J. (2018). AI en de rechtspraak: Meer dan alleen de 'robotrechter'. *Nederlands Juristenblad*. 93(4), 260-268.

Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie*, The Hague, September 2022, available at: https://www.hogeraad.nl/publish/pages/738/onderzoek_in_een_geautomatiseerd_werk_2022_.pdf.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40-81. https://doi.org/10.1080/17579961.2018.1452176.

Quintel, T. "Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive." *Eur. Data Prot. L. Rev.* 4 (2018): 104.

Reichman, N., Managing crime risk: towards an insurance based model of social control, *Research in Law and Social Control* 8: 151-72, 1986.

Richards, N.M. en H.J. King (2013) 'Three paradoxes of Big Data', *Stanford Law Review Online* 41, Available at: http://ssrn.com/abstract=2325537.

Richardson, R., ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force," AI Now Institute, December 4, 2019, https://ainowinstitute.org/ads-shadowreport-2019.html.

Richardson, R. and Schultz, J. and Crawford, K., Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (February 13, 2019). 94 *N.Y.U. L. REV. ONLINE* 192 (2019). Available at SSRN: https://ssrn.com/abstract=3333423.

Rinik, C., Oswald, M., & Babuta, A. (2019). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges.

Robinson D (2017) The Challenges of Prediction: Lessons from Criminal Justice. I/S: A *Journal of Law and Policy for the Information Society*. https://ssrn.com/abstract=3054115. Last accessed 30 September 2018.

Roig, A., Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR), *European Journal of Law and Technology* Vol 8, No 3 (2017).

Rubinstein, I., 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, 2013.

Rubinstein, I., Lee, R., Schwartz, P., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, *The University of Chicago Law Review* (75) 2008, p. 261.

Sajfert J. & Quintel T., The Law Enforcement Directive, in: *Cole & Boehm, GDPR Commentary*, Edward Elgar Publishing 2019.

Samadi, M. (2020), *Normering en toezicht in de opsporing: Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen*, dissertatie Universiteit Leiden.

Savin, A., Profiling in the Present and New EU Data Protection Frameworks (December 1, 2015). In: Nielsen, P.A., Schmidt, P.K., Dyppel Weber, K. (eds.) Erhvervsretlige emne, Juridisk Institut CBS (Djøf 2015) ISBN 978-87-574-3524-5. Available at SSRN: https://ssrn.com/abstract=2697531.

Schakel, R. Rienks and R. Ruissen, Knowledge-Based Policing: Augmenting Reality with Respect for Privacy. In: *B. Custers, T. Calders, B. Schermer, T. Zarsky (eds.), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Springer 2013.

Schauer, F., 2003. *Profiles, probabilities and stereotypes*. Cambridge, MA: Harvard University Press.

Schermer, B. W. (2017). Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, *Tijdschrift voor Bijzonder Strafrecht & Handhaving* (4).

Schermer, B. W. (2022). De gespannen relatie tussen privacy en cybercrime. Inaugural lecture, Universiteit Leiden, 7 November 2022. Retrieved from https://hdl.handle.net/1887/3484256.

Schermer, B. W., & Galič, M. (2022). Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen? *Nederlands Tijdschrift voor Strafrecht*, 3(3), 167-177. [2022/38], https://doi.org/10.5553/NTS/266665532022003003006.

Schermer, B. W., & Oerlemans, J. J. (2020). AI, strafrecht en het recht op een eerlijk proces. *Computerrecht*, 2020(3).

Schermer, B. W., & Oerlemans, J. J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022/02.

Schermer, B., The limits of privacy in automated profiling and data mining, *Computer Law & Security Review* 27 (2011) 45-52.

Schiek, D. and Lawson, A. (eds), EU Non-Discrimination Law and Intersectionality—Investigating the Triangle between Racial, Gender and Disability Discrimination (Aldershot, Ashgate, 2011).

Schreurs, W., Hildebrandt, M., Kindt, E., Vanfleteren, M. (2008). Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In: *Hildebrandt, M., Gutwirth, S. (eds) Profiling the European Citizen*. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-6914-7_13.

Schuilenburg, M. "Predictive policing: de opkomst van een gedachtenpolitie." *Ars Aequi* 65, no. 12 (2016): 931-936.

Seawright, J., & Gerring, J., Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options, *Political Research Quarterly* 2008 61:294.

Selbst A, Barocas S (2017) Regulating Inscrutable Systems. Available at: http://www.werobot2017.com/wp-content/uploads/2017/03/Selbst-and-Barocas-Regulating-Inscrutable-Systems-1.pdf.

Selbst A. and Powles J., Meaningful information and the right to explanation. *International Data Privacy Law*, 2017, Vol. 7, No. 4.

Selbst, A., et al., 2019. Fairness and Abstraction in Sociotechnical Systems. In FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19), January 29–31, 2019, Atlanta, GA, USA. ACM, New York, NY, USA. https://doi.org/10.1145/3287560.3287598.

Seyyar, M. B., & Geradts, Z. J. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, 33, 200906.

Shapiro, A. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17(3/4): 456-472. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487.

Sheehey, B. Algorithmic paranoia: the temporal governmentality of predictive policing. *Ethics Inf Technol* 21, 49–58 (2019). https://doi.org/10.1007/s10676-018-9489-x.

Slobogin, C. Principles of Risk Assessment: Sentencing and Policing (February 27, 2018). *Ohio State Journal of Criminal Law*, Vol. 15, 2018; Vanderbilt Law Research Paper No. 18-09. Available at SSRN: https://ssrn.com/abstract=3131027.

Small, J. 'Structure and Substance: Developing a Practical and Effective Prohibition on Discrimination under the European Convention on Human Rights' (2003) 6 *International Journal of Discrimination and the Law* 45.

Smits, J. M. (2012). *The mind and method of the legal academic*. Edward Elgar Publishing.

Solanke, I., 'Putting Race and Gender Together: A New Approach to Intersectionality' (2009) 72 *Modern Law Review* 723; Timmer, 'Toward an Anti-Stereotyping Approach for the European Court of Human Rights' (2011) 11 *Human Rights Law Review* 707.

Solove D, 'Data Mining and the Security–Liberty Debate' (2008) 75 *University of Chicago Law Review* 343.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44, 745.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

Stevens, L., Hirsch Ballin, M., Galic, M., Buisman, S., Groothoff, B., Hamelzky, Y., & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2021(4), 234-245.

Strandburg, K. (2014). Monitoring, datafication and consent: legal approaches to privacy in the big data context. In: *Lane, J., Stodden, V., Bender, S., Nissenbaum, H. (Eds.). (2014). Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge University Press.

Swedloff, R., Risk Classification's Big Data (R)evolution (2014). Connecticut Insurance Law Journal, Vol. 21, 2014. Available at SSRN: https://ssrn.com/abstract=2566594.

Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer.

Taylor, L., Leenes, R., & van Schendel, S. (2017). *Public sector data ethics: From principles to practice*. Tilburg: Tilburg University.

Ten Brink, L.T., Waakzaam tussen wijk en wereld: Nationaal Intelligence Model Sturen op en met informatie, available at: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/69628.pdf.

Tene, O. en J. Polonetsky (2012) 'Privacy in the age of Big Data: A time for big decisions', *Stanford Law Review Online* 64.

Tene, O., and Polonetsky, J., Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239 (2013).

Tijssen, H., *De juridische dissertatie onder de loep*, The Hague, Boom juridische uitgevers 2009.

Timmer, A., 'Toward an Anti-Stereotyping Approach for the European Court of Human Rights' (2011) 11 *Human Rights Law Review* 707.

Tzanou, M., Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, No. 2.

Ukrow, J., "Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention 108," *European Data Protection Law Review* (EDPL) 4, no. 2 (2018): 239-247.

United Nations Special rapporteur on extreme poverty and human rights, Report of 11 October 2019, A/74/48037. Available at: https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx.

United Nations Special Rapporteur on extreme poverty and human rights, Brief as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/HA ZA 18/388), available at: https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.

Van Bekkum M. & Zuiderveen Borgesius F., Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? (2022), available at: arXiv:2206.03262.

Van Brakel, B., & De Hert, P., Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies* 2011-3, no. 20, Maklu, ISBN 978-90-466-0412-0.

Van Brakel, R. Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing (April 28, 2016). pp. in 117-141 in: *van der Sloot, B. et al (ed.) (2016) Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press.

Van Brakel, R., and P. De Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies." *Technol. Led Policing* 20 (2011).

Van der Auwera, J., & Van de Velde, L. (2021). Risicoprofiling of risicovolle profiling tijdens grenscontroles? Naar een verantwoord gebruik van proactieve risicoprofielen door rechtshandhavingsinstanties. *Tijdschrift voor Veiligheid*, 20(3), 1-17.

Van der Leun, J. P., & van der Woude, M. A. (2011). Ethnic profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profiling and a changing social and political context. *Policing and society*, 21(4), 444-455.

Van der Meij, Commentaar op artikel 132a Sv, Opsporingsonderzoek (T&C Strafvordering) (online).

van der Sloot, B. (2012). From Data Minimization to Data Minimummization. In B. Custers, T. Calders, B. Schermer & T. Zarsky (eds.), 'Discrimination and Privacy in the Information Society', Springer, Heidelberg 2012, p. 273-287.

Van der Sloot, B. (2016) 'The Individual in the Big Data Era: Moving towards an Agent based Privacy Paradigm', pp. 177- 203 in: *B. van der Sloot, D. Broeders and E. Schrijvers (eds.) Exploring the Boundaries of Big Data*, WRR-Verkenning 32, Amsterdam: Amsterdam University Press.

Van der Sloot, B. (2016). The Practical and Theoretical Problems with 'Balancing'. Delfi, Coty and the Redundancy of the Human Rights Framework. *Maastricht Journal of European and Comparative Law*, 23(3), 439-459.

van der Sloot, B., & van Schendel, S. (2019). De juridische randvoorwaarden voor een datagedreven samenleving. *Nederlands Juristenblad*, 2019(44), 3302.

van der Sloot, B., & van Schendel, S. Tien voorstellen voor aanpassingen aan het Nederlands procesrecht in het licht van Big Data. *Computerrecht*, 2020(1), 4-13.

Van der Sloot, B., & Van Schendel, S., De modernisering van het Nederlands procesrecht in het licht van big data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving. WODC/Tilburg Univeristy, 2019, Tilburg.

Van der Sloot, B., & Van Schendel, S., *International and Comparative Study on Big Data*, Working Paper no. 20, Dutch Scientific Council for Government Policy (WRR) 2016.

Van der Sloot, B., (2017). Where is the Harm in a Privacy Violations? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(4).

Van der Sloot, B., (2021) The right to be let alone by oneself: narrative and identity in a data-driven environment, *Law, Innovation and Technology*, 13:1, 223-255, DOI: 10.1080/17579961.2021.1898315.

Van der Sloot, B., 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities', In: *S. Gutwirth, R. Leenes & P. De Hert (eds.), 'Data Protection on the Move'*, Springer, Dordrecht, 2016.

Van der Sloot, B., Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under Article 8 ECHR. *In: Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies*. Dordrecht: Springer, p. 267-268.

Van der Sloot, B., van Schendel, S., & Fontanillo López, C. A. (2022). *The influence of (technical) developments on the concept of personal data in relation to the GDPR*. WODC/TILT. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-summary.pdf?sequence=3&isAllowed=y.

Van der Sloot, B., and E. Kosta. "Big brother watch and others v UK: Lessons from the latest Strasbourg ruling on bulk surveillance." *Eur. Data Prot. L. Rev*. 5 (2019): 252.

Van Dijck, G. (2020). Algoritmische risicotaxatie van recidive. Over de Oxford Risk of Recidivism tool (OXREC), ongelijke behandeling en discriminatie in strafzaken. *Nederlands Juristenblad*, 95(25), 1784-1790.

Van Hoecke, M., *Is de rechtswetenschap een empirische wetenschap?*, The Hague, Boom juridische uitgevers, 2010.

Van Otterlo M (2013) A machine learning view on profiling. In: *Hildebrandt M and de Vries K (eds) Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*. Abingdon: Routledge, pp. 41–64.

Van Schendel, S. (2019). The challenges of risk profiling used by law enforcement: Examining the cases of COMPAS and SyRI. In L. Reins (Ed.), Regulating new technologies in uncertain times (pp. 225-240). (Information Technology and Law Series; Vol. 2019, No. 32). T.M.C. Asser Press/Springer. https://doi.org/10.1007/978-94-6265-279-8_12.

Van Schendel, S. (2020). Inzet SyRI onvoldoende inzichtelijk en controleerbaar en strijdig met fundamentele rechten. *Privacy & Informatie*, 2020(2), 69-71. [66]. https://www.uitgeverijparis.nl/reader/206858/1001485529.

Van Schendel, S., Data used in governmental automated decision-making & profiling: towards more practical protection, In: *The boundaries of data: Technical, practical and regulatory perspectives. van der Sloot, B. & van Schendel, S. (eds.)*. Amsterdam: Amsterdam University Press. (Accepted/In press).

Van Soomeren, P., Beerepoot, A., Meijer, R., & de Waard, J. (2005). Tegenhouden als nieuw paradigma voor de politie? Available at: https://www.dsp-groep.eu/wp-content/uploads/11abTegenhouden_als_nieuw_paradigma_voor_de_politie.pdf.

Van Wingerden, S. G. C., Leonardus Martinus Moerings, and J. A. Van Wilsem. *Recidiverisico en straftoemeting*. No. 2011-3. Sdu Uitgevers, 2011.

Veale M., Binns R. and Van Kleek M., Some HCI Priorities for GDPR-Compliant Machine Learning. The General Data Protection Regulation: An Opportunity for the CHI Community? (CHI-GDPR 2018), Workshop at ACM CHI'18, 22 April 2018, Montréal, Canada.

Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, 34(2), 398-404.

Veale, M., and R. Binns. "Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data." *Big Data & Society* 4, no. 2 (2017): 2053951717743530.

Vedder, A. KDD: The challenge to individualism. *Ethics and Information Technology* 1, 275–281 (1999). https://doi.org/10.1023/A:1010016102284.

Vedder, A., and Naudts, L., 'Accountability for the Use of Algorithms in a Big Data Environment' (2017) 31 *International Review of Law, Computers & Technology* 206.

Vedder, A., Why data protection and transparency are not enough when facing social problems of machine learning in a big data context. In: Emre Bayamlioglu et al. (eds), *Being profiled: Cogitas, ergo sum. 10 Years of Profiling the European Citizen*. Amsterdam University Press, 2018, Available at SSRN: https://ssrn.com/abstract=3407853.

Vogiatzoglou, P., Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity, *European Journal of Law and Technology*, Vol 10, Issue 1, 2019.

Vogiatzoglou, P., Quezada Tavarez, K., Fantin, S., Dewitte, P., "From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 11, no. 3 (2020): 274-302.

Vogiatzoglou, P., Marquenie, T., 2022. Assessment of the implementation of the Law Enforcement Directive. Publisher: European Union Publications Office.

Wachter, S., "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising," *Berkeley Technology Law Journal* 35, no. 2 (2020): 367-430.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, 7(2), 76-99.

Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567.

Wachter, S., Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review* 34 (2018) 436–449.

Ward, A., "The Impact of the EU Charter of Fundamental Rights on Anti-Discrimination Law: More a Whimper than a Bang?." *Cambridge Yearbook of European Legal Studies* 20 (2018): 32-60.

Ward, J. D. (2002). Race, ethnicity, and law enforcement profiling: Implications for public policy. *Public Administration Review*, 62(6), 726-735.

Washington, A.L., "How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate," *Colorado Technology Law Journal* 17, no. 1 (2018): 131-160.

Werth, R., Risk and punishment: The recent history and uncertain future of actuarial, algorithmic, and evidence based penal techniques. *Sociology Compass*. 2019; 13:e12659. https://doi.org/10.1111/soc4.12659.

Westen, P., 'The Empty Idea of Equality' (1982) 95 *Harvard Law Review* 537.

Whittaker et al., AI Now Report 2018, December 2018, available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf.

Wigan M and R Clarke, 'Big Data's Big Unintended Consequences' (2013) 46 *Computer* 46.

Williams, P., and Kind, E., (2019) Data-driven Policing: The hardwiring of discriminatory policing practices across Europe. Project Report. European Network Against Racism (ENAR).

WRR, *Big Data in een vrije en veilige samenleving*, Dutch Scientific Council for Government Policy (WRR), Amsterdam University Press 2016.

Xenidis, R. (2020). Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. *Maastricht Journal of European and Comparative Law*, 27(6), 736–758. https://doi.org/10.1177/1023263X20982173.

Yang, M., Wong, S.C., Coid, J., The efficacy of violence prediction: A meta-analytic comparison of nine risk assessment tools. *Psychol. Bull*. 136, 740–767 (2010).

Zaccaroni, G. "Differentiating Equality? The Different Advancements in the Protected Grounds in the Case Law of the European Court of Justice." In: *The Principle of Equality in EU Law*, pp. 167-195. Springer, Cham, 2017.

Zafar, M.B., I. Valera, M. Gomez Rodriguez, and K. P. Gummadi. 2017. Fairness Constraints: Mechanisms for Fair Classification, v5. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Fort Lauderdale, FL. http://arxiv.org/abs/1507.05259.

Zand, E. van 't, Matthijsse, S., Fischer, T., & Wagen, W. van der. (2020). Interventies voor cyberdaders. In: *J. J. Oerlemans & M. Weulen Kranenbarg (Eds.), Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (pp. 259-287). Den Haag: Boom criminologie. Retrieved from https://hdl.handle.net/1887/3307585.

Zarsky T (2016) The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision-making. *Science, Technology and Human Values* 41(1): 118–132.

Zarsky T. Z. (2002-2003), `Mine Your Own Business!`: Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion." *Yale Journal of Law & Technology* 5, pp. 1-56.

Zarsky, T.Z., 2013. Transparent predictions. *University of Illinois law review*, 2013 (4), 1503–1569.

Zarsky,T., Understanding Discrimination in the Scored Society, *Washington Law Review*, Vol. 89:1375, 2014.

Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, 237, 350-361.

Žliobaitė, I. Measuring discrimination in algorithmic decision-making. *Data Min Knowl Disc* 31, 1060–1089 (2017). https://doi.org/10.1007/s10618-017-0506-1.

Žliobaitė, I., and B. Custers. "Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models." *Artificial Intelligence and Law* 24, no. 2 (2016): 183-201.

Zouave, E.T., & Marquenie, T., An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling, *2017 European Intelligence and Security Informatics Conference*.

Zuiderveen Borgesius, F. (2015). *Improving privacy protection in the area of behavioural targeting*. PhD thesis, Faculty of Law (FdR), Institute for Information Law (IViR). Available at SSRN 2654213.

Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-andalgorithmic-decision-making/1680925d73.

Zuiderveen Borgesius, F.J., (2020) Strengthening legal protection against discrimination by algorithms and artificial intelligence, *The International Journal of Human Rights*, 24:10, 1572-1593, DOI: 10.1080/13642987.2020.1743976.

Miscellaneous references

- Author unknown, Harvard Law Review, March 2017, Volume 130, No. 5, 'State v. Loomis, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing, available at: https://harvardlawreview.org/2017/03/state-v-loomis/. Last accessed 28 March 2020.

- Autoriteit Persoonsgegevens, 'Methods used by Dutch Tax Administration unlawful and discriminatory', 17 July 2020, available at: https://www.autoriteitpersoonsgegevens.nl/en/current/methods-used-by-dutch-tax-administration-unlawful-and-discriminatory.

- Chammah, M. Policing the future: In the aftermath of Michael Brown's death, St. Louis cops embrace crime-predicting software, 3 February 2016, The Verge. Available at: https://www.theverge.com/2016/2/3/10895804/st-louis-police-hunchlab-predictive-policing-marshall-project.

- Chicago Police Department Special Order S09-11, Subject Assessment and Information Dashboard (SAID), 9 January 2019, available at: http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html.

- City of Chicago Office of Inspector General, Advisory concerning the Chicago Police Department's Predictive Risk Models, January 2020, available at: https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf.

- Coudert, F., "The Directive for data protection in the police and justice sectors: towards better data protection?", April 2016, via: https://www.law.kuleuven.be/citip/blog/the-directive-for-data-protection-in-the-police-and-justice-sectors-towards-better-data-protection/.

- Council of Europe, 'Modernisation of the Data Protection "Convention 108", available at: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.

- Council of Europe, 16 February 2018, 'Newly adopted: Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime', available at: https://www.coe.int/en/web/data-protection/-/newly-

adopted-practical-guide-on-the-use-of-personal-data-in-the-police-sector-how-to-protect-personal-data-while-combatting-crime-.

- Council of Europe, Commissioner for Human Rights, 'Unboxing Artificial Intelligence: 10 steps to protect Human Rights' (May 2019) 11 <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>.

- Council of Europe, Press release , 'Council of Europe adopts recommendation on profiling and data protection', Strasbourg, 25.11.2010. Available at: https://rm.coe.int/168071e498.

- Department of Corrections, State of Wisconsin, on the Correctional Offender Management Profiling for Alternative Sanctions tool, available at: https://doc.wi.gov/Pages/AboutDOC/COMPAS.aspx.

- European Parliament, 'Artificial Intelligence Act': https://www.europarl.europa.eu/committees/en/artificial-intelligence-act/product-details/20230417CDT11481.

- European Parliament, Legislative Train Schedule, 'Anti-discrimination directive: In "A New Push for European Democracy", available at: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-anti-discrimination-directive, last accessed 20-10-2021.

- Goldston, J., 'Ethnic Profiling and Counter-Terrorism: Trends, Dangers and Alternatives' (2006) Open Society Justice Initiative, available at: https://www.justiceinitiative.org/publications/ethnic-profiling-and-counter-terrorism-trends-dangers-and-alternatives.

- Gorner, J., and Sweeney, A., Chicago Tribune January 24, 2020: https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html.

- Hansken: https://www.hansken.nl/an-introduction-to-hansken.

- Jouvenal, J., The New Way Police Are Surveilling You: Calculating Your Threat 'Score,' Washington Post (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac.

- OxRec, information is available via: https://oxrisk.com/oxrec-nl-2-backup/.

- Practitioner's Guide to COMPAS Core, available at: https://www.equivant.com/wp-content/uploads/Practitioners-Guide-to-COMPAS-Core-040419.pdf.

- Probation Netherlands, 'RISC', available at: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

- SyRI subpoena: https://pilpnjcm.nl/wp-content/uploads/2019/08/EN-Subpoena-SyRI.pdf.

- The Netherlands Institute for Human Rights, 'Discriminatie door risicoprofielen - Een mensenrechtelijk toetsingskader', available at: https://publicaties.mensenrechten.nl/publicatie/61a734e65d726f72c45f9dce.

- TNO, 'Rule of law and investigation', available at: https://www.tno.nl/en/tno-insights/articles/how-big-data-is-reducing-burglaries-in-amsterdam/.

- Visiedocument, 2001/4: Projectgroep Opsporing (Raad van Hoofdcommissarissen), Visiedocument 'Misdaad laat zich 'tegenhouden"; Advies over bestrijding en opsporing van criminaliteit, Amsterdam, 2001.

- Voss, A., and Padova, Y., 'We need to make big data into an opportunity for Europe' (Euractiv, 25 June 2015) available at: https://www.euractiv.com/section/digital/opinion/we-need-to-make-big-data-into-an-opportunityfor-europe.

- Walt, S.M. (2013) 'The real threat behind the nsa surveillance programs', available at: http://foreignpolicy.com/2013/06/10/the-real-threat-behind-the-nsasurveillance-programs/.

- Wolpert, S. (2015, October 7). Predictive policing substantially reduces crime in Los Angeles during months-long test. UCLA Newsroom. Retrieved from http://newsroom.ucla.edu/releases/predictive-policing-substantially-reduces-crime-in-losangeles-during-months-long-test.