Chapter 1
Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities

Francesca Bosco, Niklas Creemers, Valeria Ferraris, Daniel Guagnin, and Bert-Jaap Koops

Abstract This paper aims to map the field of profiling, its implications for fundamental rights and values, and the measures which are or can be taken to address the challenges of profiling practices. It presents a working definition of profiling and elaborates a typology of its basic methods. In the second section the paper gives an overview of the technological background of profiling to display how fundamental rights and values of European societies are endangered by the use of profiling. Finally the paper presents the findings of a questionnaire addressed to European DPAs on the current and future legal framework, the domains of application, the complaints and remedies procedures regarding the use of profiling techniques, the main risks and benefits for the fundamental rights, and citizens' awareness on this topic. These findings contribute important insights for the ongoing discussion on the regulation of profiling in Europe.

F. Bosco (✉)
Emerging Crimes Unit, UNICRI, Turin, Italy
e-mail: bosco@unicri.it

N. Creemers • D. Guagnin
Centre for Technology and Society (CTS), Technische Universität Berlin (TUB), Berlin, Germany
e-mail: creemers@ztg.tu-berlin.de; guagnin@ztg.tu-berlin.de

V. Ferraris
Law Department, University of Turin, Torino, Italy

Amapola Progetti per la sicurezza delle persone e delle comunità, Torino, Italy
e-mail: valeria.ferraris@amapolaprogetti.org

B.-J. Koops
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg, The Netherlands
e-mail: e.j.koops@uvt.nl

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_1

1.1 Introduction

The term "Big Data" is grounded in socio-technological developments, which began with the invention of the computer and has unfolded a rapidly growing dynamic over the past decades. Technological advancement has fueled the digitization of our societies by increasingly powerful infrastructures, basing on digital devices and software. Mediated communication today has mostly become digital communication, and information has consequently become easy to process and store as data, and is at the same time fluid and persistent. New potentials of gathering data raise hopes for developing more advanced ways to manage societies. The more we know the better we can control social processes and steer societal progress. At least that is what we are promised by "Big Data" proponents. "Big Data" appears to be a fetish, a crystal ball which allows those who use it to not just look into the future but to gain information which enables them to shape it at their needs.[1]

However, big data itself is not information but still mere data.[2] The more data we gather the harder it is to extract usable information as the huge amounts of data exceed human capabilities of consideration. Consequently data needs powerful tools to be utilized as a marketable resource. These tools are considered to be found in technologies such as data mining. They are supposed to turn "Big Data" into the new oil.[3]

Profiling can be understood as a specific data mining method. In this perspective profiling is regarded as an (semi-)automated process to examine large data sets in order to build classes or categories of characteristics. These can be used to generate profiles of individuals, groups, places, events or whatever is of interest. Profiles structure data to find patterns and probabilities. Using actuarial methods in this context is supposed to generate prognostic information to anticipate future trends and to forecast behavior, processes or developments. The aim is to develop strategies in order to manage uncertainties of the future in the present. In this regard, the

[1] See Fraunhofer. IAIS, *Big Data – Vorsprung durch Wissen. Innovations potenzial analyse*, http://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents/FraunhoferIAIS_Big-Data-Analyse_Doku.pdf, last accessed 01 April 2014. The programs of the world's largest ICT fair CeBIT 2014, the Big Data Days 2013, and the European Data Forum and the presentations given there, draw an interesting picture of the potentials the ICT industry attributes to "Big Data" and big data analytics: http://www.cebit.de/home, last accessed 03 April 2014, http://www.big-data-days.de, last accessed 03 April 2014, and http://2014.data-forum.eu/, last accessed 03 April 2014.

[2] Sasa Baskarada and Andy Koronios, "*Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension*," in Australasian Journal of Information systems, Vol 18, No 1 (2013): 5–24.

[3] Karl-Heinz Streibich, "*Big Smart Data. Mehrwert für Unternehmen*" (paper presented at the Big Data Days, Berlin, Germany, November 11–12, 2013).

ideology of "Big Data" and analytical tools such as profiling can be understood as an important facilitator and part of a preventive paradigm which can be found in diverse societal contexts.[4]

Even though the reality of profiling might not live up to the expectations of its prophets,[5] the assumed potentials of gathering and processing data spawn the dream of overcoming human deficiencies with technology, these new technologies also draw fears and skepticism as they impose threats on some of the core values and principles of European societies. Key challenges which have been identified by scholars include infringements of democratic principles and the rule of law: Data gathering, exchange, and processing potentially harm central values like individual autonomy and informational self-determination as well as the fundamental rights of privacy, data protection, and non-discrimination.

This paper aims to map the field of profiling. It focuses on its implications for fundamental rights and values in different fields of application and on the assessment of the existing countermeasures to address the challenges of profiling practices. In the following section this paper proposes a working definition of profiling. The third section gives an overview of the technological evolution building the ground for the emergence of profiling, afterwards it is demonstrated how fundamental rights and values of European societies are endangered by the application of profiling in various contexts (Sect. 1.4). In Sect. 1.5 the legal regulation of profiling is sketched. Finally the paper presents the first findings of a questionnaire carried out by the project PROFILING,[6] in order to gain knowledge about European Data Protection Authorities' awareness, attitudes, and activities regarding profiling and its societal impacts.

1.2 Profiling: Towards a Definition

Profiling is a highly evocative term with multiple meanings, used in both specialist and non-specialist contexts. Whereas the literature on statistics does not pay specific attention to definitions and tends to focus on technical aspects (e.g. data mining

[4]See Susanne Krasmann, "*Der Präventionsstaat im Einvernehmen. Wie Sichtbarkeitsregime stillschweigend Akzeptanz produzieren*," in *Sichtbarkeitsregime: Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*, ed. Leon Hempel, Susanne Krasmann and Ulrich Bröckling (Wiesbaden: VS Verlag, 2010), 53–70 and Pat O'Malley, "*Risk, power and crime prevention,*" *Economy and Society* 21/3 (1992): 252–275.

[5]For some of the technical problems which harm the reliability of profiling results, see Daniel Guagnin, Leon Hempel and Justin Jung, "Evolution of Technologies in Profiling", Working Paper, http://profiling-project.eu/wp-content/uploads/2013/08/Evolution-of-Technologies-in-Profiling_0208.pdf, last accessed 02 April 2014.

[6]The PROFILING project is funded from the European Union's Fundamental Rights and Citizenship programme. The 2 year project started in November 2012. More information on the project can be found on the website http://profiling-project.eu.

techniques and predictive models), providing a definition appears an issue among socio-legal scholars and policy makers. However a widely shared definition has not yet emerged.

Gary T. Marx gave one of the oldest definitions of profiling in a paper that analyses systems of data searching. Profiling (defined by the author in contrast to "matching") is defined by stressing the logic behind it: "the logic of profiling is more indirect than that of matching. It follows an inductive logic in seeking clues that will increase the probability of discovering infractions relative to random searches. Profiling permits investigators to correlate a number of distinct data items in order to assess how close a person or event comes to a predetermined characterization or model of infraction".[7] According to the author's background, this definition is strictly related to the law enforcement domain.

Almost 10 years later, Roger Clarke defined profiling as a "dataveillance 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".[8]

A legal scholar, Bygrave again stressed: "profiling is the inference of a set of characteristics (profile) about an individual person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics".[9]

Later on, Mireille Hildebrandt was the one who put the best effort to precisely define profiling and its distinctive features and the working definition proposed here has built on her work. She defines profiling as "the process of 'discovering' patterns in data in databases that can be used to identify or represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify a subject as a member of a group (which can be an existing community or a discovered category)."[10]

Profiling creates a new form of knowledge that makes visible patterns that are otherwise "invisible to the naked human eye".[11] They are based on correlations found in data sets, and cannot be "equated with causes or reasons without further

[7]Marx, Gary and Reichman Nancy. "*Routinizing the Discovery of Secrets: Computers as Informants*," in *American Behavioral Scientist*, 27, 4 (1984): 429.

[8]Clarke, Roger, "*Profiling: A Hidden Challenge to the Regulation of Data Surveillance*," in *Journal of Law and Information Science* 4, 2 (1993): p. 403.

[9]Bygrave, Lee A., *Data protection law: Approaching its rationale, logic and limits* (The Hague: Kluwer Law International, 2002), 301.

[10]Mireille Hildebrandt, "*Profiling and AML*," in *The Future of Identity in the Information Society. Challenges and Opportunities*, ed. Kai Rannenberg, Denis Royer and Andre Deuker (Heidelberg: Springer, 2009a), 275.

[11]Mireille Hildebrandt, "*Who is Profiling Who? Invisible Visibility*" in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009c), 241.

inquiry; they are probabilistic knowledge."[12] Profiling represents a shift from the idea that knowledge is the result of tested hypothesis. It generates hypotheses: "the correlations as such become the 'pertinent' information, triggering questions and suppositions".[13] Consequently profiling fosters new forms of generating and applying knowledge. Due to the growing capacities of databases, and capabilities of advanced analysis profiling procedures become increasingly complex. In this context the human role in interpreting data changes significantly.

As pointed out by Hildebrandt, profiling can be categorized into non-automated, automated and autonomic profiling. Non-automated profiling is a form of reasoning that does not rely on any process of automation. Automated profiling is based on "automated functions that collect and aggregate data" and develop into "automation technologies that can move beyond advice on decision-making, taking a load of low-level and even high-level decisions out of human hands."[14] Differently, autonomic profiling describes the process whereby the human role is minimized and the decision making process is entirely driven by the machine.[15] Autonomic profiling "goes one step further than automated profiling."[16] The machines drive the decision making process, providing for a readjusted environment based on their profiling and without calling for human intervention. Besides their degree of automation profiling methods can be distinguished by their object and application. Profiling can be applied as group profiling or individual profiling: the techniques that identify and represent groups can also focus on individuals.[17] Moreover profiling relies on data collected from one single person or group to apply the information derived from data processing to the same person or group – direct profiling – or it relies on categorization and generalisation from data collected among a large population to apply it to certain persons or groups – indirect profiling. Group profiling can also

[12]Gloria González Fuster, Serge Gutwirth and Ellyne Erika, "*Profiling in the European Union: A high-risk practice*," in *INEX Policy Brief* 10 (2010): 2.

[13]Gloria González Fuster, Serge Gutwirth and Ellyne Erika, "*Profiling in the European Union: A high-risk practice*," in *INEX Policy Brief* 10 (2010): 2.

[14]Mireille Hildebrandt, "*Defining profiling: a new type of knowledge?*," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 28.

[15]See Mireille Hildebrandt, "*Profiling: from Data to Knowledge. The challenges of a crucial technology*," in *DuD Datenschutz und Datensicherheit* 30(9) (2006): 548–552 and Mireille Hildebrandt, "*Defining profiling: a new type of knowledge?*," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 17–47.

[16]Mireille Hildebrandt, "*Profiling: from Data to Knowledge. The challenges of a crucial technology*," in *DuD Datenschutz und Datensicherheit* 30(9) (2006): 550.

[17]See Anton, Vedder, "*KDD: The challenge to individualism*," in *Ethics and Information Technology* (1999): 275–281 and Arnold Roosendaal, *Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts*, Oisterwijk: Wolf Legal Publishers.

be classified as distributive group profiling or non-distributive group profiling.[18] A distributive group profile identifies a certain number of people having the same attributes. All the members of the group share the same characteristics. In contrast, a non-distributive group profile identifies a certain number of people who do not share all the attributes of the group's profile.

These distinctions give an idea of the different types of profiling and their application. The forms of profiling, which are subject of this article are automated and autonomic profiling and their various forms and fields of application.

The following proposed definition takes into account the preceding evolution of technologies in which profiling is embedded and focuses on the purpose profiling is being used for. It will be the basis for this paper:

> Profiling is a technique of (partly) automated processing of personal and/or non-personal data, aimed at producing knowledge by inferring correlations from data in the form of profiles that can subsequently be applied as a basis for decision-making.
>
> A profile is a set of correlated data that represents a (individual or collective) subject.
>
> Constructing profiles is the process of discovering unknown patterns between data in large data sets that can be used to create profiles.
>
> Applying profiles is the process of identifying and representing a specific individual or group as fitting a profile and of taking some form of decision based on this identification and representation.

1.3 Societal Consequences of Digitization

Advanced data analysis tools have established new social practices of knowledge production and have created new types of knowledge. We argue that the practices of profiling have facilitated and are part of a broader societal paradigm of prevention. We will elaborate on the societal implications of changing social practices through emerging profiling technologies as a ground for the examination of threats for fundamental rights and values of European societies in Sect. 1.4.

Observations made by human beings need to be written down to be made explicit. The written documentation of observations can be regarded as a first step to enable a generalized and objectified way of keeping information and exchanging it between individuals and institutions.[19] Digitized information, however, can be processed and analysed automatically so that information is easier and cheaper to store, process and analyse. An illustrative example of how exhaustive and expansive

[18] See Anton, Vedder, "*KDD: The challenge to individualism*," in *Ethics and Information Technology* (1999): 275–281.

[19] The important role the implementation of written files played as storage and medium for information but also as a symbol of power for the Inquisition trials in Italy is displayed by Thomas Scharff, "*Erfassen und Erschrecken. Funktionen des Prozeßschriftguts der kirchlichen Inquisition in Italien im 13. und frühen 14. Jahrhundert*. "in A*ls die Welt in die Akten kam. Prozeßschriftgut im europäischen Mittelalter*, ed. Susanne Lepsius and Thomas Wetzstein (Frankfurt a.M.: Vittorio Klostermann, 2008), 255–274.

the detailed documentation of people's activities and behaviour has been, is the comparison between digital data the NSA stores with the amounts of files the Stasi – German Democratic Republic's domestic secret service – produced. All the information captured throughout the Stasi history would fill about 48.000 cabinets covering approximately 0,019 km^2. The NSA's planned data centre in Utah will host about 5 zettabytes of data which could roughly be converted in about 42 quadrillion file cabinets covering 17 million km^2 – bigger than the European continent.[20] The example also shows the differing efforts needed to collect and archive data depending on whether using analog or digital data processing. While the Stasi needed to install microphones, hire staff to monitor and document people's behaviour to gain information about their habits, attitudes and social networks, in a digitized world a lot of that information can be monitored and stored on the fly through sensors, log data or user generated content. This shows that the digitization of communication and transactions does not only produce more data but also provides new kinds of information[21] which can be used to extract knowledge about individuals: their social relations, interests and activities. Once stored and made accessible via computer networks, data becomes easily exchangeable worldwide. At the same time it becomes hard to grasp how data is exchanged, which information is gained and by whom. Furthermore the specific mediums can store specific data. Certain elements which can be archived on paper cannot be archived digitally and vice versa. Moreover certain information can hardly be digitized respectively digitally analyzed, e.g. hand-written information, and smells. By that, archives have a filtering function which shapes the accessibility of information as data. But simplified storage and exchange of data are only one aspect of the ongoing process of digitization of everyday life. Beyond that advanced methods of data analysis have fundamentally changed the procedures of knowledge production through automation.

Another effect of the digitization of data becomes evident when we think of the different haptic and cognitive perceptions of digital versus analog files and folders. Different items and elements can be put in an analog or digital file, and at the same time, the availability of and the access to certain kinds of information fundamentally changes. In other words: accessing information at a (real) desktop is very different from accessing information when sitting in front of a computer screen. Paper folders can be touched and felt, digital files are browsed on a screen and can be searched by keywords. Consequently, the way of reasoning changes, as first findings of one of the case studies conducted in PROFILING show.[22] More interaction of the analyst is

[20] Open Data City, *Stasi versus NSA*, accessed February 27, 2014, http://apps.opendatacity.de/stasi-vs-nsa.

[21] Bert-JaapKoops, "*Technology and the Crime Society: Rethinking Legal Protection*," in *Law, Innovation & Technology*, 1, 1 (2009): 93–124.

[22] Technische Universität Berlin conducted a case study about the transformation of policing practices due to the application of data processing technologies. Expert interviews were conducted with scholars, civil rights activists, directors of security technology companies, a police representative, and a lawyer. Police as well as technology providers mentioned changes in the workflow and the

oriented towards computer interfaces and thus influenced by the way user interfaces are designed, information is presented, and how searches can be conducted.[23] The transformation of the human role in knowledge production processes is even more significant when it comes to examining large-scale databases. Learning algorithms are trained on specific data sets to build categories or to find patterns in the data. Assumptions or hypotheses made by the analyst play a minor role during data processing, they are to a certain degree hidden in the process of writing algorithms and training the algorithms. Finally, hypotheses are derived "from the material".[24] As a consequence implicit assumptions driving the actors during the selection of training data, preprocessing target data and suitable algorithms become invisible and the outcomes produced by "the data" seem objectified. Subjective assumptions and social norms are hidden in the technology during the process of automatization, while outcomes based on computed models and databases are often perceived as solid statistics and thus more objective than human interpretation.[25] This perception as objectified knowledge of computer-generated models supports the thesis of a general tendency of technology to make social norms more durable[26] and more specifically the thesis that social sorting becomes strengthened if mediated through technology.[27] Profiles, as mentioned above, can be seen as hypotheses. These hypotheses are inductive as they are not necessarily developed on the basis of a theory or a common sense expectation, but often emerge in the process of data mining. This can be regarded as a shift from a more traditional, rather assumption-

construction of theses from digitally stored information. The report of the case study's final results will be available at http://profiling-project.eu/.

[23] See Nina Degele, *Einführung in die Techniksoziologie* (Stuttgart, UTB, 2002), p. 167–168.

[24] The results software can draw from data material are dependent on the quality of the data sets, which are examined, including the selection and pre-processing of data. Major problems, especially regarding large-scale data sets which combine data from various sources, are poor data quality, data incompatibility, and biased data sets which corrupt data mining outcomes. Furthermore operators might not be familiar with such reliability problems. Consequently operators might not act properly upon these problems. See Ana Canhoto and James Blackhouse, "General Description of Behavioural Profiling," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 47–63 and Bernhard Anrig, Will Brown, and Mark Gasson, "The Role of Algorithms in Profiling," in *Profiling the European Citizens, Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 65–87.

[25] See Toon Calders and Indrė Žliobaitė, "*Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*," in *Discrimination and Privacy in the Information Society*, ed. Bart Custers et al. (Berlin: Springer, 2013), 43–57.

[26] See Bruno Latour, "Technology is Society Made Durable," in *A Sociology of Monsters: Essays on Power, Technology and Domination*, ed. John Law (London: Routledge, 1991), 103–131.

[27] See Michaelis Lianos and Douglas Mary, "*Dangerization and the End of Deviance: The Institutional Environment*," in *British Journal of Criminology* 40, 2 (2000): 261–278 and Rosamunde van Brakel and Paul De Hert, "*Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies*," in *Cahier Politiestudies* 2011–3 no. 20 (2011): 163–192.

driven approach to a discovery-driven approach to knowledge generation.[28] This shift results not only from growing data capabilities and advancing technological methods. Lyon argues that the conceptualization of social threats as actuarially identifiable and addressable risks and the desire for intelligence-led management of populations play a key role in the spread of profiling technologies.[29] In this context data mining is considered a key technology for risk assessment in various fields of application such as eHealth, airport security, and policing. Profiling techniques are used to identify categories and groups in order to assess risks and probabilities of certain future developments. The generated profiles can then be used to sort individuals, groups, events or processes in order to make them addressable for specific practices.[30] In this regard profiling is a technology to structure potential futures in order to make them governable in the presence. Therefore profiling is an important practice of a broader societal preventive paradigm, which is based on probabilistic knowledge used to manage social processes in the form of risk management.[31] By that profiling technologies provide means of control, which can be exercised for care and protection or coercion and repression.[32]

1.4 Profiling as a Threat for Fundamental Rights and Values

Even though the results of data mining are often limited reliable,[33] proponents claim that the potentials for managing social and technological processes in more efficient ways through data gathering and analysis are immense. They expect that the growing amount of data and increasingly advanced tools for examination will provide information which will allow organisations to identify, target, and act upon undesirable developments at an early stage – preferably before they occur.

[28] See Mireille Hildebrandt, "*Defining profiling: new type of knowledge?*," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 17–47.

[29] See David Lyon, "*Surveillance as Social Sorting. Computer Codes and Mobile Bodies*," in *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*, ed. David Lyon (London: Psychology Press, 2003), 20.

[30] Profiling appears to create a dialectic form of practical knowledge, which is non-representative and representative, as defined in Sect. 1.2, at the same time. It is non-representative as profiles do not describe a given reality, but are detected by the aggregation, mining and cleansing of data. Nevertheless as these profiles are used to address populations according to this knowledge, they constitute them as a reality and thus do have a representative function.

[31] See Pat O'Malley, "*Risk, power and crime prevention*", *Economy and Society* 21/3 (1992): 252–275.

[32] Torin Monahan, "Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance," in *Surveillance and Democracy issue* (2010): 91–110.

[33] See Bernhard Anrig, Will Brown, and Mark Gasson, "The Role of Algorithms in Profiling," in *Profiling the European Citizens, Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 65–87.

Preemptive policing, early detection of pandemic risks, and the prevention of tax fraud are examples of the societal benefits of the use of sophisticated data mining methods. Yet there is a downside to these opportunities implied by the technological evolution of digitization: it threatens key aspects of fundamental citizen rights, such as the rights to privacy, data protection and non-discrimination, and core values of European societies – democracy, the rule of law, autonomy and self-determination. As societies rely more and more on profiling methods to steer social and technological processes the urgency of dealing with these threats grows.

1.4.1 Fundamental Values

The clash between liberal democracy[34] and profiling is brought about by their inherent characteristics. Profiling is considered a glamour technology: it gives the idea that human beings can attain unforeseeable knowledge that allows making better decisions. But the dark side of profiling is that it makes "invisible all what cannot be translated into machine-readable data."[35] This means that the decision-making process is prone to be biased in the data collection phase and because of the complexity of the applied algorithms, human beings cannot properly intervene in repairing this bias. Consequently, "as far as the governance of people and things becomes dependent on these advanced profiling technologies, new risks will emerge in the shadow of the real time models and simulations these technologies make possible. What has been made invisible can grow like weeds."[36] In other words, not to consider some of the aspects of an issue can turn, at least, into ineffective and wrong decisions or, at most, in serious risks and damages for the population.[37]

Not only human intervention is reduced during the decision-making process, but also citizens do hardly have any access to the procedure behind the construction and application of profiles. This seriously hampers the quality of a liberal democracy because of the unbalanced distribution of power[38] and knowledge asymmetries[39] between the ordinary citizens, on the one hand, and the government on the other hand. Knowledge asymmetries are a common phenomenon but it reaches a new peak in profiling technologies. In most of the cases, citizens are not aware of the

[34] See Fareed Zakaria, "*The rise of illiberal democracy*," in *Foreign Affairs*, 76, 6 (1997): 22–43.

[35] Serge Gutwirth and Mireille Hildebrandt, "*Some Caveats on Profiling*," in *Data protection in a profiled world*, ed. Serge Gutwirth, Yves Poullet and Paul de Hert (Dordrecht: Springer, 2010.), 33.

[36] Ibid.

[37] As an example we can think of applying automated profiling to the health sector were the risks of taking wrong decisions could cost lives.

[38] See Daniel J. Solove, *Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004).

[39] See Serge Gutwirth and Mireille Hildebrandt, "*Some Caveats on Profiling*," in *Data protection in a profiled world*, ed. Serge Gutwirth, Yves Poullet and Paul de Hert (Dordrecht: Springer, 2010.), 31–41.

information circulating and how they could be used in the future. In particular, when profiles are constructed from data that is not of the data subjects, information is used to take decisions about them without their involvement. So there is no easy protection on the horizon. Moreover some sophisticated profiling technologies like Behavioural Biometric Profiling (BBP) "do not require identification at all"[40] and by that increase this problem.

If the position that citizens enjoy versus the state is one of the indicators of the quality of a liberal democracy, the governmental use of profiling techniques seriously challenges some essential democratic features. This is not only related to the recognition of rights by the state, but also to the opportunities these rights entail for the full and free development and expression of citizens' personalities and their effective participation in democratic life. In this framework are placed the fundamental values of autonomy and self-determination. Against the backdrop of the discussion about profiling, self-determination acquires the specific meaning of informational self-determination, which means that an individual needs to have control over the data and information produced by and on him/her. This control is "a precondition for him/her to live an existence that may be said 'self-determined'."[41] As shown in the prior section digitization of everyday life has led to opaque ways of data gathering, exchange and processing. Consequently technologies like profiling do not leave much space for autonomy and self-determination.[42]

As in any other field, the application of profiling in healthcare can be helpful, yet harmful. eHealth and mHealth (electronic health and mobile health) technologies enable constant monitoring and profiling of persons' physical conditions, their activities, medical treatment, or diet. That way e- and mHealth-applications might help people to pick up healthier lifestyles as well as improve cures for illnesses and the individual treatment of diseases. At the same time there is potential for gathering information about patients' lifestyles from a hard to grasp range of sources that could be used for an actuarial assessment of lifestyles to build risk categories which are not only used for "individualized" treatments, but also to offer "individual" insurance fees or other incentives to make clients adapt certain lifestyles. Yet the categories on which these incentives are created by profiling are anything but individual. They derive from abstract calculations conducted under the premise of profit maximization and transfer this economic logic to individual lifestyle choices by rewarding behaviours assessed as low risk or healthy, while sanctioning the ones which are considered as increasing risks for accidents or diseases. Even though profiling in this context is supposed to empower healthy

[40] Mireille Hildebrandt, "*Who is Profiling Who? Invisible Visibility*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009c), 243.

[41] Antoinette Rouvroy and Yves Poullet, "*The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 51.

[42] Mireille Hildebrandt, "*Who is Profiling Who? Invisible Visibility*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009c), 243.

lifestyles, it also undermines individuals' autonomy. It facilitates the economization of everyday life by addressing individuals as dividuals – bundles of risks and behavioural probabilities, reducing them to profiles.[43] eHealth is only one area in which this logic is executed. Risk factors or behavioural probabilities, which are identified and addressed, vary contextually as aims and scopes of profiling agents differ. "Although we are constantly being monitored in some way or another we do not live in an Orwellian 'Big Brother' dystopia. [. . .] Rather, an intricate network of small surveillance societies exists, often overlapping, connectable or connected, but each with their own features and rules."[44] What links these *small surveillance societies* is the idea to create knowledge gathered from certain populations which allows steering individuals, groups, and social processes. At this point autonomy and informational self-determination are closely interwoven as putting one at risk can jeopardize the other.

In policing, the development of preventive measures is a key argument for the implementation of growing capacities of gathering, exchanging and analyzing information. In Germany, police forces host large numbers of distinct databases for various purposes. They are fed and maintained by different institutions, such as the federal police organizations, state police organizations, or domestic secret services. The rules for gathering and exchanging data as well as for the access to the information for different institutions are hardly comprehensible. They are defined by federal data protection and criminal justice law (e.g., Bundesdatenschutzgesetz, Bundeskriminalamtgesetz, Strafprozessordnung), and various other laws and orders on state and federal level.[45] Beyond that several technical orders and so called "Errichtungsanordnungen" determine the architecture, use and purposes of data bases installed by the police.[46] This opaque framework still lacks a legal definition that covers data mining measures like profiling as stated by the German

[43]Gilles Deleuze, "Postskriptum über die Kontrollgesellschaften," in *Unterhandlungen 1972–1990*, Gilles Deleuze (Frankfurt a.M.: Suhrkamp, 1992), 254–262.

[44]Bert-Jaap Koops, "*Technology and the Crime Society: Rethinking Legal Protection*," in *Law, Innovation & Technology*, 1, 1 (2009): 104.

[45]See Deutscher Bundestag, *Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen*, Drucksache 17/11582, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014.

[46]Even though "Errichtungsanordnungen" can be requested by citizens, an expert on political activism in TUB's case study reported that police refused to give him requested information as handing out this information would hamper police work. Additionally several answers of the German government to requests of members of the parliament regarding data gathering, storage and analytics conducted by German police forces show that essential information about this practice is kept secret in order to avoid infringement of police work. See Deutscher Bundestag, *Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen*, Drucksache 17/11582, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014 and Deutscher Bundestag, *Computergestützte Polizeitechnik bei Polizeibehörden*, Drucksache 17/8544 (neu), 06 Feb 2012, http://dipbt.bundestag.de/dip21/btd/17/085/1708544.pdf, last accessed 01 April 2014.

Government.[47] This results in serious threats for informational self-determination and in particular cases it affects citizens' political participation and finally even the development of a liberal democracy. For example, the German federal police, Bundeskriminalamt (BKA), maintains databases for politically motivated offenders (distinguished as left, right and foreign offenders), which are fed by and accessible for the state police organizations (Landeskriminalamt, LKA). The information stored can be used for example to reconstruct social networks, allocate people to groups or institutions, or to identify people to be kept away from certain events of special interest, for instance NATO or G8 summits. First findings of interviews, conducted within a PROFILING case study,[48] with activists who are an involved in civil rights groups, show that interviewees considered data gathering, exchange and its use in the policing practice as non-transparent and by that intimidating, especially for people which are just starting to join civil rights groups. (Potential) activists do not know if and which information is gathered at which events, for which reasons, for whom this information is accessible, and how it might be used – or if it could lead to further police measures. This uncertainty may result in hindering the exertion of civil rights or lead to adaptive behaviour. Persons might change their behaviour in order to not seem conspicuous or suspicious and avoid to be linked with e.g. civil rights groups. Even though the technology used in this context cannot be considered as fully automated profiling, the computer-assisted data storage and representation already leads to opaque structures which undermine informational self-determination and restrain citizens' political participation. Furthermore it indicates challenges emerging from "predictive policing" approaches which aim on using (semi-)automatically generated profiles to score the risk of certain groups and individuals to commit particular crimes.

1.4.2 Fundamental Rights

The fundamental values presented before are strictly interrelated with the right to privacy and data protection and to the protection from discrimination. As clearly underlined by Rodotà, "the strong protection of personal data continues to be a 'necessary utopia' if one wishes to safeguard the democratic nature of our political

[47] See Andrej Hunko, *Suchbewegungen zu Data Mining-Software gehen über gesetzlichen Auftrag des BKA hinaus*, 17 March 2014, http://www.andrej-hunko.de/presse/1934-suchbewegungen-zu-data-mining-software-gehen-ueber-gesetzlichen-auftrag-des-bka-hinaus, last accessed 26 March 2014, and Deutscher Bundestag, *Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen*, Drucksache 17/11582, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014.

[48] For information about the case study conducted by Technische Universität Berlin see footnote 22.

systems."[49] Data protection is necessary in a democratic society, as Rouvroy and Poullet pointed out, to sustain a vivid democracy. The right to non-discrimination is equally important.[50] It is not by chance that the European Court of Justice, in two recent profiling-related cases[51] has invoked both the legislation on Data Protection and anti-discrimination to protect citizens' rights.

1.4.2.1 The Right to Privacy and the Right to Data Protection

Leaving aside all difficulties of defining the various notions of privacy[52] it is useful to shortly revisit the interplay between privacy and data protection. Following Gellert and Gutwirth, most privacy definitions[53] can be summarized in either the problem of being left alone, or the question of how to cope with information stemming from social interaction in a way that certain areas of one's personal life are hidden from unwanted views.[54] Data protection law however is made to ease the free flow of information by safeguarding personal data. In this respect privacy is a matter of opacity while data protection is related to transparency.[55] In the field of profiling it is highly relevant to consider the scope of both terms: while privacy is broader in the sense that privacy covers more than mere personal data the misuse of personal data can affect much more than someone's privacy. As outlined above various technologies nowadays potentially create digital data which can be part of automated processing and profiling. Accordingly the concepts of privacy and data protection are

[49] Stefano Rodotà, "*Data Protection as a Fundamental Right*", in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 78.

[50] See Antoinette Rouvroy and Yves Poullet, "*The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy*", in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 57.

[51] Huber v. Germany, C-524/06 (2008), find a summary of the judgment at: http://ec.europa.eu/dgs/legal_service/arrets/06c524_en.pdf; Test-Achats v. Council of Ministry, C-236/09 (2011), find a summary of the judgment at: http://ec.europa.eu/dgs/legal_service/arrets/09c236_en.pdf

[52] See Daniel J. Solove, "*I've Got Nothing to Hide' and Other Misunderstandings of Privacy*", in *San Diego Law Review* Vol. 44 (2007): 754–764.

[53] There is a large amount of literature on privacy taxonomies. Finn, Wright, and Friedewald summarizes the debate and propose a taxonomy of 7 types of privacy: privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy). See Rachel L Finn, David Wright and Michael Friedewald, "*Seven Types of Privacy*", in *European Data Protection: Coming of Age*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2013), 3–32.

[54] See Raphael Gellert and Serge Gutwirth, "*Beyond accountability, the return to privacy?*," in *Managing Privacy through Accountability*, ed. Daniel Guagnin et al. (Houndmills: Palgrave Macmillan, 2012), 261–284.

[55] See Raphael Gellert and Serge Gutwirth, "*Beyond accountability, the return to privacy?*," in *Managing Privacy through Accountability*, ed. Daniel Guagnin et al. (Houndmills: Palgrave Macmillan, 2012), 261–284.

increasingly challenged by the capabilities of data usage and analytics. The concepts evolve over time as technologies develop and have to catch up with the constant progress: "its content varies from the circumstances, the people concerned and the values of the society or the community."[56] Moreover profiling technologies, as shown in this paper, lead to more black boxing, more opacity of data processing. It is in fact questionable how the factual use of data can be made transparent.

In order to build an exhaustive framework of the threats towards the right to privacy and the right to data protection, the OECD Privacy Principles[57] are taken as term of reference as one of the most comprehensive and commonly used privacy frameworks.[58]

These principles include (1) Collection Limitation Principle: data should be obtained by lawful and fair means and with the knowledge or consent of the data subject; (2) Data Quality Principle: data which are to be used, should be accurate, complete and kept up-to-date; (3) Purpose Specification and (4) Limitation Principle: The purposes for data collected should be specified only be used for the specified purposes; (5) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards; (6) Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. (7) Individual Participation Principle: Individuals should have the right: (a) to obtain the data stored relating to them; (b) to be informed about data relating to them (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended. (8) Accountability Principle: A data controller should be accountable for complying with measures, which give effect to the principles stated above.[59]

---

[56]Pierre Trudel, "*Privacy Protection on the Internet: Risk Management and Networked Normativity*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 322.

[57]The Privacy Principles are contained in the OECD Guidelines on the protection of privacy and transborder flows of personal data. In 2013 these Guidelines have been updated; the original version, developed in the late 1970s and adopted in 1980, was the first internationally agreed upon set of privacy principles. See OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, accessed 14 March, 2014, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[58]The basic data protection principles largely overlaps with the principles outlined in the Council of Europe's Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data (http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm) and the Directive 95/46/EC on the Protection of Personal Data (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML), however the OECD Guidelines already included the principle of accountability which has been prominently resumed in the Article 29 Working Party's Opinion on the Principle of Accountability in 2010 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, all accessed 03 March 2014).

[59]Data protection accountability has recently been debated among privacy scholars (See Daniel Guagnin et al., eds, *Managing Privacy Through Accountability* (Houndmills: Palgrave, 2012.)) and is taken into account in the discussions of the current draft of the GDPR.

RFID-enabled travel cards (as used in many metropolis, e.g. Oyster Card in London and Octopus Card in Hong Kong) can serve as an example to display how new technologies challenge the right to privacy and data protection. The cards contain personal information about their holders so that they can be allocated to a single person to avoid abuse by others. Beyond that the RFID chips can be used to generate sophisticated traveler profiles,[60] or even consumer profiles, where the cards can also be used to pay in shops. Furthermore traveling profiles could be used to find suspicious traveling patterns, revealing potentially deviant behaviour (e.g. people which are using uncommon amounts and combinations of subway stations indicating activities from drug dealing to infidelities, as illustrated in Doctorow's Novel "Little Brother"). This shows that data which is not conceived as sensitive or potentially harmful can become such through combinations with other data.[61] Even data which is anonymized or de-identified can be used to generate outcomes which lead to issues from privacy infringements to discrimination. Furthermore the effectiveness of those approaches is doubted by scholars. Big Data analytics allow to draw unpredictable inference from information and by that undermine strategies of de-identification as by combination of anonymized data identities can be reconstructed.[62] New technologies such as RFID-chips make it difficult to keep track of which information is collected for which purposes and to keep track of the factual use of such data. The temptation for those gathering data to use it in new ways and generate new knowledge is high, and getting aware of such (unspecified) use can be very difficult. The discussions about putting data protection into practice through measures of accountability aims on making the use of data proactively transparent and traceable, but the practical implication is complicated.[63] There is

[60] Some RFID chips which use unique identifiers for initializing connections to RFID readers can also be tracked by third parties through this unique ID without any need to establish an authorized connection with the chip. See for instance http://www.spiegel.de/netzwelt/netzpolitik/sparkassen-pilotprojekt-kontaktlose-geldkarte-verraet-ihren-besitzer-a-831711.html.

[61] For a problematisation of inferring private data from large databases and efforts to avoid disclosure of private data see LiWu Chang and Ira S. Moskowitz, "An Integrated Framework for Database Privacy Protection", in *Data and Application Security*, ed. By Bhavani Thuraisingham et al., IFIP International Federation for Information Processing 73 (Springer US, 2001), 161–72; Stefan Sackmann, Jens Strüker, und Rafael Accorsi, "Personalization in Privacy-aware Highly Dynamic Systems", *Commun. ACM* 49, Nr. 9 (September 2006); Vassilios S. Verykios et al., "State-of-the-art in Privacy Preserving Data Mining", *SIGMOD Rec.* 33, Nr. 1 (März 2004): 50–57.

[62] See Paul Ohm, "*Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*," *UCLA Law Review* Vol. 57 (2010): 1701.

[63] Some scholars critizice that accountability could become just another ineffective bureaucratic measure, yet other scholars see potential of achieving stronger communication about data processing practices and verifiable accounts of data processors. The impact and effectiveness of accountability will depend on the actual implementation and the adoption by data processors. A number of contributions to the debate of the principle of accountability can be found in Daniel Guagnin et al., eds, *Managing Privacy Through Accountability* (Houndmills: Palgrave, 2012).

a general lack of transparency in profiling techniques[64] and also data processor's accountability is challenged by opaque practices and black boxed technologies inherent to data mining and profiling. This makes both the Security Safeguards Principle and the Openness Principle far from being taken into consideration. Individuals become more and more transparent, as public bodies, and even private companies, become more and more intrusive, moving on legal borderlines.

1.4.2.2 The Right to Non-discrimination

The right to non-discrimination "emanates from the general postulate of the equal dignity of human beings."[65] It constitutes a general principle in EU Law and lately has been enshrined as a fundamental right in Article 21 of the EU Charter of fundamental rights. It consists of a general principle of equality (i.e. similar situations have to be treated in the same way and different situations have to be treated differently) and of specific provisions developed in anti-discrimination legislations related to certain protected grounds (e.g. age, race, gender, religion, sexual orientation, etc.) and specific domain of application (i.e. labour market, vocational training, education, social security, health care, access to goods and services, criminal law).

The basic conceptual distinction in EU law is that between direct and indirect discrimination, both of which are prohibited in the EU law. Direct discrimination occurs when a person is treated less favourably than another and this difference is based directly on a forbidden ground. Indirect Discrimination occurs when apparently neutral criteria, practices or procedures have a discriminating effect on people from a particular protected group. This distinction is highly relevant in the context of profiling because rarely does the classification and categorization made by profiling techniques occur directly on forbidden grounds. More often the categorization is based on algorithms used to classify some attributes that can result as proxies of a protected ground. As stated by Romei and Ruggieri "the naive approach of deleting attributes that denote protected groups from the original dataset does not prevent a classifier to indirectly learn discriminatory decisions, since other attributes strongly correlated with them could be used as a proxy by the model extraction algorithm."[66] The best-known example is the one of "redlining", which

[64] See Mireille Hildebrandt, "*Profiling and AML*," in *The Future of Identity in the Information Society. Challenges and Opportunities*, ed. Kai Rannenberg, Denis Royer and Andre Deuker (Heidelberg: Springer, 2009a), 273–310 and Mireille Hildebrandt, "*Technology and the End of Law*," in *Facing the Limits of the Laws*, ed. Erik Claes, Wouter Devroe and Bert Keirsbilck (Heidelberg: Springer, 2009b), 443–465.

[65] Melik Özden, "*The Right to non-discrimination*," in *Series of the Human Rights Programme of the CETIM* (2011): 7.

[66] Andrea Romei and Salvatore Ruggieri, "*Discrimination Data Analysis: A Multi-disciplinary Bibliography*," in *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, ed. Bart Custers et al. (Berlin: Springer, 2013) 121.

is explicitly forbidden by US law. Redlining is used to identify the practice of denying products and services in particular neighbourhoods, marked with a red line on a map. Due to racial segregation or increasing demographic concentration of people similar for social class, employment condition and even nationality, people living in a particular neighbourhood may belong to a specific racial group or an ethnic minority. Hence, an apparently neutral attribute such as ZIP Code may turn into an indirect discrimination situation. In general profiling applied to marketing (web marketing, loan market, price determination, etc.) can easily hide practices of indirect discrimination. For this reason the research on data mining techniques that prevent discrimination (a kind of "discrimination proof data mining") is a fruitful research field.[67]

Another example is the smart approach to border surveillance. It relies on the use of technologies to automatically check the passengers at the border (so called smart borders). This use of technology consists of databases, sophisticated tools such as body, iris scanners and comprehensive programme of surveillance (e.g. Eurosur) whose final aim is to speed up border crossing for bona fide travellers, fight against illegal migration and enhance security. The proposed databases (Passenger Name Record, Registered Traveller Programme, Entry/Exit System) rely on an extensive collection of personal and non-personal data in order to differentiate among welcome and unwelcome travellers. Besides the risks related to privacy and data protection due to the use of biometrics and the lack of respect of the principle of purpose-binding and use limitation, the opacity of the logic behind the data mining procedure is in itself hard to harmonize with the obligation not to discriminate on prohibited grounds and above all raise huge concerns on the respect of human dignity.

The manifold risks which profiling imposes on fundamental values and rights as well as the complex effects of the implementation of this technology show that it is a challenge to provide adequate measures to protect European values and rights. The next section gives a brief overview of the state of this process in Europe.

1.5 So Far so Good – Regulating Profiling

In the current EU data protection legislation the word profiling does not appear. However. Article 15 of the Directive 95/46/EC (hereinafter, Data Protection Directive, DPD) concerns 'automated individual decisions' and thus is closely related to profiling. According to article 15(1): "every person has the right not to be subject to a decision which produces legal effects concerning him or significantly

[67] See Dino Pedreschi, Salvatore Ruggieri, and Franco Turini, "*The Discovery of Discrimination*," in *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, ed. by Bart Custers et al. (Berlin: Springer: 2013), 91–108.

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." At the same time, article 15(2) states an exception: "a person may nevertheless be subjected to an automated individual decision if that decision is taken: (a) in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests".

In the light of Article 15 of the DPD, it is relevant whether the processing is meant to evaluate a certain aspect of the person's behavior, character or identity on which a decision can be based. A decision based on a profile can comply with the law, but a natural person has to be involved in the process. To sum up, Article 15 does not take the form of a direct prohibition on a particular type of decision-making; rather, it directs each EU Member State to confer on persons a right to prevent them from being subjected to purely automated decisions in general.[68]

The directive proved unable to provide for sufficient protection in a fast-developing information society. In response to the technological developments of the past decades, the European Commission released in January 2012 a draft General Data Protection Regulation (GDPR) and a Data Protection Directive in the law enforcement context.

The GDPR contains one Article, Article no. 20, which concerns the data subject's right not to be subject to a measure based on profiling. It represents an evolution, with modifications and additional safeguards, of Article 15(1) and takes account of the Council of Europe's recommendation on profiling (Recommendation CM/Rec(2010)13). Compared to article 15, Article 20 better defines the right of a person not to be subject to a measure that is based solely on automated processing[69] and in particular clarifies that profiling cannot be based only on sensitive types of data (e.g. race or ethnic origin, religion, political opinion or sexual orientation), which would carry a too strong risk of discrimination on the basis of a prohibited ground.[70] Moreover it allows profiling in certain cases, but compared to article 15, the rules are stricter. Profiling is allowed when: (a) it is required for contracts, and

[68] Bygrave, Lee A., *Data protection law: Approaching its rationale, logic and limits* (The Hague: Kluwer Law International, 2002), 3.

[69] Article 20 par. 1: "Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour."

[70] Article 20 par. 3: "Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9".

the data subject has the right to request a human intervention; (b) it is permitted by law; or (c) under certain conditions, the data subject gives a free, explicit and informed consent.[71]

The novelty of this regulation is the provision contained in the fourth paragraph, which obliges data controllers to provide 'information as to the existence of processing" for an automated decision and about "the envisaged effects of such processing on the data subject".[72] As underlined in the advice paper released by Article 29 WP in May 2013[73] the GDPR does not include a definition of profiling. Blank spots like this prove that there is still a lot of work to do grasping profiling to enable an adequate regulation.

Another important aspect of learning more about profiling, its impacts, and the need for its regulation is getting to know about the awareness, the attitudes, and the activities of those authorities who are dealing with data protection and privacy on a day-to-day basis. That is why the project PROFILING has conducted a survey, which will be introduced in the next section.

1.6 National Data Protection Authorities' (DPAs) Responses to Profiling Questionnaire

In its aim to collect and compare information in the issue of profiling and, in particular automated profiling, the project PROFILING has developed a questionnaire – partly based on input from DPAs of Romania, Germany and Italy, the

[71] Article 20 par. 2: "Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or
(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards."

[72] See for weaknesses and strengths of this provision Bert-Jaap Koops, "*On decision transparency, or how to enhance data protection after the computational turn*," in *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, ed. Mireille Hildebrandt and Katja de Vries (Abingdon, Routledge, 2013), 189–213 and Mireille Hildebrandt, "*The Dawn of a Critical Transparency Right for the Profiling Era*," in *Digital Enlightenment Yearbook 2012*, ed. Jacques Bus et al. (Amsterdam: IOS Press, 2012), 41–56.

[73] Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf.

EDPS and the Council of Europe[74] – that was sent to the 28 European National Data Protection Authorities and Switzerland. The questionnaire aimed to gain an overview of the profiling landscape in European Member States, meaning: the current and future legal framework, the domains of application, the complaints and remedies procedures regarding the use of profiling techniques, the main risks and benefits for the fundamental rights and, finally, citizens' awareness on this topic.

Eighteen DPAs completed the questionnaire; three DPAs informed us that they would not be able to complete the questionnaire, mainly for reasons of lack of resources (but two provided some information related to the questionnaire); the other eight DPAs did not respond.[75] We started compiling and analyzing the answers of the 18 DPAs and the first findings of the profiling questionnaire were presented at CPDP in January 2014. Here, we present a more elaborate first analysis of the survey results.

1.6.1 Findings

1.6.1.1 Legal Aspects

Even if the understanding of the meaning of automated profiling varies among countries, it seems the DPAs agree in three principal characteristics of profiling:

- It is based on a collection, storage and/or analysis of different kind of data;
- and on automated processing using electronic means;
- with an objective of prediction or analysis of personal aspects or personality and/or the creation of profile.

Additionally, a fourth key aspect for some DPAs is that the profiling results in legal consequences for the data subject.

Fifteen out of eighteen DPAs express the need of a legal definition of profiling in order to clarify the definition and conditions it can be used. Three DPAs (Hungarian, Swedish and British) are not in favor of a definition by law because it would create misinterpretation and it would be difficult to provide an exhaustive definition including every imaginable profiling situation. All along the questionnaire, the UK DPA explains it might be better to see profiling as another form of personal data

[74] We thank the Italian, Romanian and German DPAs, the EDPS and the Council of Europe for their feedback to our pre-test questionnaire.

[75] Within 2 months we received the questionnaire completed by 18 DPAs: Austria, Bulgaria, Croatia, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, and United Kingdom. Three DPAs informed us that they would not be able to complete the questionnaire, mainly because of lack of resources: Denmark, Luxembourg and Netherlands. However, DPAs from Luxembourg and Netherlands provided some information related to the questionnaire. Eight DPAs did not respond: Belgium, Cyprus, Czech Republic, France, Latvia, Poland, Portugal and Spain.

processing which should be regulated within the normal data protection framework and should be treated as just one variant of data processing.

The two main risks of profiling techniques mentioned by DPAs are the challenge posed to individuals' liberties and fundamental rights at large (privacy and data protection, self-determination, dignity, personal integrity, personality, free speech and movement), and the lack of transparency and awareness about the existence of profiling. On the other hand, some DPAs also state that profiling can be a useful tool for tailored commercial services.

All DPAs (except Estonia) agree that profiling is a challenging area to be regulated. And a majority (10/18) agrees that all steps[76] should be subject to strict regulation both at EU and national level. It is important to notice that for the Greek and Italian DPAs, profiling should be considered and regulated as a whole process not in different stages.

All the European Union countries answering (except Greece) have transposed Article 15 of the Directive 95/46/EC.[77] Switzerland is not bound to the Directive but its national Data Protection Act includes a definition of profiling. In contrast, no country has implemented Recommendation (2010)13 of the Council of Europe on profiling. Thirteen DPAs out of seventeen have directly or indirectly implemented Article 7 of the Decision 2008/977/JHA of the Council Framework on individual automated decision in the context of police and judicial cooperation in criminal matters through a specific Law or Act.

Apart from national provisions transposing Article 15 of the Directive 95/46/EC, only two countries (Germany and Italy[78]) have specific legal provisions on automated profiling in their legal framework.

One question inquired whether DPAs have written internal guiding policy or public policy addressing data controllers on the implementation of Article 15 and 12 of Directive 95/46/EC with regard to automated decision based on profiling.

[76] As defined by the Council of Europe, mainly (1) collection and storage of data, (2) correlation and analysis of data and (3) practical application of profiles.

[77] According to article 15(1): "every person has the right 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." At the same time, article 15 (2) states an exception: "a person may nevertheless be subjected to an automated individual decision if that decision is taken: (a) in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests".

[78] Profiling is envisaged in the German Telemedia Act for the purposes of advertising, market research or in order to design the telemedia in a needs-based manner; in Italy, legal provisions on the assessment of income tax provide some type of profiling.

The questionnaire reveals that there are only few DPAs that have written policies[79] or have taken decisions[80] (4/18) on the implementation of those Articles 15 and 12. However, five[81] mentioned other policies related to them. It appears that those policies produced by DPAs are mostly addressed to data subjects' awareness and explain how to assert their rights rather than to DPA employees or to data controllers in order to clarify how to carry out the profiling.

Asked what are the main aspects that are important to be included in the General Data Protection Regulation (GDPR), first and foremost European DPAs call for a precise and broad definition of profiling and for adequate safeguards for individuals.

On the present draft of Article 20 of GDPR, eight DPAs estimate that it must be improved, while five support the new Article in whole or with some improvements. The major identified weaknesses of this Article concern the scope of the article, which should be broader and cover the entire processing of personal data, not only the result of the processing; some unclear terms that are dangerous for legal certainty (such as "legal effects" and "significantly affects" in the first paragraph and "suitable measures" or "safeguards" in the second paragraph); and the future use of sensitive data, which is unclear too. But they recognize that the fourth paragraph on data controller obligations is an improvement.

Nine DPAs out of twelve consider the Amendments from the European Parliament[82] as beneficial for establishing the final version of the Regulation (broader scope, clarifying the transparency obligations of data controllers, and hence improving data subjects' rights, and banning the use of sensitive data), but three do not support the recommendation of the report. Eight DPAs out of thirteen agree with

[79] Finland have a Guide on the processing of personal data in context of direct marketing and a Guide on a data subject's right of accede to his/her data which serve as official guidance to all); UK have Guides on subject access rights.

[80] Austria Data Protection Commission took nine decisions which may serve as guideline of their activities, available online at: http://www.ris.bka.gv.at/Dsk/; Italian DPA issued several decisions on profiling, for example on loyalty cards, on customer profiling as carried out by telecom operators, in employment sector and in respect of interactive TV.

[81] Hungarian former commissioner for data protection and freedom of information issued a report, in cooperation with the commissioner for ethnic and minority rights, on the processing of data relating to ethnic origin; Irish DPA provides general information and advice on the right of access of data subjects to their personal data, but not specifically tailored to the issue of automated profiling; Slovenia issued a couple of non-binding opinions on a credit worthiness system both to the data controller and to data subjects; Swedish DPA has published a leaflet on Article 12 that contains information about which public and private actors that process personal data and on how to proceed to exercise the right of access to personal data; Swiss DPA has provided guidance on subject access rights.

[82] Committee on Civil Liberties, Justice and Home Affairs of the European Parliament. Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 17/12/2012. Available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

the three main arguments of the EDPS[83] supporting Article 20, especially the recommendation to restore the right for individuals to submit their point of view, but five out of thirteen are in favour of a more far-reaching Regulation on profiling. The Advice paper of the Article 29 Working Party[84] which proposes a definition of profiling[85] and provides several suggestions[86] on how to improve article 20 of the GDPR is approved by all the answering DPAs excepting Ireland, which prefers the proposal version.

Concerning Article 9 of the proposed Directive on Data Protection in the Law enforcement sector (COM(2012)10 final), five DPAs[87] support the current version or do not have any comment or serious concern about it. Three DPAs have a mixed opinion because even if they consider Article 9 as sufficient, they still have some hesitation: the Italian DPA recognizes the modification of "decisions" by "measures" as an improvement but would open the scope to "sensitive data which may also be generated by profiling and not only included in such activity" and would prefer reference to "personal data" rather than to "data"; the Maltese DPA suggests that "more specific guidance could be necessary on the application of this article when this is incorporated under national law"; and the Romanian DPA recommends the adoption of "legislative acts regulating the use of profiles in order to avoid the excessive collection of data" and the inclusion of "additional safeguards in order to protect the data subjects' rights, similarly with those provided by article 20 of the draft Regulation". Three DPAs share the opinion that Article 9 is not sufficiently protective: the Austrian and Irish DPAs do not approve the addition of "solely" in the second paragraph (see explanation above); the Finnish DPA asks for sufficient safeguards and ensure the purpose limitation principle. Regarding the Greek answer, the DPA considers that "Whereas the corresponding in the Regulation article seems as the EDPS mentions in its Opinion to build upon the existing art. 15 of the

[83] Opinion of the European Data Protection Supervisor on the data protection reform package. 7/03/2012.

[84] Article 29 Data Protection Working Party. Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation. 13/05/2013.

[85] The definition proposed states that: "Profiling means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements".

[86] Main proposals for improvement concern the scope: "It [. . .] welcomes Rapporteur Albrecht's proposal to broaden the scope of Article 20 covering processing of personal data for the purpose of profiling or measures based on profiling. The Working Party regards this as a necessary step towards more legal certainty and more protection for individuals with respect to data processing in the context of profiling"; a greater transparency and control for data subjects; more responsibility and accountability of data controllers; a balanced approach to profiling and the role of EDPS.

[87] Bulgaria estimates there are good balances between individual rights and data controllers' activity and between the general prohibition for processing sensitive data and the exceptions); Hungary support the Article, Croatia, Slovakia and Sweden do not have any comments or objections.

Directive 95/46/EC and extends its scope, art. 9 of the proposed Directive essentially only reiterates the relevant art. 7 of the Council Framework Decision 2008/977/JHA. Moreover, the content of this article is inconsistent with the Regulation as (for example) it does not explicitly provide for the analysis and evaluation of behaviour, whilst the prohibition of a measure based on automated processing of personal data (profiling) is conditioned only on the producing "an adverse legal effect" and not "a legal effect' as cited in the Regulation. Additionally, the relevant subject rights are specifically (with regard to the profiling) detailed in the Regulation, while similar provisions are absent in the proposed Directive. In our opinion the provisions of the Directive need to be more in line with the equivalent ones of the Regulation".

1.6.1.2 Domains of Application

We listed a number of domains where profiling is likely to be used, inviting the DPAs to identify in which of them profiling applied in their country at the national level. Finance sector (credit rating, anti-money laundering) is the most incline to apply profiling (18 DPAs/18), followed by marketing (15/18), social media and web and behavioral advertising (13/18), criminal investigation and employment (11/18), intelligence, national security, counter-terrorism, healthcare domain (including insurance) (10/18) and border control (9/18). Education domain resorts to profiling in only five countries. Irish DPA underlines that profiling happen in "insurance quotation generally" and Bulgarian DPA also mentions domains which were not predetermined: "namely-sociological agencies" and "TV and radio programs rating research".

The compilation of answers reveals that the most challenged domain for the DPAs is marketing (10 DPAs out of 14) followed by finance – credit rating, anti-money laundering – (9/14), social media and Internet, behavioral advertising (7/14), employment (6/14), healthcare (5/14), criminal investigation (4/14) and, finally, border control and national security (3/14).

One question related to the existence of any national law/regulation on the collection of personal data and on the use of such database. Numerous countries have pass regulations, through their Data Protection Act or through specific regulations and even, through Code of conduct approved by the DPA (Bulgaria).

1.6.1.3 Fundamental Rights

The main fundamental rights and principles challenged by profiling are private life and data protection, freedom rights (such as human personality, self-determination, free development, freedom of expression and movement, portrait rights or personal autonomy) and respect of the principles of purpose limitation, proportionality and necessity. And the risk of infringement of citizens' right of the protection of their personal data is considered higher in the financial domain (mentioned by 14 DPAs out of 14).

Article 20 of Directive 95/46/EC envisages a "prior checking", means that DPA should examine processing operations likely to present specific risks data subjects' rights prior to the start thereof. We asked whether the DPA envisage any specific procedure to be carried out to assess possible cases of infringements of fundamental rights and freedoms in profiling processes. Only 9 DPAs[88] out of 18 answered they have this possibility. Nevertheless, among the DPAs which do not envisage a prior checking, the Finnish DPA pointed out that it can control codes of conduct draft by controllers, in Germany prior checks are carried out by the data protection officers of public authorities and of private companies and the Romanian DPA can perform a preliminary control before the start of certain processing operations which are likely to present special risks for the persons' rights and liberties.

Thinking about concrete cases of infringements, according to the DPAs, the fundamental rights or principles most challenged by profiling are the right to data protection, followed by the right to privacy, the right to non-discrimination, the right to transparency, the right to autonomy and self-determination, and the right to due process in the rank of mentions.

1.6.1.4 Procedure to Complaint

A general procedure for data subjects' to directly complain about a data protection violation to the DPA can be designed following national legislations: a request is submitted by the plaintiff to the DPA against an act or omission of the data controller violating the law or his/her rights. If the complaint is admissible, the DPA initiates an investigation and then pronounces a decision (which is generally not as powerful as a court decision) in order to correct the violation. The individual is generally kept informed on the developments and notified of the final decision. The reasons for complaining are numerous (complaints based on violation of data subject rights or data breach) and concern various domains, but principally occur in the marketing domain.

About half of the DPAs have already received a complaint on automated profiling. Fifteen DPAs out of eighteen mention having already received complaints through legal entities, institutions, associations, law firms, attorney, representative to natural persons, bodies, organizations, NGOs, Trade Unions, foundation or local and central public authorities. All the DPAs can also investigate data processing practices at their own initiative but only 7 out of 15 have already used this right.

Article 23 of the actual Directive on data protection invites Member States to provide a compensation for "any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions". According to DPAs' answers, such compensation mechanisms

[88] Austria, Bulgaria (but only for sensitive data), Croatia (not explicitly mention in the Data Protection Act), Hungary (audit and impact assessment envisaged as a prior checking procedure), Italy, Malta, Slovakia, Slovenia, UK (prior checking is in the Data Protection Act but has never been enforced).

are usually envisaged in European countries.[89] If the national Data Protection Acts do not necessarily foresee such compensation, data subjects can resort to civil, penal or administrative procedures. In some countries there are also other entities able to take care of it, such as the Competition Authority or the Authority for Consumer Protection in Hungary. On the relevant court cases on automated profiling, only the Italian DPA mention that a case is currently pending before the Italian Supreme Court of Cassation regarding the case of profiling carried out by the National Printing Institution on its employees. The case originated from the challenging of a decision adopted by the Italian DPA on 21 July 2011.[90]

One question concerned the existence of a specific national training, instruction or guidance on profiling for the DPA officials. There are only three countries where DPA officials receive this kind of training. The Finnish DPA has issued a number of guidance (particularly on marketing practices), the Italian DPA has organized some internal seminars regarding the most controversial aspects of profiling and the Slovakian DPA performs training of its employees but not only in the area of profiling.

1.6.1.5 Awareness

Among a list of reasons likely to influence data subjects' decisions to submit a complaint in case of automated profiling that significantly affects them, DPAs principally mention the awareness of the legal effects of individual measures based on profiling (15/17), closely followed by the awareness of their fundamental rights, transparency of the profiling process and to be informed that a certain decision is (partly) based on profiling (14/17 for each). As a corollary, the main limitation for data subjects' understanding of profiling risks and implications according to the DPAs is considered to be a lack of knowledge of the existence of the profiling and of transparency over the processing.

---

[89] Austria (before a court but not in practice), Bulgaria (under civil law not in the Data Protection Act which foresee administrative penalties-fines/sanctions), Croatia (before a court of general jurisdiction), Estonia (no precision), Finland (before a district court in civil procedure), Germany (the DPA of the non-public sector can impose a fine and civil procedure also apply), Greece (under civil procedure), Hungary (through civil and other procedures), Ireland (no direct compensation before the DPA but possible through civil procedure), Italy (judicial authorities competence), Lithuania (civil court competence), Malta (civil court competence), Romania (court of Law competence), Slovakia (not under the DPA but through civil Court), Slovenia (the civil law give competence to Court and relevant Authorities), Sweden (the Data Protection Act envisage compensation but not specific to profiling), UK (court competence). Switzerland did not answer.

[90] Answer of the Italian DPA ('Garante'): "*On 21 June 2011, our DPA adopted a decision concerning the profiling carried out by the National Printing Institution on its employees, in particular as a result of the monitoring of the employees' activities on the Internet. In such decision our DPA prohibited the unlawful data processing operations which had been carried out, inter alia, without informing the data subjects and notifying the processing to the Garante (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1829641*).*"

DPAs use many ways to improve the awareness of the general public about their rights as regards data collected and used for profiling purposes: websites, written documentation (reports, guidelines, newsletter, leaflet . . .), internal and external seminars/conferences, media contributions, annual surveys and hotlines. Ten DPAs out of eighteen have already produced a report or study on the issue of profiling to increase data subjects' awareness. Finally, almost all DPAs think data subjects' awareness of automated profiling and its possible implications should be increased. In order to perform this aim, they suggest using numerous ways/tools and to involve private entities and consumer protection bodies.

1.7 Conclusions

The respect of fundamental rights and values is essential to guarantee democracy and the rule of law. But in a world where new technologies fundamentally change social relations and practices, it is not always clear what human rights and the rule of law actually mean, and how respect for human rights can be safeguarded. This paper has delivered an overview of the technological evolution and elaborated the socio-technological preconditions of profiling. It demonstrated how the new technological advances change social practices and how pose threats to fundamental rights and values of European societies when applied in various fields and contexts. Despite these critical implications, the DPA questionnaire highlights a lack of a common definition and of a mutual vision on how to deal with the challenges emerging from profiling.

The survey showed that national legal frameworks on automated profiling within the European Union and Switzerland look quite similar. Moreover, there is a sense of global coherence between the DPAs' points of view on the understanding of automated profiling, even if it is a new and fast-moving domain. Furthermore a majority of DPAs express the need for legal regulation. However, when discussing future regulation, discrepancies appear amongst the DPAs, both concerning Article 20 of the GDPR and Article 9 of the proposed Directive. Whereas one group supports the new proposal as is, the other group is calling for reinforcing its data protection measures. A full discussion is needed in order to better identify dangers associated with the use of automated profiling and to identify the importance given to fundamental rights protection, in particular data protection.

DPAs within the European Union and Switzerland have received only few complaints on profiling. This can be due to the novelty of the use of automated profiling, and also to a general lack of awareness by the citizenry. The awareness of the legal effects of individual measures based on profiling, and the awareness of citizens' fundamental rights and of profiling as a process are factors likely to influence data subjects' abilities to submit complaints in cases of automated profiling that significantly affect them. Our survey reveals that even though data subjects' awareness is an important and a highly worrisome issue for DPAs, there is a lack of guidance dedicated to profiling. Therefore, it is important for DPAs to

provide complete and understandable information on the concept of profiling, its purposes and the potential risks and implications of this method.

To conclude, national data protection authorities state that profiling is a challenging and risky activity. They now need to take the necessary measures to improve the training of employees, make data controllers aware of their responsibilities; and in particular, enhance citizen awareness, for the lack of knowledge about profiling and the lack of transparency in information processing are the main limitations for data subjects' understanding of profiling's risks and implications.

The new issues posed by technological development challenge current and future regulation to adequately respond to matters related to self-determination especially regarding the problem of the general applicability of data protection to profiling and the efficiency of technical approaches such as anonymity and de-identification. It is paramount to enhance the critical thinking on the possibilities, as well as the limitations, of improving data protection in the current and future technological setting.

References

Anrig, Bernhard, Brown, Will and Gasson, Mark, "The Role of Algorithms in Profiling," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 65–87, Dordrecht: Springer, 2008.

Baskarada, Sasa and Koronios, Andy, "Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension." *Australasian Journal of Information Systems*, Vol 18, No 1 (2013): 5–24.

Brakel, Rosamunde van and Paul de Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies." *Cahier Politiestudies* 20 (2011): 163–192.

Bygrave, Lee A. *Data protection law: Approaching its rationale, logic and limits*. The Hague: Kluwer Law International, 2002.

Calders, Toon and Žliobaitė Indrė. "Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures." In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 43–57. Berlin: Springer, 2013.

Canhoto, Ana and Blackhouse, James, "General Description of Behavioural Profiling," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 47–63, Dordrecht: Springer, 2008.

Chang, LiWu, und Ira S. Moskowitz. "An Integrated Framework for Database Privacy Protection" In *Data and Application Security*, herausgegeben von BhavaniThuraisingham, Reind van de Riet, Klaus R. Dittrich, und ZahirTari, 161–72. IFIP International Federation for Information Processing 73. Springer US, 2001. http://link.springer.com/chapter/10.1007/0-306-47008-X_15.

Clarke, Roger, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance". In *Journal of Law and Information Science* 4, 2 (1993): 403–419.

Degele, Nina, *Einführung in die Techniksoziologie*. Stuttgart: UTB, 2002.

Deleuze, Gilles. "Postskriptum über die Kontrollgesellschaften" In *Unterhandlungen 1972–1990*, Gilles Deleuze, 254–262. Frankfurt a.M.: Suhrkamp, 1992.

Deutscher Bundestag, "Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen." *Drucksache 17/11582*, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014.

Deutscher Bundestag, "Computergestützte Polizeitechnik bei Polizeibehörden." *Drucksache 17/8544 (neu)*, 06 Feb 2012, http://dipbt.bundestag.de/dip21/btd/17/085/1708544.pdf, last accessed 01 April 2014.

Finn, Rachel L, David Wright and Michael Friedewald. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth et al., 3–32, Dordrecht: Springer, 2013.

Fraunhofer. IAIS, "*Big Data – Vorsprung durch Wissen. Innovationspotenzialanalyse*," http://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents/FraunhoferIAIS_Big-Data-Analyse_Doku.pdf, last accessed 01 April 2014.

Fuster, Gloria González, Gutwirth Serge, and Ellyne Erika. "Profiling in the European Union: A high-risk practice" *INEX Policy Brief* 10 (2010): 1–12.

Gellert, Raphael and Serge Gutwirth. "Beyond accountability, the return to privacy?" In *Managing Privacy through Accountability*, edited BY Daniel Guagnin et al., 261–284. Houndmills: Palgrave Macmillan, 2012.

Guagnin, Daniel et al., eds. *Managing Privacy Through Accountability*. Houndmills: Palgrave, 2012.

Gutwirth, Serge and Hildebrandt Mireille. "Some Caveats on Profiling." In *Data protection in a profiled world*, edited by Serge Gutwirth, Yves Poullet and Paul de Hert, 31–41. Dordrecht: Springer, 2010.

Gutwirth, Serge and Paul de Hert. "Regulating profiling in a Democratic Constitutional State." In *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 272–293 Dordrecht: Springer, 2008.

Hildebrandt, Mireille. "The Dawn of a Critical Transparency Right for the Profiling Era". In *Digital Enlightenment Yearbook 2012*, edited by Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides, 41–56. Amsterdam: IOS Press, 2012.

Hildebrandt, Mireille. "Defining profiling: a new type of knowledge?" In *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 17–47. Dordrecht: Springer, 2008.

Hildebrandt, Mireille. "Profiling and AML," in *The Future of Identity in the Information Society. Challenges and Opportunities*, edited by Rannenberg Kai, Denis Royer and André Deuker, 273–310. Heidelberg: Springer, 2009a.

Hildebrandt, Mireille. "Profiling: from Data to Knowledge. The challenges of a crucial technology." *DuD Datenschutz und Datensicherheit*, 30, 9 (2006): 548–552.

Hildebrandt, Mireille. "Technology and the End of Law." In *Facing the Limits of the Law*, edited by Erik Claes, Wouter Devroe and Bert Keirsbilck, 443–465. Heidelberg: Springer, 2009b.

Hildebrandt, Mireille. "Who is Profiling Who? Invisible Visibility." In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 239–252. Dordrecht: Springer, 2009c.

Hunko, Andre, *"Suchbewegungen zu Data Mining-Software gehen über gesetzlichen Auftrag des BKA hinaus,"* 17 March 2014, http://www.andrej-hunko.de/presse/1934-suchbewegungen-zu-data-mining-software-gehen-ueber-gesetzlichen-auftrag-des-bka-hinaus, last accessed 26 March 2014.

Koops, Bert-Jaap (2013). "On decision transparency, or how to enhance data protection after the computational turn." In *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, edited by Mireille Hildebrandt and Katja de Vries, 189–213. Abingdon: Routledge.

Koops, Bert-Jaap. "Technology and the Crime Society: Rethinking Legal Protection." *Law, Innovation & Technology*, 1, 1 (2009): 93–124.

Latour, Bruno "Technology is Society Made Durable." In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 103–131. London: Routledge, 1991.

Lianos, Michaelis and Mary Douglas. "Dangerization and the End of Deviance: The Institutional Environment." *British Journal of Criminology* 40, 2 (2000): 261–278.

Lyon, David "Surveillance as Social Sorting. Computer Codes and Mobile Bodies," in *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 13–31. City: Psychology Press, 2003.

Marx, Gary and Reichman Nancy. "Routinizing the Discovery of Secrets: Computers as Informants". In *American Behavioral Scientist*, 27, 4 (1984): 423–452.

Monahan, Torin "Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance." *Surveillance and Democracy issue (*2010): 91–110.

O'Malley, Pat. "Risk, power and crime prevention." *Economy and Society* 21, 3 (1992): 252–275.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 (2010): 1701–1777.

Özden Melik "The Right to non-discrimination", in *Series of the Human Rights Programme of the CETIM*, 2011.

Pedreschi, Dino, Ruggieri Salvatore, Turini Franco. "The Discovery of Discrimination." In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 91–108. Berlin: Springer, 2013.

Polakiewiecz, Jörg. "Profiling – The Council of Europe's Contribution." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth et al., 367–377, Dordrecht: Springer, 2013.

Rodotà, Stefano. "Data Protection as a Fundamental Right." In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 77–82. Dordrecht: Springer, 2009.

Romei, Andrea and Ruggieri Salvatore. "Discrimination Data Analysis: A Multi-disciplinary Bibliography." In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 109–135. Berlin: Springer, 2013.

Roosendaal, Arnold. *Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts*, Oisterwijk: Wolf Legal Publishers.

Rouvroy, Antoinette and Yves Poullet. "The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy." In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 45–76. Dordrecht: Springer, 2009.

Sackmann, Stefan, Strüker, Jens, and Accorsi, "Personalization in Privacy-aware Highly Dynamic Systems". *Commun. ACM* 49, Nr. 9 (September 2006): 32–38. doi:10.1145/1151030.1151052.

Scharff, Thomas. "Erfassen und Erschrecken. Funktionen des Prozeßschriftguts der kirchlichen Inquisition in Italien im 13. Und frühen 14. Jahrhundert." In *Als die Welt in die Akten kam. Prozeßschriftgut im europäischen Mittelalter*, edited by Susanne Lepsius and Thomas Wetzstein, 255–274. Frankfurt a.M.: Vittorio Klostermann, 2008.

Schermer, Bart. "Risks of profiling and the limits of data protection law." In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 137–154. Berlin: Springer, 2013.

Solove, Daniel J. "I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review*, 44 (2007): 745–772.

Solove, Daniel J. *Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004.

Streibich, Karl-Heinz, "Big Smart Data. MehrwertfürUnternehmen", (paper presented at the Big Data Days, Berlin, Germany, November 11–12, 2013).

Susanne Krasmann, "Der Präventionsstaat im Einvernehmen. Wie Sichtbarkeitsregime stillschweigend Akzeptanz produzieren." In *Sichtbarkeitsregime: Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*, edited by Leon Hempel, Susanne Krasmann and Ulrich Bröckling, 53–70. Wiesbaden: VS Verlag, 2010.

Trudel, Pierre. "Privacy Protection on the Internet: Risk Management and Networked Normativity." In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 317–334. Dordrecht: Springer, 2009.

Vedder, Anton. "KDD: The challenge to individualism." *Ethics and Information Technology* (1999): 275–281.

Verykios, Vassilios S. et al., "State-of-the-art in Privacy Preserving Data Mining". *SIGMOD Rec.* 33, Nr. 1 (März 2004): 50–57. doi:10.1145/974121.974131.

Zakaria, Fareed. "The rise of illiberal democracy." *Foreign Affairs*, 76, 6 (1197): 22–43.

Zarsky, Tal Z., "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 (2002–2003): 1–56.