Profiling Technologies in Practice
Applications and Impact on Fundamental Rights and Values

Edited by Niklas Creemers, Daniel Guagnin and Bert-Jaap Koops
With contributions by Francesca Bosco, Niklas Creemers, Elena D'Angelo, Valeria Ferraris, Daniel Guagnin, Mireille Hildebrandt, Bert-Jaap Koops, Bogdan Manolea, Arnold Roosendaal and Elise Vermeersch

Profiling Technologies in Practice

Applications and Impact on Fundamental Rights and Values

Edited by Niklas Creemers, Daniel Guagnin and Bert-Jaap Koops
With contributions by Francesca Bosco, Niklas Creemers, Elena D'Angelo, Valeria Ferraris, Daniel Guagnin, Mireille Hildebrandt, Bert-Jaap Koops, Bogdan Manolea, Arnold Roosendaal and Elise Vermeersch

ISBN: 9789462402416

Published by:
Wolf Legal Publishers (WLP)
PO Box 313
5060 AH Oisterwijk
The Netherlands
E-Mail: info@wolfpublishers.nl
www.wolfpublishers.com

All URLS have been valid in time of printing, and no guarantee can be given that they will stay.

Table of Contents

I. Profiling Technologies and Fundamental Rights. An Introduction

Francesca Bosco, Niklas Creemers, Valeria Ferraris, Daniel Guagnin, Bert-Jaap Koops and Elise Vermeersch[1]

The global technological evolution of information and communication has modified the behaviour of citizens regarding their personal data and the use of this data by private companies and Public Authorities. Technological advancement has fuelled the digitalization of our societies. Infrastructure is increasingly based on digital devices and software. Today, mediated communication is mostly digital communication, making information easy to process and store as data. New potential for gathering data raises hopes for developing more advanced ways to manage societies. However, the availability of new sources of information requires the use of new and efficient analytical tools, able to collect, store and process huge amounts of data in order to extract usable information. These tools are typically utilized in technologies such as data mining[2].

Profiling can be understood as a specific data mining method. In this perspective, profiling is regarded as a (semi-)automated process used 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 discover patterns and probabilities.

Using actuarial methods in this context is supposed to generate prognostic information to anticipate future trends and to forecast behaviour, processes and/or developments. The aim is to develop strategies in order to manage uncertainties of the future, while still in the present. In this regard, analytical tools, such as profiling, can be understood as important facilitators and elements of a preventive paradigm that can be found in diverse societal contexts (see Krasmann 2010, O'Malley 1992). But these new data processing tools also result in the data subject's loss of control over his/her personal data and over the decisions being made based on this information. Therefore, these new technologies also draw fears and scepticism as they impose threats on some of the core values

---

1 This chapter is based on a previously published paper from Francesca Bosco, Niklas Creemers, Valeria Ferraris, Daniel Guagnin, and Bert-Jaap Koops. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities." Dordrecht: Springer 2015.

2 Han and Kamber define data mining as "automated or convenient extraction of patterns representing knowledge implicitly stored or catchable in large databases, data warehouses, the Web, other massive information repositories or data streams" (Han and Kamber 2006, xxi).

and principles of European societies. Key challenges that have been identified by scholars include the infringement 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 to privacy, data protection, and non-discrimination.

Scholars are not alone in their concern for the risks related to the automated processing of data. A number of organisations, Institutes and Authorities (such as the European Parliament, the Council of Europe, the Article 29 Working Party, the national Data Protection Authorities and the European Data Protection Supervisor) regularly bring attention to the importance of respecting and reinforcing data protection, privacy rights and other fundamental rights in the context of technological evolution.

This volume has been prepared within the framework of the project entitled PROFILING - Protecting Citizens' Rights Fighting Illicit Profiling[3], financed by the European Commission's Directorate-General for Justice, under the Fundamental Rights and Citizenship programme. The project has been implemented by a consortium of five European partners, led by the United Nations Interregional Crime and Justice Research Institute (Turin, Italy), and including Amapola (Turin, Italy), the Romanian Centre for European Policies (Bucharest, Romania), the Technical University of Berlin (Berlin, Germany) and Tilburg University (Tilburg, The Netherlands). The project has focused on identifying and tackling the challenges posed by technology to the fundamental right to data protection. It was aimed at addressing some major issues, such as identifying the risks related to the extensive use of profiling, identifying the level of awareness of the responsible authorities of the Member States on the risks deriving from the use of profiling and assessing the countermeasures adopted in all EU Member States. As a first step, this introduction provides the working definition of profiling, as elaborated within the framework of the project, and tries to demonstrate how fundamental rights and values of European societies are endangered by the application of profiling in various contexts and the possible effects of the review of the current legal regulations.

Following this introduction, the volume contains two parts which are based on the project outcomes. The first one (chapter II) presents the results of a survey conducted with the 28 European National Data Protection Authorities regarding profiling issues. The questionnaire attempted to gain an overview of the profiling landscape in European Member States, including the current and future legal framework, the domains of application, the complaint and remedy procedures regarding the use of profiling techniques, the main risks and benefits for fundamental rights and citizens' awareness on this topic.

---

[3] More information available at: http://profiling-project.eu/

The second part presents three fieldwork studies carried out in Romania, Italy and Germany. The first case study (chapter III) aims at identifying what are the current profiling practices and their respective privacy implications related to e-commerce in Romania. In particular, it investigates current practices and examines the vision of local actors concerning the process – both in technical and legal terms – while also trying to probe certain key-issues from a data protection point of view. The second case study (chapter IV), implemented in Italy, examines the involvement of automated decision making and profiling in border control. This study focuses its attention on the newly developed Schengen Information System II and on Eurodac, examining how these biometric databases are implemented and used in Italy for immigration control. Moreover, it explores development at European Union level in terms of new databases for migration control (the so called smart borders package) and the information exchange initiatives aimed at increasing surveillance in the Mediterranean area. The third case study (chapter V) investigates the collection, storage and evaluation of digital information by German police authorities, especially in their efforts to combat so-called political extremism and/or politically motivated crime. An analysis is also provided regarding how the use of digital information, databases and data analysis tools changes police practices and of the effects these changes have on civil rights as well as fundamental democratic values.

The final chapter discusses the mismatch between current data protection laws and profiling activities and the tension between potential benefits and threats in fundamental rights. Arnold Roosendaal argues that instead of regarding this as a dichotomy, it is key to think of innovative solutions in order to reduce the threats and enable privacy friendly services and technologies. Privacy could thus become a competitive argument.

This edition is intended both for presenting to the public the main results of the PROFILING project and for providing inputs to the various stakeholders involved in the field of automated profiling in order to expand the knowledge of this phenomenon and give useful information to policy-makers, governments and civil society.

1. Profiling: Finding a definition

The formation of a common definition for profiling has not yet been agreed upon. The term profiling, in itself, evokes a range of meanings, employed in both specialized and non-specialized scenarios. The issue of forming a definition of profiling represents a challenge for policy makers and socio-legal scholars, especially since current literature on the subject is technical rather than explanatory.

Gary T. Marx provided one of the oldest definitions of profiling in a paper that analyses systems of data searching. This definition refers almost exclusively to

profiling in the sector of law enforcement and states that profiling (as 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" (Marx and Reichman 1984, 429). Roger Clarke, slightly less than a decade later, 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" (Roger 1993, 403). Lee A. Bygrave, remarked that: "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" (Bygrave 2002, 301). Subsequently, Mireille Hildebrandt defined 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)" (Hildebrandt 2009a, 275). This has served as the main working definition of profiling and represents the best attempt at forming a universal definition of the term. Profiling allows for the visualization of patterns that are otherwise "invisible to the naked human eye" (Hildebrandt 2009c, 241). They are based on correlations found in data sets, and cannot be "equated with causes or reasons without further inquiry; they are probabilistic knowledge" (Gonzalez Fuster, Gutwirth and Ellyne 2010, 2). Profiling represents a shift from the idea that knowledge is the result of tested hypotheses. It generates hypotheses: "The correlations as such become the 'pertinent' information, triggering questions and suppositions" (Gonzalez Fuster, Gutwirth and Erika 2010, 2). With advancements in technology and the increased capacities of databases, profiling is able to bring forth new ways on generating and utilizing information. However, these advancements also create ramifications in the ever more complex profiling process, altering the role of human data controllers. Hildebrandt divides profiling into three categories: 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 it 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" (Hildebrandt 2008, 28) Conversely, in autonomic profiling the role of the human is extremely minimal and the machine has control of the process of decision making (see Hildebrandt 2006 and 2008). Autonomic profiling "goes one step further than automated profiling" (Hildebrandt 2006, 550). Methods used in profiling can also be characterized by their objectives and application,

in addition to their level of automation. Profiling can be applied to both groups and individuals: the techniques that identify and represent groups can also focus on individuals (see Roosendaal 2013,Vedder 1999) Furthermore, profiling either relies on data collected from one single person or group in order 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. Distributive group profiling and non-distributive group profiling are further classifications falling under the general category of group profiling (see Vedder 1999). Distributive group profiling identifies a certain number of people having the same attributes and characteristics. Non-distributive group profiling, on the other hand, identifies a number of people who do not share all of the characteristics of the group's profile. The above-mentioned distinctions provide an idea as to the various categorizations of profiling and their respective applications.

As regards a definition of profiling for the purposes of this book, we are utilizing the definition proposed within the framework of the PROFILING project, which specifically makes reference to the evolution of technology associated with profiling and to the purposes for employing the profiling process in society.

> *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.*

2. The Threat of Profiling for Fundamental Rights and Values

The creation of knowledge represents the core of the profiling process as it allows the anticipation of future trends and the prognostication of behaviour, processes or developments. Proponents of profiling tout its potential for gathering data and conducting analysis, claiming that the limited reliability of data mining will improve as technological capabilities increase and eventually organizations will be able to address negative developments in a pre-emptive manner. Early detection of tax fraud and pandemics are examples of issues that could be addressed through the use of big data analytics. At the same time, fundamental rights such as the rights to privacy, data protection, and non-discrimination, among others, could be put at risk through profiling and its associated practices. The threat of infringement on these rights is growing as the use profiling expands throughout the world.

2.1 Fundamental Values

Liberal democracy (see Zakaria 1997) and profiling are at odds with one another due to their inherent characteristics. Profiling is considered a glamour technology: it gives the idea that human beings can attain unforeseeable knowledge that allows for the making of better decisions. But the dark side of profiling is that it makes "invisible all what cannot be translated into machine-readable data" (Gutwirth and Hildebrandt 2010, 33). Due to the complexity of the applied algorithms present within automated profiling, human beings cannot properly intervene and repair the bias consequently created by the machine not being able to read certain data. As a result, "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" (Gutwirth and Hildebrandt 2010, 33). By not considering some aspects of an issue profiling can lead to the making of ineffective and wrong decisions, or, in severe cases, result in serious risks and damages for a population. Human intervention is not the only aspect that is reduced during the decision-making process. Citizens have hardly any access to the process of constructing and applying of profiles. The resulting unbalanced distribution of power is detrimental to the workings of a liberal democracy (see Solove 2004) and to balancing knowledge asymmetries (see Gutwirth and Hildebrandt 2010) between citizens and the government. Knowledge asymmetries are not uncommon, but profiling technologies have the capacity to push them to a new high. In most cases, citizens are neither aware of the information in circulation, nor in the ways in which it can be utilized in the future. This is particularly the case when profiles are constructed from data that is not of the data subject's own, leading to the information being used to take decisions about the subjects without their involvement. There is no simple solution for data protection in the foreseeable future, and this issue is being exacerbated via some sophisticated profiling technologies like Behavioural Biometric Profiling (BBP), which "do not require identification at all" (Hildebrandt 2009c, 243). If the position that citizens enjoy vis-à-vis 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 not only relates 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" (Rouvroy and Poullet 2009, 51). As previously mentioned, digitization of everyday life has led to opaque ways of data gathering, exchange and processing. Technologies like profiling do not leave much space for

autonomy and self-determination (see Hildebrandt 2009c). The use of profiling in the field of healthcare can be helpful and harmful at the same time. E-health and m-health (electronic health and mobile health) technology allow for the around-the-clock monitoring of factors, such as a person's diet, activities, medical treatment, condition of physical maladies, etc., paving the way for a revolution in the areas of disease control, treatment, finding cures, and more. There is also the potential for gathering multi-source information about patients' that could be used in conducting an actuarial assessment of lifestyles in order to build risk categories that are not only used for "individualised" treatments, but also for developing "individual" insurance fees or other incentives to make clients adapt to certain lifestyles. However, the categories created through profiling are not individualized in the least, being derived from abstract calculations conducted on the premise of profit maximization. This economic logic is transferred to individual lifestyle choices by rewarding behaviours assessed as low risk or healthy, while penalizing the ones that are considered high risk for accidents or diseases. Although profiling in this context is supposed to empower healthy lifestyles, it also undermines individuals' autonomy, and it facilitates the economisation of everyday life by addressing individuals, not as individuals but as bundles of risks and behavioural probabilities, effectively reducing them to profiles (see Deleuze 1992). E-health is only one example of an 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" (Koops 2009, 104). The narrative linking these *small surveillance societies* involves the creation of knowledge taken from certain populations, which has the power to influence and steer individuals, groups, and social processes. This facilitates an environment where informational self-determination and autonomy are jeopardised for the idea of an advanced control over social developments.

2.2 Fundamental Rights

The fundamental values presented earlier on are very much interrelated with the rights to privacy, data protection and the protection from discrimination. As highlighted 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 systems" (Rodotà 2009, 78) As Rouvroy and Poullet point out, data protection is vital in sustaining a vivid democracy. The right to non-discrimination is equally important (see Rouvroy and Poullet 2009, 57) and it is not by chance that in two recent profiling-related cases, the European Court of Justice invoked legislation on both Data Protection and anti-discrimination in order to protect citizens' rights.

2.2.1 The Rights to Privacy and Data Protection

Without attempting to define the various notions of privacy (see Solove 2007), it is beneficial to re-examine how privacy and data protection interact with one another. Following Gellert and Gutwirth, most privacy definitions can be summarized as 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 undesired exposure (see Gellert and Gutwirth 2012). Data protection law, however, is created to ensure the safety of personal data while also facilitating the free flow of information. In this scenario, privacy is a rather vague issue. While data protection is related to transparency (see Gellert and Gutwirth 2012), privacy is broader in the sense that privacy covers more than just personal data, and the misuse of personal data can affect more than someone's privacy. As previously mentioned, modern technology has the capacity to create digitalized data that can be used in automated processing and, therefore, profiling challenges the concepts of privacy and data protection. As technologies develop, these concepts have to evolve and catch up with an environment of constant progress in which: "its content varies from the circumstances, the people concerned and the values of the society or the community" (Trudel 2009, 322). Profiling technologies, as shown in this book, lead to more black boxing and more obscurity related to data processing. It is actually questionable as to how the factual use of data can be made transparent. In order to build an exhaustive framework representing threats to the right to privacy and the right to data protection, the OECD Privacy Principles[4] are regarded as terms of reference and as one of the most comprehensive and commonly used privacy frameworks.[5] The 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

---

[4] 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 (2014) "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*".

[5] The basic data protection principles largely overlaps with the principles outlined in the Council of Europe's (1982) Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal and the Directive 95/46/EC on the Protection of Personal Data, however the OECD Guidelines already included the principle of accountability which has been prominently resumed in the Article 29 Working Party's (2010) Opinion on the Principle of Accountability.

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.[6]

RFID-enabled travel cards (as used in many metropolises, e.g. Oyster Card in London and Octopus Card in Hong Kong) can serve as an example for displaying how new technologies challenge the right to privacy and data protection. The cards contain personal information about their individual holders, so as not to be abused by others. Going a step further, the RFID chips can be used to generate sophisticated traveller, profiles[7] and even consumer profiles in cities where the cards can also be used to pay in shops. For the issue of traveller profiles, these could be used to track suspicious travel patterns, revealing potentially deviant behaviour (e.g. people using uncommon routes and combinations stations when taking the subway, indicating activities ranging from drug dealing to infidelity. This exemplifies the fear that data which is not conceived as sensitive or potentially harmful could become so through combinations with other data.[8] Even anonymous or de-identified data can be used to generate outcomes ranging from privacy infringement to discrimination. Furthermore, the effectiveness of such approaches is doubted by scholars. Big Data analytics allow for the extraction of unpredictable inferences from data, putting at risk and undermining de-identification strategies. This is due to the risk of reconstructing real identities when combining anonymized data identities in the profiling process (see Ohm 2010, 1701). New technologies, such as RFID-chips, make it difficult to follow which information is collected for which purposes and to keep track of the factual use of such data. It is tempting for the human data controllers to push the envelope when it comes to utilizing data in new ways, attempting to generate higher levels of knowledge. For the average person, becoming aware of unspecified data usage is a challenge. There are a host of practical complications for implementing sound data protection through the enacting of accountability,

---

6 Data protection accountability has recently been debated among privacy scholars (see Guagnin et al. 2012) and is taken into account in the discussions of the current draft of the GDPR.

7 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*

8 For a problematisation of inferring private data from large databases and efforts to avoid disclosure of private data see Chang and Moskowitz 2001; Sackmann, Strüker and Accorsi 2006; Verykios et al. 2004.

transparency, and traceability measures.[9] Currently, there is a general lack of transparency in profiling techniques (see Hildebrandt 2009a and 2009b) and data processors' accountability is challenged by the employment of vague practices and the black boxed technologies inherent to data mining and profiling. Within this environment, neither the Security Safeguards Principle nor the Openness Principle is being taken into consideration. Individuals become increasingly more transparent in this setting, just as public bodies and even private companies become more intrusive, operating along the fringe of legality.

2.2.2 The Right to Non-Discrimination

The right to non-discrimination "emanates from the general postulate of the equal dignity of human beings". (Özden 2011, 7) This right constitutes a general principle in EU Law and 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 contains specific provisions developed in anti-discrimination legislation related to certain protected grounds (e.g. age, race, gender, religion, sexual orientation, etc.) and specific areas of application (i.e. labour market, vocational training, education, social security, health care, access to goods and services, criminal law). Within the canon of EU law, there is a conceptual distinction between direct and indirect discrimination, both of which are prohibited. Direct discrimination occurs when a person is treated less favourably than another, and this difference is based directly on the protected grounds previously mentioned. 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. Frequently, 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" (Romei and Ruggieri 2013, 121). The best-known example of this relates to "redlining", a practice that is explicitly forbidden by US law. Redlining is the practice of denying products and services

---

[9] Some scholars criticise 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 Guagnin et al. 2012.

in particular neighbourhoods, marked with a red line on a map. Due to racial, ethnic or social segregation an apparently neutral attribute such as ZIP Code may turn into a qualifier for indirect discrimination. In most circumstances, profiling, as it is applied to marketing (web marketing, loan market, price determination, etc.), can easily hide practices of indirect discrimination. Consequently, research on data mining techniques that prevent discrimination is a fruitful field of study (see Pedreschi, Ruggieri and Turini 2013). Another example of infringement on the right to non-discrimination is that of Eurosur, a European approach to smart border surveillance. This system relies on technology to automatically check passengers crossing a border. Its use of technology consists of databases and sophisticated tools, such as body and iris scanners. Eurosur's final aim is to speed up the border crossing process for bona fide travellers, fight 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 distinguish between welcome and unwelcome travellers. Aside from the privacy risks, data protection issues due to the use of biometrics, and the lack of respect for the principle of purpose-binding and use limitation. The ambiguousness of the logic behind the data mining procedure is in itself hard to reconcile with the obligation not to discriminate on prohibited grounds. However, above all, the smart borders approach raises huge concerns about the respect for human dignity.

The multitude of risks that profiling imposes on fundamental rights and values, as well as the complex effects related to the implementation of this technology, reveal just how challenging it is to impose adequate measures for the protection of European rights and values. The next section provides a brief overview of the state of this process in Europe.

3. Regulating profiling - an outlook

The word profiling does not appear in current EU data protection legislation. However article 15 of Directive 95/46/EC (henceforth, Data Protection Directive, DPD) addresses 'automated individual decisions' and is therefore 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 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 light of Article 15 of the DPD, it is relevant whether or not processing is meant to evaluate a certain aspect of a person's behaviour, character or identity on which a decision can be based. A decision based on a profile can comply with the law, but a real person must be involved in the process. In short, Article 15 is not a direct prohibition on a particular type of decision-making; but rather, it directs each EU Member State to confer on persons a right preventing them from being regularly subjected to purely automated decisions (see Bygrave 2002, 3). The DPD has been unable to provide sufficient protection in our fast-developing information society. In January 2012, a draft General Data Protection Regulation (GDPR) and a Data Protection Directive, developed for the context of law enforcement, were released by the European Commission in an attempt to respond to the technological developments of recent decades.

Article no. 20 of the GDPR concerns a data subject's right not to be subjected to a measure based on profiling. This article is representative of an evolution with respect to Article 15(1). It implements modifications and safeguards and takes into consideration the Council of Europe's recommendation on profiling (Recommendation CM/Rec(2010)13). Compared with Article 15, Article 20 better defines the right of a person not to be subjected to a measure that is based solely on automated processing[10] and, in particular, elucidates the principle that profiling cannot be based only on sensitive forms of data (e.g. race or ethnic origin, religion, political opinion or sexual orientation), which would carry too strong a risk for discrimination on the basis of a prohibited grounds[11]. Article 20, in comparison with Article 15, places more stringent rules on the application of profiling allowing the practice only when: a) it is required for contracts, and the data subject has the right to request a human intervention; b) it is permitted by law; or 3) under certain conditions, the data subject gives a free, explicit and informed consent[12]. A unique aspect of Article 20 concerns the

---

[10] 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."

[11] 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".

[12] 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

provision contained in the fourth paragraph, obliging data controllers to provide 'information as to the existence of processing" for an automated decision and information pertaining to "the envisaged effects of such processing on the data subject".[13] As highlighted by the advice paper released by Article 29 WP in May 2013[14], there is no definition of profiling included in the GDPR. The existence of blank spots such as this is a testament to the fact that there is still a lot of work to be done in understanding the scope of profiling and facilitating the formation of adequate regulation in this rapidly expanding field.

References

Article 29 Working Party. 2010. *Opinion on the Principle of Accountability in 2010.* Accessed 8 May, 2015. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

Bosco, Francesca, Niklas Creemers, Valeria Ferraris, Daniel Guagnin and Bert-Jaap Koops. 2015. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities." *In Reforming European Data Protection Law*, edited by Serge Gutwirth, Ronald Leenes, and Paul de Hert. Dordrecht: Springer.

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

Council of Europe. 1981. "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data", *Convention 108*. Accessed 8 May, 2015. http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Chang, Li Wu and Ira S. Moskowitz. 2001. "An Integrated Framework for Database Privacy Protection." In *Data and Application Security*, edited by Bhavani Thuraisingham et al., 161-172. New York: Springer.

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

---

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."

13 See for weaknesses and strengths of this provision Koops 2013 and Hildebrandt 2012.

14 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

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

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281, 23/11/1995,* p. 0031 – 0050. Accessed 08 May, 2015. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Finn, Rachel L., David Wright and Michael Friedewald. 2013. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet, 3-32. Dordrecht: Springer, 2013.

Gellert, Raphael and Serge Gutwirth. 2012. "Beyond accountability, the return to privacy?" In *Managing Privacy through Accountability*, edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kröger, Daniel Neyland and Hector Postigo, 261-284. Houndmills: Palgrave Macmillan.

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

Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kröner, Daniel Neyland and Hector Postigo (eds.), 2012. *Managing Privacy Through Accountability.* Houndmills: Palgrave.

Gutwirth, Serge and Mireille Hildebrandt. 2010. "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.

Han, Jiawei and Micheline Kamber. 2006. *Data Mining: Concepts and Techniques.* Oxford: Elsevier Ltd.

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

Hildebrandt, Mireille. 2008. "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.

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

Hildebrandt, Mireille. 2009b. "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.

Hildebrandt, Mireille. 2009c. "Who is Profiling Who? Invisible Visibility." In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile Terwagne and Sjaak Nouwt, 239-252. Dordrecht: Springer.

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

Krasmann, Susanne. 2010. "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.

Marx, Gary and Nancy Reichman. 1984. "Routinizing the Discovery of Secrets: Computers as Informants," *American Behavioral Scientis*, 27, 4: 423-453.

OECD 2014. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Accessed 14 March, 2014. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

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

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

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

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

Rodotà, Stefano. 2009. "Data Protection as a Fundamental Right." In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile Terwagne and Sjaak Nouwt, 77-82. Dordrecht: Springer.

Romei, Andrea and Salvatore Ruggieri. 2013. "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, Toon Calders, Bart Schermer and Tal Zarsky, 109-135. Berlin: Springer.

Roosendaal, Arnold. 2013. *Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts*. Oisterwijk: Wolf Legal Publishers.

Rouvroy, Antoinette and Poullet, Yves. 2009. "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, Yves Poullet, Paul de Hert, Cecile Terwagne and Sjaak Nouwt, 45-67. Dordrecht: Springer.

Sackmann, Stefan, Jens Strüker and Rafael Accorsi, 2006. "Personalization in Privacy-aware Highly Dynamic Systems." *Communications of the ACM - Privacy and security in highly dynamic systems.* 49, 9: 32-38.

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

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

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

Verykios, Vassilios S. et al. 2004. "State-of-the-art in Privacy Preserving Data Mining." *SIGMOD Rec.* 33, 1: 50–57.

Zakaria, Fareed. 1997. "The rise of illiberal democracy." *Foreign Affairs* 76, 6: 22-43.