

Working Paper 3

The impact of profiling on fundamental rights

V. Ferraris (AMAPOLA); F. Bosco, E. D'Angelo (UNICRI)
Internal reviewer: B.J. Koops (Tilburg University)

Table of Contents

Introduction	2
1. Profiles and digital personae: new frontiers for fundamental values and rights	2
2. Profiling and application areas	5
2.1 Anti-money laundering (AML) and counter-terrorism	6
2.2 Prevention of financial and credit-card fraud	8
2.3 Employment and Education (E-learning)	10
2.4 E-health	12
3. Profiling and fundamental values and rights	13
3.1 Fundamental values	14
3.2 Fundamental rights	17
4. The legal protection provided by the present legal framework: legal instruments and existing mechanisms	23
4.1 Right to privacy and Right to Data Protection	23
4.2 Right to non-discrimination	33
Conclusions	34
References	36

With financial support from the
“Fundamental Rights and Citizenship Programme” of the European Union



Introduction

There is no doubt that the respect of human rights is essential to guarantee democracy and rule of law. But as it often happens, there is disagreement on how to guarantee access to such rights and on what these rights and democracy itself mean. It is beyond the scope of this paper to get into this discussion, even if it is possible to agree with the statement that individuals are clearly subject of rights. But what happens when the individual is not flesh and bones but s/he has an online life? How does profiling affect, if it does, the fundamental rights of a person and the fundamental values of a society? Does the online context influence the guarantee of a person's rights?

The impact of profiling on fundamental values and citizens' fundamental rights

This paper, starting from an appreciation of the definition of profiling, will focus on the impact of profiling on citizens' fundamental rights.

In chapter 1 we will first elaborate on the concepts of profiles and digital personae and how they represent new frontiers for fundamental rights and values. In chapter 2 it will be shown how different application areas of profiling (2) have different issues to be analysed, as anti-money laundering and counter-terrorism (2.1), prevention of financial and credit-card fraud (2.2), employment and education (2.3) and what is defined as "e-health" (2.4). Chapter 3 will discuss fundamental values (3.1) and rights (3.2) which might be affected by profiling practices, namely democracy and the rule of law (3.1.1), autonomy and self-determination (3.1.2), the right to privacy and the right to data protection (3.2.1) and the right to non-discrimination (3.2.2). The closing chapter 4 will present the legal protection provided by the present legal framework, which are the legal instruments and the existing mechanisms, focusing on the right to privacy and data protection (4.1) and on the right to non-discrimination (4.2).

1. Profiles and digital personae: new frontiers for fundamental values and rights¹

Digital representations of a person makes the debate on rights more sophisticated

Technological developments have created new representations (Goody, 1997, cited by Roosendaal, 2013), i.e. digital representation (Roosendaal, 2013) of a person that makes any

¹ The European Union defines its funding values as human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.

debate about the guarantees of individuals' fundamental rights and value much more sophisticated.

Before discussing how fundamental rights and values are challenged by profiling, it is worth recalling the adopted definition of profiling and underlining the differences between the concepts of profiling and digital *personae*. This clarification is needed because it helps underscore the sensitivity of the issue of

Two forms of digital representation of a person: Profiling and Digital Personae

fundamental values and fundamental rights and the serious challenge posed by profiling as to fundamental rights and values.

As stated in the Working Paper "Defining Profiling"², profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from data in the form of constructing profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (human or non-human, individual or group) subject. Constructing profiles is the process of discovering unexpected 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 subject or to identify a subject as a member of a specific group or category and then taking some form of decision based on this identification and representation.

So Profiles are a set of correlated data that represent a subject. They can be distinguished in group (distributive and non-distributive) and individual profiles; direct and indirect profiles.

Group profiles identify and represent a group. They are **distributive group profiles** if the people identified share all the same attributes. A **non-distributive group profile** identifies a certain number of people who do not share all the attributes of the group's profile.

Direct profiles imply that data is collected from one single person or a group and the information derived from the data elaboration will be applied just to the same person or group. **Indirect profiling** involves the collection of data from a large population. Individuals are then identified using the attributes emerging from this data collection.

Another form of digital representation of a person is the **digital personae** (concept introduced firstly by Clarke³, 1994). Largely used by Solove (2004), this

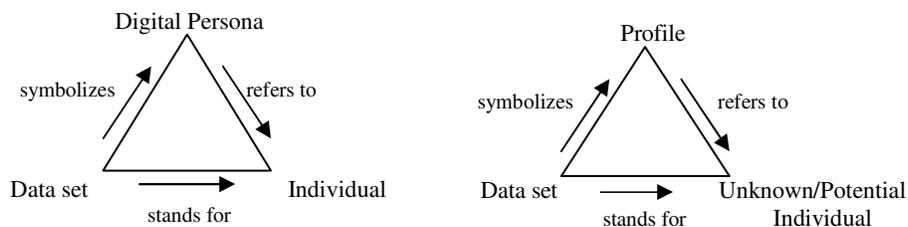
² Available on the PROFILING project webpage: <http://profiling-project.eu/defining-profiling-first-paper-of-profiling-project-online/>

³ Clarke defined *the digital persona* as "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual" (see, <http://www.rogerclarke.com/DV/DigPersona.html>). He also distinguishes between projected digital

concept has been recently investigated by Roosendaal (2010; 2013), who explores the differences between profiles and digital *personae* in an in-depth manner.

In Roosendaal's (2013, p.41) words "a digital persona is a digital representation of a real-world individual, which can be connected to this real-world individual and includes a sufficient amount of (relevant) data to serve, within the context and for the purpose of its use, as a proxy for the individual". Using the Peirce's triads⁴ of object, sign and interpretation, Roosendaal identifies the differences between digital personae and profiles: Digital Persona is the interpretation that refers to the object Individual and Profile is the interpretation that refers to the object unknown/potential individual.

Digital Persona refers to Individual whereas Profiling refers to potential individual



Source: Roosendaal (2013, p.34)

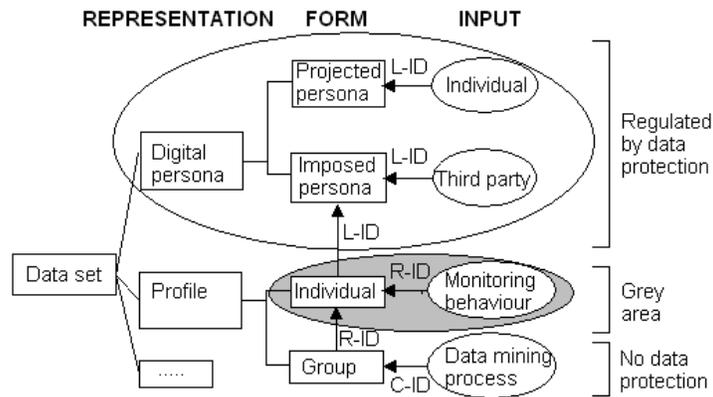
This distinction is essential because as it will be seen in the following pages, it has serious consequences in the application or not of the Data Protection legal instruments.

To make the differences clearer, Roosendaal (2013) takes the four types of identifiers singled out by Leenes (2008)⁵ so as to build a flow chart that helps delineate the characteristics of profiles and digital personae.

personae and imposed digital personae according to the degree of control the individual has on the formation of his/her digital representation.

⁴ The semiotic theory of the 'triad of meanings' was developed by Charles Sanders Peirce.

⁵ Leenes distinguishes four types of identifiers to underline that there are several on-line ways that make users identifiable. L-identifiers and R-identifiers (where R stands for recognition) are those referring to individuals. L-identifiers (where L stands for look-up) are the one that provide "the connection between the identifier and a named individual", R- identifiers allow "an individual to be recognized without being able to associate the identifier with a named individual". C- identifiers are a form of group identification because it "allows the classification of individuals as belonging to one or more categories". S-identifiers are identifiers that allow "to track a user during a particular interaction" in a single "session".



Source: Roosendaal (2013, p. 32)

As can be seen from the figure, group profile is in the realm of C-identifiers, where there is no identification of an individual, but classification of individuals in a category. Individual profile, on the other hand, is a case of R-identifiers. Digital personae instead contain L-identifiers that always allow the identification of a specific person.

The complexity of the issue of fundamental rights being applied to profiling is based on this distinction. If in order to recognize rights to the digital personae (the digital proxy of a flesh and bones person), there is a need to conceptualize

Profiles and Digital Personae: how they relate with fundamental rights personal data and privacy rights in an extensive way, when it comes to profiles the picture is rather more articulated. Profiles do not identify specific individuals when they are created, since they are “probabilistic knowledge”, as defined by Hildebrandt (2009c). However, they may turn into digital personae: individual profiles are so close to digital personae that even among scholars the distinction is not always clear.

2. Profiling and application areas

The distinction between profiles and digital personae is a key component in the analysis of the impact of profiling on fundamental rights and values. Before going through the different human rights and values which can be affected by profiling practices, we will focus our attention first on some of the main fields of profiling where human rights and values are applied, and the related possible benefits and risks for individuals.

Within each field of application, we will try to outline:

- How profiling is applied in that particular field, by providing some examples;
- On which fundamental rights the profiling has a possible impact;
- A brief indication on what are the main issues with profiling in the specific field requiring attention from the legislation at European level.

Both public and the private sectors will be explored. The modern technique of profiling, “widely used in the private sector, is now also increasingly being portrayed as a useful, appropriate technique for various security-related purposes” (Fuster, Gutwirth, Ellyne, 2010, p.1), due to its potential benefits on the public sector. Moreover, the permeability between the public and the private sector in the transfer of data⁶ is a challenging and controversial issue, as the recent case on US surveillance on phone and internet communications and the features of the PRISM programme have shown⁷.

2.1 Anti-money laundering (AML) and counter-terrorism

One of the areas where profiling is applied is the financial sector, particularly for what concerns the fight against money-laundering (and the fight against terrorism), the prevention of credit card frauds as well as the broader issue of taxation.

AML regulations have increased in the recent years and more and more governments require relevant bodies to cooperate in preventing and detecting money-laundering. When an institution suspects that a customer is engaging in financial transfers from criminal proceeds, it is required to submit a “Suspicious Activity Report” to the relevant national anti-money laundering agency, which will take the appropriate follow-up measures. The European Union has provided support to this type of practice through the “Third Money Laundering Directive” (2005/60/EC). This Directive “brought about the application of a risk-based approach to customer due diligence for the ongoing monitoring transaction activities, and obliged member states to require that the designed bodies establish policies and procedures of risk assessment to forestall and prevent money laundering or terrorist financing” (Fuster, Gutwirth, Ellyne, 2010, p.3).

However, one of the main problems of the use of automated profiling in AML is that profiles usually rely on tried and tested money laundering typologies and

⁶ See Guagnin D., Hempel L., Jung J. (2013), available at <http://profiling-project.eu/evolution-of-technologies-download-the-new-paper-of-profiling-project/>

⁷ For more information see for instance: <http://www.theguardian.com/world/edward-snowden>

they do not keep up with the complex and advanced mechanisms of money laundering (Canhoto, 2005).

The use of AML profiling is also related to the fight against terrorism, since the analysis of the financial systems can help detect terrorist groups and understand how they fund their activities. One example of data mining techniques used in the financial sector with the aim of detecting potential terrorists is the Investigative Data Warehouse (IDW) of the FBI. The IDW represents a platform that provides access to numerous databases through a single interface. The platform incorporates search and analysis tools. According to the Electronic Frontier Foundation's 2009 report on the IDW, among available data sources in the IDW, there are files relating to terrorist financing, including the Financial Crimes Enforcement Network (FinCen) databases; databases containing biographical data supplied by foreign financial institutions on individuals suspected of having connections with terrorist financing; the State Department's list of lost and stolen passports as well as documents from passport fraud investigations.

Initiatives to counter-terrorism through profiling techniques exist also at European level. In 2002, the Article 36 Committee of the EU "submitted a draft Council Decision which would establish terrorist profiles to be used in European counter-terrorism efforts" (Moeckli, Thurman, 2008, pp.28-29). According to this draft decision, Member States would exchange information amongst each other and with Europol and also cooperate to develop profiles. The Committee defined the creation of terrorist profiles as involving "putting together a set of physical, psychological or behavioural variables, which have been identified, as typical of persons involved in terrorist activities and which may have some predictive value in that respect" (Article 36 Committee, 2002, p.5).

Besides the functional implication of using profiling practices to detect potential terrorists, there are several concerns for the respect of human rights and the principle of non-discrimination. For example, it still remains unclear as to whether it is possible to come up with effective profiles of terrorists. Furthermore, "Much attention has been devoted to Al Qaeda and Islamic terrorism. This focus may perhaps be appropriate due to the relative level of threat, but it could also bring with it the enhanced risk of discrimination on the basis of religion, ethnicity or national origin [...] Moreover, behavioural profiling - which would include reliance on travel patterns - may pose less risk of discrimination on the basis of personal attributes (though there might still be a risk of indirect discrimination), but can be just as

**Concerns for privacy,
data protection and
non-discrimination**

problematic in terms of infringement of the right to privacy” (Moeckli, Thurman, 2008, pp. 34-35).

Thus both in the field of anti-money laundering and, even more, in counter-terrorism data mining and profiling can raise concerns with regard to the right to privacy, the data protection principles and the right to non-discrimination⁸. “Even where States provide explicit legal authorization for data mining to combat terrorism, broad scale programmes are unlikely to conform to the principle of proportionality due to the resulting interference with the right to respect for private life of a large number of innocent individuals” (Moeckli, Thurman, 2008, p.2).

2.2 Prevention of financial and credit-card fraud

As described above, data processing activities may play an important role in pattern recognition and prediction practices. In the field of prediction techniques, the prevention of credit card fraud is also an important example of application. This can be gauged from the fact that, “for the high data traffic of 400,000 transactions per day, a reduction of 2.5% of fraud triggers a saving of one million dollars per year” (Brause, Langsdorf, Hepp, 1999, p.2).

The main goal should be avoiding a fraud through a credit card transaction before it is identified as “illegal”. Since it is impossible to check all transactions, the experience in this field should be used to develop systems of analysis. The main disadvantage is brought about by continuous and rapid changes in the

Early detection is useful for credit grantors

experts’ knowledge uncovering new forms of attacks and frauds. “In order to keep track with this no predefined fraud models [...] but automatic learning algorithms are needed” (Brause, Langsdorf, Hepp,

1999, p.2).

Data mining gives financial institutions information about loan information and credit reporting. By building a model from historical customer’s data, the bank and financial institutions can determine good and bad loans (ICCS, 2009). Early detection of risks associated with financing, such as credit or debt risks and business risks, can help credit grantors to reduce losses and establish appropriate policies for different products. Due to the size of the modern financial databases, “large-scale data mining techniques that can process and analyze massive amounts of electronic data in a timely manner become a key component of many financial risk detection strategies and continue to be a subject of active research” (Yi Peng, Gang Kou, Yong Shi, 2009, p.535).

⁸ See also paragraph 3.2.1 and 3.2.2 below.

An example of a financial database assisting in the prevention of financial fraud is the German system SCHUFA. With the consent of their clients, the providers of bank and financial services transfer the data concerning the bank accounts and the financial behaviours to the SCHUFA. The behaviour of so-called reference-groups is then analysed with massive data volumes. The profiling gives a scoring value, which should express the risk based on personal behaviours. These data, together with other information, are used “to determine the risk of defaulting on credit and conditions under which someone can obtain credit” (Canhoto, 2005, p.59). However, due to the trade secrecy there is not full transparency in the calculation of these scores and the customers have not full access to the information. In addition, the SCHUFA scoring value is claimed to violate the Federal German Data Protection Act (Möller, Florax, 2002, pp. 806-811).

Furthermore, indirect discrimination, in particular racial discrimination, can happen in the practice of redlining⁹: “[...] people living in a certain neighbourhood are frequently denied credit [by banks or credit institutions]; while not explicitly mentioning race, this fact can be an indicator of discrimination, if from demographic data we can learn that most of people living in that neighbourhood belong to the same ethnic minority” (Custers, Calders, Schermer, Zarsky, 2013, p.92).



Indirect
discrimination
in redlining
practices

Another aim of the use of profiling techniques in the financial domain is the fight against tax-evasion. The information about citizens' financial situations and their spending habits can be analyzed in order to find discrepancies and non-standards transactions. A controversial tool used for this purposes, is the “Redditometro”, developed by the Italian government and the Agenzia delle Entrate to fight the phenomenon of tax evasion in the country. The idea behind the creation of this tool is to collect, pre-emptively, all data concerning the taxpayers and place it in a unique database. Then, specific data-mining software tries to detect “non-standard” transactions according to the previously identified parameters¹⁰. This generalized profiling of all citizens and the way they use their own money, however, raised several concerns about the lack of transparency on the definition of the parameters' and the possible violation of citizens' rights to privacy.

⁹ According to the Oxford Dictionary, the action of red-line is defined as: the action or practice of a bank, etc., in refusing to grant a loan or insurance to an area considered to be of significant financial risk, or offering these services at prohibitively high rates.

¹⁰ For further information see (Italian source): <http://thefielder.net/11/03/2013/redditometro-il-ricorso-va-a-segno/#.Ufkbz6xo-ho>

2.3 Employment and Education (E-learning)

Within the employment and the education sector, profiling has become increasingly important for different aspects and peculiarities.

In employment, at private and public level, the processing of personal data is often introduced for security reasons with the consequent implications for citizens' rights.

For instance, the FIDIS¹¹ research reports that in German supermarkets, profiling is used "to determine unusual cash flow often caused by embezzlement by cashiers" (Meints, 2005, p.57). In fact, there are different techniques for illicitly taking money out of cash. One method can be by using false certificates for bottle deposits with usually small amounts of money. In the profiles, cashiers using this method can be determined by a higher rate of refund transactions than the average rate. Of course, in order to detect the fraudulent employee further investigation will be necessary, but these can be carried out on an already targeted group of people.

Profiling causes a shift of balance in the employment relationship

The employment relationship can be defined as one borne out of a contract where the employer is allowed to exercise authority over the employee only with relevance to the terms of the contract. Of course the right of privacy and the principle of data protection need to be respected. Profiling caused a shift of balance in the employment relationship in favor of the employer: in this context, the fundamental right of data protection is aimed at re-balancing the power relation between the contracting parties.

Data protection regulation in the workplace thus provides general principles regarding the processing of personal data and also guarantees the workers granting right of access to these data (right to know about their data being processed, right to be informed about it, right to object etc.).

To give an example on how to avoid infringement of fundamental rights in this particular field, we can refer to the case of security control based on the surveillance of internet access and e-mail communication made by the employers both in the public and private sector. While for HR management the distributive group profiling is used, in this case the profiling is personalized: intrusion detection/response systems are implemented. Besides the reporting of

¹¹ The FIDIS - "Future of Identity in the Information Society" - project received research funding from the Community's Sixth Research Programme

incidents, this can be a preventive tool in view of possible information thefts or other unlawful content-related activities from and inside the organization.

In this context, the best way to prevent any infringement of workers' rights is to establish a clear regime applicable to all employees on the restrictions concerning the use of private e-mails, for instance. Moreover, a set of guidelines can define who and under which circumstances the traffic data and even the contents thereof can be accessed and analyzed for security reasons.

On the other hand, in certain cases profiling can also represent an opportunity. In the case of "traditional" education, for instance, profiling is a crucial element, and a lot of theories and practices have been developed in order to profile the students, to identify their characteristics and their ability to fit in a particular job (Nabeth, 2005). In the modern world of e-learning, profiling is considered in a different way. For instance, student modeling and profiling – besides being central in the adaptive systems – is also important in the implementation of Learning Management Systems (LMS)¹². The student profile is an important component of the LMS, since it is used to centralize all the information associated with a particular student, and also all the information concerning his/her scholar background and the progression of his/her career.

User profiling also plays an important role in the field of user adaptive (or personalized) systems, such as intelligence tutoring systems. "[...] [A]daptive systems promise to revolutionize education by providing each student with a personal tutor, addressing therefore the problems of the overcrowded classroom, and of the students that do not get enough attention from the teaching staff" (Nabeth, 2005, p.63).

Therefore, once again we have underlined the possible risks and benefits of profiling in important fields of application, such as the employment and education sectors. In one case (employment), strict rules and a set of guidelines are needed in order to prevent, as much as possible, rights' infringement and to guarantee the correct balance in the contract relationships. In the other case (education), the important role of profiling techniques should be taken into account in order to take advantage of its useful implications.

¹² According to Ellis (2009), a LMS is a software application for the administration, documentation, tracking, reporting and delivery of e-learning education courses or training programmes.

2.4 E-health

According to Della Mea (2001), the term e-health refers to those health practices, which are supported by electronic processes and communication. The term can cover a range of services or systems at the edge of medicine/healthcare and information technology.

“e-Health is an important tool in establishing safe, efficient, and sustainable health care delivery around the world [...] Many WHO regions, in particular the European, Americas and Eastern Mediterranean, have already invested heavily in e-Health solutions to meet the challenges of ageing populations, and are beginning to embrace the idea that in order to meet health care needs in the context of demographic change, a paradigm shift towards more patient-centred care delivered outside the traditional hospital or general practitioner office environment will have to occur” (WHO, 2012, p.12).

The primary aim of e-health systems’ technology is to improve and simplify communication, by enabling information transfer from citizens to healthcare providers who can treat them. This entails, as a side effect, the generation of large databases of diagnostics, medical imagery, symptom descriptions etc., primarily because data is often required to be stored so as to be later examined. These databases create enormous opportunities to explore data and obtain further knowledge from it. For instance, the Centerstone Research Institute has developed tools for analyzing the treatment of all their patients and discerning the methods that give the best result in order to apply the resultant data for future patients (CRI, 2010).

**e-Health databases
create opportunities to
explore data and obtain
further knowledge**

Focusing on the application of profiling techniques to the healthcare sector, data mining techniques are particularly useful in the field of healthcare management – such as in the evaluation of treatment effectiveness, management of healthcare, customer relationship management, the detection of fraud and abuse – and in predictive medicines, which mainly deals with learning models to predict patients’ health or the likelihood of a treatment being successful with a particular patient based on certain group’s characteristics. The final and most important objective is of course prevention, with crucial consequence for citizens’ health and safety. Besides the difficulties related to the financial funds for implementing e-health systems and those connected to the digital divide - in terms of equal access to technologies and consequently to certain health services and medical products - “a change in the legal context for healthcare provision is also necessary, because such systems will have to be able to accommodate secure transfer of information

between health facilities and patients' homes and a range of stakeholders in the public, private, and international sectors" (WHO, p.12).

At international level there are both binding and non-binding regulations concerning privacy and protection of personal data in health related information¹³. However, much more has to be done to ensure the full protection of patients' rights when both private and public bodies collect, use and disseminate their sensitive healthcare-related personal data.

3. Profiling and fundamental values and rights

While we need to acknowledge the potential benefits of profiling in certain sectors, as just highlighted in the case of E-health, it is undoubtable that profiling may pose serious risks to individuals and the society in general as a consequence of its possible impact on fundamental rights¹⁴. Such risks concern discrimination, inequality, stereotyping, stigmatization and inaccuracy of the decision-making process. These risks impact on the rights to privacy, data protection, and non-discrimination.

However there is even more than the risk of the infringements of some specific rights. The growing relevance of profiling technologies, among the general evolution of digital technologies, makes society face the risk of dependence (Hildebrandt, 2009c) and unable to control the process and the effects of those technologies. This turns into a serious threat for the quality of liberal democracy and equality among human beings.

All these risks are interrelated and therefore any taxonomy of these risks hardly avoids some overlapping and repetition. The choice made here is to distinguish a first level of fundamental values, connected with society as a whole, and individuals as members of it; and a second level of specific fundamental rights.

Risks for values and rights are interrelated

¹³ Among the existing efforts to deal with privacy protection of electronic health information: the Council of Europe's 1981 Convention for the protection of individual with regard to the automatic protection of personal data; the OECD Guidelines governing privacy and transborder data flows; the Directive 95/46/EC, among others.

¹⁴ Among the fundamental rights, as stated in the Charter of Fundamental Rights of the European Union, those concerned by the issue of profiling are mainly the protection of personal data (art. 8) and the right to non-discrimination (art. 21). On the other side, the European Union itself recognizes, among its funding values, human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.

3.1 Fundamental values

3.1.1 Democracy and the rule of law

The clash between liberal democracy (Zakaria, 1997) 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 the taking of better decisions. But the dark side of profiling is that it makes “invisible all what cannot be translated into machine-readable data” (Gutwirth, Hildebrandt, 2010, p.33). This means that decision-making process could be biased in the data collection phase and because of the complexity of the applied algorithms, human being cannot properly intervene in repairing this possible original 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” (Gutwirth, Hildebrandt, 2010, p.33). 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 (e.g. profiling technologies applied to health sector give a clear-cut idea of the level of risks).

Complex algorithms make difficult recognizing and repairing bias

Not only human intervention is reduced during the decision-making process, but also citizens do not 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 (Solove, 2004) and the knowledge asymmetries (Gutwirth, Hildebrandt, 2010) between the ordinary citizens, on one side, and government (and corporate business enterprises)¹⁵, on the other side. Knowledge asymmetry is everyday experience but it reaches probably its maximum in profiling technologies. In most of the cases, citizens are not aware that a profile is going to be built with the data they provide in a specific circumstance. Taking the consent of the data subject is far from being fully realized. Here the problem is not the limited effectiveness of the consent to the use of data but the fact that, without giving it, a person cannot obtain the service s/he is asking for (consent is a locked-in choice, Roosendaal 2013, p.72). In profiling, it is even hard to imagine how and for which actions to ask the data

Lack of human intervention, unbalanced distribution of power, knowledge asymmetries: the risks for democracy

¹⁵ The power and the exclusive knowledge of the corporate business enterprises have an impact on democracy and rule of law because of the growing relevance of big players as Google or Yahoo and the easy access that government authorities have to their data (see Guagnin D., Hempel L., Jung J., 2013).

subject's consent. Profiles may be constructed from data that is not of the data subject: consequently it is meaningless to ask consent but there is no easy protection on the horizon. Is there any room to ask citizens to give their consent – for example in order to obtain better services - to the application of profiles based on someone else's data? Then, profiles may be applied because certain subject's data match the profile, but in reality this correspondence can be true or not, in particular in the case of non-distributive profiling (see Defining profiling, Working paper 1, Profiling project¹⁶).

Moreover some sophisticated profiling technologies like Behavioural Biometric Profiling (BBP) “do not require identification at all” (Hildebrandt, 2009c, p.243).

Then profiling activities are not yet a reality when the data are collected. And a general consent on a generic future use is certainly meaningless. Finally, it is worth mentioning that “as far as this knowledge is protected as part of a trade secret or intellectual property, the citizens to which this knowledge may be applied have no access whatsoever” (Hildebrandt M. 2008b, p. 63)

In addition, in the context of administrative rulemaking and criminal investigation the use of profiling techniques may raise concerns on the respect of the Due

The threats of the Due process right

Process clause¹⁷. Due Process of law is largely recognized in international law as a fundamental principle protecting the citizen from arbitrary and unfair treatment by the State. In 2000, principles close to the Due Process clause¹⁸ had been foreseen in the Charter of the Fundamental Rights of the European Union. This Charter has acquired legal value since the inclusion in the Treaty of Lisbon¹⁹, entry into force the 1 December 2009. It is too early to say if this will have some effects at the member states level, taking into consideration that, differently from United States, few member states of the European Charts includes Due Process Clause, as a binding Constitutional rule. Profiling techniques “raise core due process questions of the right to be notified of the government's claim and to be heard in opposition” (Steinbock, 2005, p.7).

¹⁶ Available at: <http://profiling-project.eu/defining-profiling-first-paper-of-profiling-project-online/>

¹⁷ “Due Process Clause is a clause in the U.S. Constitution that embodies a system of rights based on moral principles. The due process principle states that the government must respect all of the legal rights that are owed to a person according to the law. Thus the due process clause in the constitution prohibits the state and local government from depriving people of their life, liberty, or property without certain steps being taken. In the U.S. Constitution, the concept of due process is discussed under the fourteenth and the fifth amendments to the constitution”. Source: US Legal.com available at: <http://definitions.uslegal.com/d/due-process-clause/>

¹⁸ It is worth noting that Article 41 ‘Right to good administration’ and Article 47 ‘Right to an effective remedy and to a fair trial’ of the European Charter of fundamental Rights introduce principles that strengthen the position of the citizen in front of a State abuse and are close to the Due Process Clause.

¹⁹ Article 6, par. 1 TUE “The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties”.

As the profiling procedure is not transparent, “citizens cannot see or debate the rules” (Citron, 2007, p.1254) and they will receive the notification of the consequence of the profiling process (e.g. the denial of the boarding in a plane²⁰), but “the person has no chance to challenge either the underlying facts or the ‘reasoning’ of the process that led to its effect. If he/she even has an opportunity to contest the result, he/she is forced to refute a label brought about by a completely opaque process, and is often helpless to respond to either errors in the data or faults in the algorithm. Nor is he/she entitled to compensation for harms wrongly imposed” (Steinbock, 2005, p.8).

The serious threat to the rule of law is linked to the use of these techniques as a sufficient basis for decision-making. This appears particularly harmful when there is no access to an effective remedy in a reasonable time (as in the example of the denial of the boarding in a plane) and when the results of profiling techniques are used as evidence in a process. This evidence relies only on a degree of probability, but it is difficult for a citizen accused to question it, because of the supposed impartiality of the algorithms beyond the profiling process.

Finally, wrong decisions taken as a result of profiling technologies make it difficult to concretely establish a person as being financially and legally responsible for the damages occurred (Hildebrandt, 2010, p.56).

3.1.2 Autonomy and Self-determination

The position that citizens enjoy versus the State is one of the indicators of the quality of a democracy. This is not only related to the recognition of rights, but also the opportunities the State gives for the full and free development and expression of one’s personality and his/her effective participation to the democratic life.

In this framework are placed the fundamental values of autonomy and self-determination. They cannot be defined as legal rights because “they are not something that the State can ‘provide’ the individuals with and the mere abstention by the State to intrude or interfere with ‘private’ or ‘intimate’ affairs is obviously not enough to ‘make’ individuals autonomous” (Rouvroy and Pouillet 2009, p.59). Autonomy is essential to have access and exercise fundamental rights defined by the law. However, despite the difficulty faced by the State to implement legal guarantees of the values of autonomy and self-determination, “showing respect for individual autonomy” (Rouvroy and Pouillet 2009, p. 60) and

²⁰ “Every week, approximately 1500 airline travelers reportedly are mislabeled as terrorists due to errors in the data matching program known as the ‘No Fly’ list” (Citron, 2007, p.1256). See also the sources cited there.

therefore creating the conditions for the full implementation of people's negative and positive freedom (Hildebrandt, 2008b) is essential for a truly liberal democracy.

Self-determination acquires a specific meaning in this discussion. It is the one of informational self-determination, concept recognized in a landmark population census decision of the German Federal Constitutional Court (Bundesverfassungsgericht), in 1983 and considered as an important factor influencing all European and national legislations on privacy. Informational self-determination means that an individual needs to have control over the data and information produced on him/her. This control is "a (necessary but insufficient) precondition for him/her to live an existence that may be said 'self-determined'" (Rouvroy and Poullet 2009, p.51).

Unfortunately autonomy and self-determination are at a crossroads when profiling comes in the picture. If I do not know that my data, personal or not, will be used to create profiles there is not much space for autonomy and self-determination: So, "the invisibility of the patterns that become visible to the

Without the awareness of you being profiled there can't be self-determination and autonomy

profiler and the inability to anticipate the consequences of the application of profiles derived from other people's data clearly rule out informed consent (...) and the lack of information on how I am being categorised and what the consequences are turns the idea of self-determination into ridicule" (Hildebrandt, 2009c, p.243). Moreover, if one is not

aware that he/she is receiving commercial proposals, a credit-card ranking or that he/she is subject of specific investigation because of a decision-making process based on profiles, he/she may be limited in his/her personal development and in his/her active participation in the democratic life. As long as "we cannot access the knowledge which may be built from the data we leak, the exchange of data for whatever advantage is not fair" (Hildebrandt, 2009a, p.450). Somehow, it is because citizens enjoy their freedom in the market economy and the new opportunities given by globalization that profiling technologies have new space to grow, while new risks emerged for the fundamental rights of human beings.

3.2 Fundamental rights

The fundamental values presented earlier are strictly interrelated with the right to privacy and data protection and to the protection from discrimination. As clearly underlined by Rodotà (2009, p.78), "the strong protection of personal data

continues to be a 'necessary utopia' (S. Simitis) if one wishes to safeguard the democratic nature of our political systems". Data protection is necessary in a democratic society, as Rouvroy and Pouillet pointed out (2009, p.57), to sustain a vivid democracy. It is equally important the right to non-discrimination. As matter of fact, only a society that bans discrimination and gives great importance to the fight against it can be considered as a full democracy. It is not by chance that the European Court of Justice, in two recent profiling-related cases²¹ has invoked both the legislation on Data Protection and on anti-discrimination to protect citizens' rights. As shown by Gellert et al. (2013, p.82), these two fundamental rights can offer complementary protection in case "one right is not sufficient, the individual can still seek for a protection form the perspective of the other right".

3.2.1 The Right to Privacy and the Right to Data Protection

Privacy has been a difficult notion to define (see Solove, 2007, pp. 754–764). There is a general agreement on its multiple dimensions and on the fact that it is an evolving concept. It evolves over time as technologies progress and "its content varies from the circumstances, the people concerned and the values of the society or the community" (Trudel, 2009 p.322). Several taxonomies of privacy problems and privacy types have been developed and there is no largely accepted definition of privacy. However, as it has been recently underlined "the multidimensionality of the concept of privacy may be necessary to provide a platform from which the effects of new technologies can be evaluated. This potential necessity is supported by the fact that different technologies impact upon different types of privacy, and further technological changes may introduce or foreground previously unconsidered privacy dimensions" (Finn, Wright, Friedewald, 2013, p.26).



New technologies
impact upon
privacy and data
protection

Data protection is also generally recognized as a fundamental, autonomous right. On the one hand, the concept of data protection is broader than the right to privacy, because it also serves to protect other fundamental rights (i.e. the freedom of expression, the freedom of religion and conscience, the principle of non-discrimination, etc.). On the other hand, data protection is more specific than privacy since it applies only when 'personal data' is processed and it does not always apply to other dimensions of privacy, such as protection of the home or bodily integrity.

²¹ Refer to: 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

It is out of the purpose of this paper to examine in detail the different notions and taxonomies²² of the right to privacy and its relation with the right to Data Protection but it is worth underlining how right to privacy and data protection are interrelated with profiling. Many new technologies represent a big challenge for the right to privacy and data protection: this is the case of body scanners, radio-frequency identification (RFID), biometrics, smart closed-circuit television (CCTV) etc.

OECD principles and the risks for privacy and data protection

All privacy/data protection concerns emerging from the use of these technologies can be raised also in the case of Profiling, which is nothing but a process that relies on several of such technologies.

In order to build an exhaustive framework of the threats towards the right to privacy and the right to data protection, the OECD Privacy Principles²³ (OECD, 2013) are taken as term of reference as the most comprehensive and commonly used privacy framework.

These principles are:

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle, except: a) with the consent of the data subject; or b) by the authority of law.
5. Security Safeguards Principle: Personal data should be protected by

²² There is a large amount of literature on privacy taxonomies. Finn, Wright, Friedewald (2013) 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).

²³ 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. It is available here:

<http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflows ofpersonal data.htm>

reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle: Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible 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.

Take as example the information stored in RFID-enabled travel cards used to construct sophisticated traveller or consumer profiles, especially when the travel cards (as the Oyster and Octopus Card largely used in London and Hong Kong) can be used for payment in many of the shops. The data of the cardholders is no more under control. Even if s/he has given consent to the use of data contained in the card, s/he may not imagine that those data can be used to track his/her movements and purchases in order to use this information to create a group profile, then applied to someone else. It is self-evident the challenge towards the collection, the purpose and the use limitation principles.

As a matter of fact, profiling technologies allows the collection of someone's data for one purpose and makes them available to others (both private companies and government agencies) for the same and other purposes; and when these technologies use Big Data risks increase. Although various commentators consider that the privacy risks related to Big Data analytics are low, pointing out the large amount of data processed by analytics and the de-identified nature of most of this data, it is worth remarking that anonymity by de-identification is a difficult goal to achieve. The power of Big Data analytics to draw unpredictable inference from information undermines any strategy based on de-identification. In many cases a reverse process in order to identify people is possible; it is also possible to identify them using originally anonymous data



**Big Data Analytics
increase risks to
privacy**

(Ohm, 2010). But even when such data is anonymous, some data-sets contain such rich information that it can be possible to identify an individual through the matrix of data that is rendered public unless proper precautions are taken. To quote the editors of the Oxford International Journal of Data Protection Law in relation to the collection of personal information, “Big data highlights the need to focus not only on ‘what’ and ‘how’ but also on ‘why’” (Kuner, Cate, Millard, Svantesson, 2012).

As already stated in the Working Paper 1, there is a general lack of transparency in profiling techniques (Hildebrandt, 2009 a, 2009 b) that makes both the Security Safeguards Principle and the Openness Principle far from being taken into consideration.

Individuals become more and more transparent while public bodies, and even private companies, become more and more intrusive, moving in a borderline, where what is lawful is not really clear.

More opacity of individual's data or more transparency of profiling techniques?

It is also important to underline that the choice to hide some information it is a Janus-faced choice. The consequence could be the lack of data quality. For this reason, some scholars (Gutwirth and De Hert 2008, Schermer, 2013) encourage a new transparency of profiling techniques rather than more opacity of the individual.

The consequence of this lack of transparency of profiling techniques is the absence of participation for the individual. As the present discussion of the draft GDPR shows, there is an on-going discussion aimed to guarantee the right to be informed of the existence of profiling and its consequence (see Hildebrandt, 2012). This will have effects not only on the participation of the citizen but also on the respect of the purpose limitation principle and on the accountability.

3.2.2 The Right to Non-Discrimination

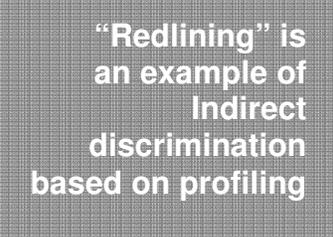
The right to non-discrimination “emanates from the general postulate of the equal dignity of human beings” (Özden, 2011, p.7). It constitutes one of the fundamental and non-derogable principles of human rights and consists of a general principle of equality (i.e. similar situations have to be treated 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. race, gender, religion, etc.) and specific domain of

application (i.e. labour market, vocational training, education, social security, health care, access to goods and services, criminal law).

In the Directive 2000/43/EC²⁴, an important distinction between direct and indirect discrimination has been developed, which is particularly relevant in the context of profiling.

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.

Why is this distinction relevant? Because profiling involves classification and categorization allowing individuals to be categorized on the basis of some characteristics. Rarely this occurs on characteristics, such as ethnicity, race, religion, gender or sexual preference. More often the categorization is based on algorithms used to classify some attributes that can result as proxies of a protected ground. This is clearly a situation of indirect discrimination (for a discussion on how to discover discrimination in large databases see Pedreschi et al,



“Redlining” is an example of Indirect discrimination based on profiling

2013). The best-known example is the one of “redlining”, which is forbidden by law in US only. Redlining is used to identify the practice of denying products and services in particular neighborhoods, 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 neighborhood 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. Another example is the use of criminal records in order to pre-select the candidates for a job. Due to the selective *modus operandi* of law enforcement agencies this may turn to exclude people belonging to specific ethnic groups. Again, an apparently neutral attribute (being respectful of the law is not an unfair request) turns into a discriminatory approach because of the correlation between the belonging to an ethnic group and being responsible of a crime.

As stated by Romei and Ruggieri (2013, p.121) “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”. This is the reason why recently a significant amount of studies relate

²⁴ Refer to: Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML>

to discrimination prevention in data mining and profiling techniques (Custers, Calders, Schermer, Zarsky, 2013, in particular Chapters 8, 12, 13, 14).

4. The legal protection provided by the present legal framework: legal instruments and existing mechanisms

This chapter will explore the actual legal protection of human rights in the field of profiling and the existing mechanisms by discussing how the rights identified in section 3 (*Profiling and fundamental values and rights*) are protected under international human rights instruments, with a focus on European instruments. For each right, we will discuss the main provisions, including its interpretation by authoritative sources as well as in case-law, and we will also discuss, where appropriate, proposals for amending the legal framework. In response to the technological evolution, to the current process of globalization, to the increasing uses and flows of personal data and to the consequent risks for civil liberties and rights, how data protection legislation responds?

4.1 Right to privacy and Right to Data Protection

4.1.1 The relevant European and International legal instruments

In this section a list of the main European and International legal instruments will be presented and briefly analysed.

The **European Convention on Human Rights** (ECHR) establishes basic rules in the context of fundamental rights and liberties. These rules are applicable in all Contracting States, that is all EU Member States and the other members of the Council of Europe. The State Parties are under the obligation to ensure that everyone within their jurisdiction, without regard to nationality or place of

Article 8 of the ECHR guarantees the individual's right to respect for his private and family life, home and correspondence

permanent residence, enjoys the rights guaranteed by the Convention. In addition to the obligations of each State Party under the ECHR, the European Union law also explicitly

incorporates the standards set out in the Convention.

With regard to the right to privacy, Article 8 of the ECHR guarantees the individual's right to respect for his private and family life, home and correspondence. The Article specifies that public authorities may only interfere with this right in narrowly defined circumstances. In particular, any interference must be in accordance with law and necessary in a democratic society, in view of

public interests such as national security and the prevention of crime (See article 8 of ECHR, 1950).

The European Court of Human Rights (ECtHR) has interpreted these provisions in a number of its decisions. In order to assess the legality of a governmental measure affecting individual privacy, under the Convention, the Court goes through 3 steps:

- the Court asks whether a right protected by Article 8 has been interfered with;
- it asks whether the interference was in accordance with law;
- it asks whether the interference was necessary in a democratic society (Privacy International, 2003).

Up to now, there is no case law specifically related to machine profiling. There are instead various relevant cases on databases (see Defining profiling, Working paper 1, PROFILING project²⁵), which is a key step towards machine profiling.

There are some outstanding cases in which the Art.8 is engaged. The ECtHR held in *Amann v Switzerland* (2000)²⁶ that "the storage by a public authority of information relating to an individual's private life amounts to interference within the meaning of Article 8" and that the "subsequent use of the stored information has no bearing on that finding". In *Amann*, the

Up to now there are just cases law related to databases, not yet on machine profiles

European Court of Human Rights found Article 8 applicable when state security services kept records indicating that the applicant was a contact of the Soviet Embassy, after intercepting a telephone call from the Embassy to the applicant. Likewise, in *Rotaru v Romania* (2000)²⁷ the Court found that the storing by the security services of information about the applicant's activities, while a university student, constituted an interference with his Article 8 rights. A good analysis of the proliferation of large-scale databases and their impact on fundamental rights and freedoms is retrievable in the INEX Policy Briefs²⁸. In INEX Policy Brief N.10, case *Heinz Huber v. Germany* is analysed: Huber, an Austrian national, moved to Germany in 1996 in order to work there as a self-employed insurance agent.

²⁵ Available at: <http://profiling-project.eu/defining-profiling-first-paper-of-profiling-project-online/>

²⁶ Refer to: *Amman v. Switzerland* (2000), find a summary of the judgment at: <http://echr.ketse.com/doc/27798.95-en-20000216/>

²⁷ Refer to: *Rotaru v. Romania* (2000), find a summary of the judgment at: [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{%22itemid%22:\[%22001-58586%22\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{%22itemid%22:[%22001-58586%22]})

²⁸ INEX project: <http://www.inexproject.eu/index.php> The Policy Briefs were developed within WP2 by Gloria González Fuster, Paul de Hert, Erika Ellyne and Serge Gutwirth.

Personal data relating to him was stored in the German Central Register of Foreign Nationals (*Ausländerzentralregister*, AZR): Taking the view that he was discriminated because no such database existed in respect of German nationals, Huber, having initially failed to secure the deletion of that data, commenced legal proceedings before the Administrative Court in Cologne, which upheld his claim. The court held that the general processing through the AZR of data regarding a Union citizen who is not a German national could be justified by the objective of the swift treatment of cases relating to the right of residence of foreign nationals. The storage and processing of that data was contrary to various provisions of European law. The European Court of Justice concluded then that the database was not contrary to Community law, but its use for crime fighting purposes had to be interpreted as the putting in place of a system of processing for personal data precluded by the principle of non-discrimination of EU-citizens.

A challenging judgement involving Art.8 was pronounced by the ECtHR in the case *S. and Marper v. The United Kingdom*. The proceedings concerned two non-convicted individuals who wanted to have their records (fingerprints, cellular samples and DNA profiles) removed from the DNA database used for criminal identification in the United Kingdom. In its ruling, the Court established that it is contrary to the requirements of the ECHR to store for unlimited periods of time that type of personal information related to innocent people in a database of that nature. It concluded that the kind of powers granted to UK authorities represented a disproportionate interference with the applicants' right to respect for private life, amounting therefore to a violation of Article 8 of the ECHR.

In addition, the protection of the right to privacy and data protection was already defined in the **Universal Declaration of Human Rights** of 1948, which states that: "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks" (Article 12, Universal Declaration of Human Rights). In addition, the concept of privacy as a right has been reiterated in numerous international human rights legal instruments, such as the International Covenant on Civil and Political Rights (ICCPR) (article 17); the UN Convention on Migrant Workers (article 14) and the UN Convention on Protection of the Child (article 16).

Council of Europe
Convention 108 is
aimed at
strengthening data
protection

The Council of Europe Convention 108 was opened for signature on 28 January 1981. The general object of the Convention is to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them. The need for such legal rules became urgent

due to the increasing use made of computers for administrative purposes. As stated in the Explanatory Report to the Convention, “[I]n modern society, many decisions affecting individuals are based on information stored in computerized data files [...] However there is a lack of general rules on the storage and use of personal information and in particular, on the question of how individuals can be enabled to exercise control over information relating to themselves which is collected and used by others”²⁹.

According to the CoE report of 2008³⁰ - Application of Convention 108 to the profiling mechanism “specific profiling”³¹ comes within the scope of Convention 108 and [...] specific or individual profiles constitute personal data in connection with which those concerned have the rights specified in that Convention”³². In order to answer the question whether profiling constitutes a form of personal data processing, the issue of anonymity is central. Convention 108, as well as Directive 95/46/EC, has offered protection against infringements of individual freedoms and privacy only in case of inappropriate uses of personal data, that is data on identified or identifiable individuals. Profiling involves the processing of data that is “anonymous, anonymised or coded in the first two stages of personal data [...], to which the rules governing the profiling of identified persons have been applied”³³. An agreement on what ‘fully anonymised data’ signifies is needed. According to Pfitzmann (2009) definition, “Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set”, which means that data that contains an individual identifier is not anonymous, if other personal data contains or might contain the same individual identifier. And the processing of data that is purely anonymous at the outset fall outside the scope of Convention 108.

There is not a shared definition of “fully anonymised data”

The preamble of Convention 108 calls for the respect of the rule of law, as well as of human rights and fundamental freedoms. “Putting individuals in control of their personal data being a major objective of the Convention, it is proposed to specifically mention the right to control one’s data and human dignity in the preamble. Another preamble paragraph refers to essential balance to be struck between data protection and freedom of expression, which takes on another

²⁹ Council of Europe, “Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, ETS n. 108, available online at: <http://conventions.coe.int/Treaty/en/Reports/Html/108.htm>

³⁰ Council of Europe, 2008, “Consultative Committee of the Convention for the protection of Individuals with regard to automatic processing of Personal Data”, T-PD(2008)01.

³¹ The term “specific profiling” is used by Bygrave (2002), Data protection law: Approaching its rationale, logic and limits when profiles are based on the collection and analysis of information about specific individuals, with no inference or prediction based on external sources.

³² CoE, 2008, p.3.

³³ CoE, 2008, p.31.

dimension with the Internet: the various applicable fundamental rights have to be reconciled” (CoE, 2012, pp. 2-3).

On the occasion of the 5th edition of the Data Protection Day, the process of modernization of Convention 108 has started. In principle, two main objectives should be pursued within the revision process: to deal with challenges for privacy resulting from the use of new ICTs and to strengthen the Convention’s follow-up mechanisms. Moreover, a discussion is ongoing on whether the Convention and its Additional Protocol should become a global international agreement on data privacy, open to all countries providing an increased level of data protection. Article 23(1) of the Convention already provides for accession by non-member States since 1981. At the Montreaux Conference of Privacy Commissioners of 2005, the representative of Switzerland stated: “[...] now would be a good time for the CoE to issue such an invitation [to third countries], as these accessions could be a step towards a much called-for universal right to data protection which is becoming all more important in today’s world of borderless telecommunication networks” (Greenlaf, 2012, p.20). Similar examples already exist, such as the Cybercrime Convention which was ratified by the U.S. and signed by three other non-European states.

However, there is a general agreement on the fact that “invitations to accede to the Convention 108 should not be issued to countries which fail the tests of democracy, human rights and the rule of law, even if they do have data privacy law” (Greenleaf, 2012, p.28).

Articles 5-8 of Convention 108 - within chapter II - provide a set of data principles including most of the elements nowadays recognized as core data privacy principles. “All that Chapter II includes are familiar principles requiring ‘appropriate’ data security (art.7) and rights to ascertain the existence of personal files, to access them, and to correct them (art.8). There is also a provision for ‘sensitive’ data in article 6: ‘personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [or criminal convictions], may not be processed automatically unless domestic law provides appropriate safeguards’ ” (Greenleaf, 2012, p.22).

**Articles 5-8 of
Convention 108
provide a set of
core data privacy
principles**

Having established the process by which profiling occurs, the Council notes that given that basing a decision on inaccurate or poorly applied statistics can have an unjustly, detrimental effect upon an individual, the definition of ‘profiling’ must be accompanied by a series of checks and balances. In specifying which checks should be enacted, the Council offers a series of relatively straight forward

guidelines. Notably, it reports that the right to access private information must be re-enforced, the right to objection should more thoroughly provided for and the principle of accurate data should be respected. Additionally, the Council points out that when discussing anything which balances private and public interests the principles of proportionality and fairness should be upheld. Although the Council does not provide a specific set of qualities that could render profiling fair and proportional, it points to some aspects of it that could be taken into consideration. Firstly, it recommends that the data collected on an individual should not be used for advertising purposes unless the person is notified. This, it adds, is not a recommendation designed at distinguishing between the private and public uses of data but is merely aimed at insuring that general data is used for purposes that respect the public interest. On this instance, the Council explicitly notes that any attempt of creating different data protection measures for public and private companies is bound to fail in principle because (a) public companies are increasingly hiring private companies to carry out their projects and (b) private companies may be carrying out work that is in public interest but simply not manageable within the public budget. Secondly, it notes that the relevance of data must always be adequately assessed; in the Council's own words "if the aim is to sell a major consumer product it is irrelevant" with few product exceptions "to ask questions about the academic success of the individual concerned, whether or not they have a goldfish or if they read Asterix. Thirdly, and finally, the Council points to the importance of maintaining reasonable storage duration times, noting that reasonableness is correlated to the value the data holds both for the individual and the public interest objective³⁴.

Focusing on the EC legislation, the following are the relevant provisions pertaining in different ways to data protection and privacy.

Other EU acts on data protection are Directive 95/46/EC, which lays down a general framework for data protection law in the Member States, Directive 2002/58/EC on privacy and electronic communications (as amended by Directive 2009/136) and Council framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Directive 95/46/EC was based on the principles of Convention 108, but specified and developed them in many ways. It aimed to provide a high level of protection and a free flow of personal data in the EU. The **Directive 95/46/EC** of the

³⁴ Observations from the analysis of the European Committee on Legal Co-operation (CDCJ) in the meeting of 17 November 2010, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling: <https://wcd.coe.int/ViewDoc.jsp?id=1693029>

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 (DPD) has been implemented by all 27 EU Member States, as well as the three EEA/ EFTA States: Iceland, Liechtenstein and Norway. Switzerland has also implemented the Directive. In addition, Directive 95/46/EC is the legislative basis for two primary aims of European integration: the Internal Market (in this case the free movement of personal data) and the protection of fundamental rights and freedoms of individuals. The DPD indicates the national law applicable when data is processed in different Member States and also prohibits the transfer of personal data to third countries (i.e., non-EU/EEA) that do not ensure an adequate level of protection (*Article 26.2*). The Directive also establishes and specifies data protection principles to harmonize legislation throughout the EU.

According to the fundamental data protection principles enshrined in the DPD, personal data must be (*Article 6*): (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and where necessary, kept up to date and in a form which permits identification of the data subject for no longer than is necessary. Personal data can only be collected and processed on a legitimate basis, that is (*Article 7*):(a) if the data subject has unambiguously given his/her consent or in other situations, such as for the performance of a contract or a legal obligation, which however, all have in common that in these situations the processing of data must be necessary. The data controller must inform a data subject of his/her representative's identity, of the purposes of the processing for which the data is intended, and of the recipients or the categories of recipients of the data. Furthermore, the data subject has a right of individual participation, which means that he/she has the right to obtain from the controller amongst others confirmation as to whether and for which purposes data relating to him are being processed, as well as knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions.

In addition, it is worthy to analyse the possible impact of Article 15 , which grants "a right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him" - on automated profiling. One might argue that Article 15(1) does not directly prohibit a particular type of decision-making or profile application. Rather it confers on persons, a right to prevent them from being subjected to

such decision-making, if their personal data is processed. This would “leave the actual exercise of the right to the discretion of each person and allow, in effect, the targeted decision-making to occur in the absence of the right being exercised” (Bygrave, 2001, p.3). In other words, the data subject must actively exercise his/her right not to be subjected to an automated decision-making process. Furthermore, there are also difficulties in interpreting the provisions of this article. It is not easy to anticipate what should fall

Article 15 of the Directive 95/46/EC leaves to the data subject the task of defending his/her right not to be subjected to an automated decision-making process

within the cumulative conditions of the article: do personalized advertising banners, that automatically adjust their content according to the visitor’s profile, involve an automated decision that significantly affects data subjects? When do decisions produce legal effects? When do decisions significantly affect data subjects? In which case can a decision be said to be based solely on automated data processing? The current context is different from the one of 1995, when the DPD was written. In any case, it cannot be denied that the use of extensive data profiles of individuals by public and private institutions indeed deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his data shadow. For example, Roosendaal argues that profiling-based advertising could, in some cases, significantly affect individuals through the Pariser’s ‘Filter Bubble’ mechanism (Roosendaal, 2013, p.148)., He also discusses examples of government-based profiling by describing the combination of online and offline data in order to take decisions affecting individuals, for example, by credit rating agencies and banks and insurance companies that collect data (Rosendaal, 2013, p. 143). However, the key question is when the DPD should apply and when not. As long as there is no clarity, the protection goals of the DPD may not be achieved. The individual has to be the central factor around which data processing and data protection takes place. That means that the changing technologies should not be leading in deciding whether the DPD is applicable or not (Roosendaal, 2013, p.234).

For the sector of electronic communications, the EU has considered it needed to complement the general Data Protection Directive with a sector-specific data-

The Directive 2002/58/EC ensures the processing of personal data in the telecommunication sector

protection directive, which was part of a larger set of directives regulating the electronic-communications sector. The Directive 2002/58/EC (Directive on privacy and electronic communications, ePrivacy Directive) particularizes and complements the Directive

95/46/EC with respect to the processing of personal data in the electronic communication sector, ensuring the free movement of such data and of electronic communication equipment and services in the Union. It has been partially amended by the Data Retention Directive 2006/24/EC. This Directive has also been recently amended by Directive 2009/136/EC (Citizens' Rights Directive) as part of the overall review of the regulatory framework for electronic communications, introducing in particular a mandatory personal data breach notification. The Directive has been implemented by all twenty seven EU Member States as well as by the three EEA-EFTA States, Iceland, Liechtenstein and Norway.

Article 7 refers to automated storage and processing of data: "In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users".

The amendment of 2009 addresses especially the growing technical possibilities of scoring and monitoring of user behaviour and profiling which constitute a threat for confidentiality of communication. The amended Article 5(3)³⁵ ePrivacy Directive implements an extended protection for users and subscribers of telecommunications. For this purpose, it introduces the limit of consent: the storing of information or access to information that is already stored in the terminal equipment of the subscriber or user is only allowed on condition that the respective subscriber or user has provided his or her consent in line with Directive 95/46/EC.

Regarding the relevance of profiling in police and judicial cooperation, the relevant legal instrument is the Council Framework Decision 2008/977/JHA. It aims at creating a EU general legislative framework for the protection of personal data in police and judicial cooperation in criminal matters. The Framework Decision does not affect the Convention 108 (and the Additional Protocol), which therefore remain relevant for certain EU instruments relating to police and judicial cooperation which contain specific data protection regimes or data protection clauses.

³⁵ Article 5 Confidentiality of the communications [...] (3) Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. [...]

Art. 20 of GDPR prohibits measures based on profiling without the individual's consent

With regard to the automated individual decisions, Article 7 states that “a decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data, intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subjects legitimate interests”.

As previously mentioned, due to the process of globalization and fast-developing information society, the Directive 95/46/EC did not manage to fully achieve its internal market policy objective. In response to the increasing issues relating to data surveillance and uses and the gaps in the legal framework, the European Commission released a draft **General Data Protection Regulation (GDPR)** in January 2012. The key goals are the following:

1. To update and modernize the existing EU data protection rules in light of technological developments to address, among other things, online privacy, in order to improve the protection of personal data processed both inside and outside the EU.
2. To address the protection of personal data processed by law enforcement and judicial authorities.
3. To give individuals more control over their personal data and facilitate access to and transfer of such data.
4. To harmonize data protection rules across the EU by establishing a strong, clear and uniform data protection framework with a single set of data protection rules and a single national data protection authority.
5. To boost the EU digital economy and foster economic growth, innovation and job creation in the EU.

It is worth mentioning that the Article 20 GDPR³⁶ provides a prohibition on measures based on profiling without the consent of the individual. “The scope of the GDPR is, therewith, much broader than the DPD”. (Rosendaal, 2013, p.260).

The important aspect of the GDPR is the “lack of differentiation” (Rosendaal, 2013, p.260) in the formulation of the provisions, which are therefore

³⁶ “Profiling” is defined as “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” (Article 20(1)).

encompassing a broad array of cases and behaviours. The Proposed Regulation states that ‘data protection is not an absolute right’³⁷, but must be considered in relation to its function in society, and must be balanced with other fundamental rights.

4.2 Right to non-discrimination

As mentioned in section 3.2.2, certain categories of personal data are more likely than others, to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, religion, political opinions, philosophical and other beliefs, as well as membership of an association or trade union. In

Art. 14 of the ECHR and art. 21 the EU Charter of Fundamental Rights protect the right to non-discrimination

response to such infringements of fundamental human rights, both the ECHR and the EU Charter of Fundamental Rights protect the right to non-discrimination.

The ECHR protects all individuals within the jurisdiction of its States Parties. The prohibition on discrimination is guaranteed by Article 14 of the ECHR, which guarantees equal treatment in the enjoyment of the other rights set down in the Convention. Protocol 12 (2000) to the ECHR, expands the scope of the prohibition of discrimination by guaranteeing equal treatment in the enjoyment of any right (including rights under national law). The protocol was created out of a desire to strengthen protection against discrimination, which was considered to form a core element of guaranteeing human rights, and due to the increasing cases regarding sex and racial equality.

The second legal instrument, the Charter of Fundamental Rights of the European Union, legally binds the EU institutions to observe its provisions on non-discrimination. Article 21 of the EU Charter of Fundamental Rights also contains a prohibition on discrimination. The Charter binds the institutions of the European Union, but will also apply to the Member States when they are interpreting and applying EU law. The provision on discrimination contains a combination of both the grounds of the ECHR and the non-discrimination directives (European Union Agency for Fundamental Rights, 2011).

In this context profiling appears when it is considered discriminatory. It is considered as such, where police powers are exercised in relation to individuals and the main reason for this is race, ethnicity or religion. To avoid being

³⁷ See European Commission (2012), p. 6. See also Pia Mifsud Bonnici (2013).

discriminatory, the police decisions should be based on additional factors. So basing on 'reasonable grounds' for identifying a suspect on behavioral factors, the risk of discrimination is reduced. It is clear, that discriminatory ethnic profiling besides being unlawful is also harmful for individuals and for society in general, as it can cause some tensions between different communities, it can harm human dignity, as it ignores that each of us is a unique individual (European Union Agency for Fundamental Rights, 2011).

It is also proper to highlight that machine profiling can also enhance non-discrimination, as it can be more neutral than a human being (for example a police officer) who might have a (racial) bias. This is one of the arguments featuring in the debate about Forensic DNA Phenotyping (FDP)³⁸ or 'ethnic inferencing' from crime-scene DNA samples. Koops and Schellekens, in their accurate paper, question that the likely ethnic origin of the source of crime-scene DNA (and hence, a potential suspect for the crime) may reinforce existing prejudices against the ethnic minority at large. At the same time, "stigmatization might occur at the individual level when the ethnic origin of the unknown suspect is made public, for instance, in a broadcast description or as a selection criterion in a dragnet investigation, particularly in smaller communities with few representatives of the ethnic minority."(Koops, and Schellekens, 2008, sec. 4)

Conclusions

As it has been underlined the digital representations of an individual pose serious challenges to the debate on how to guarantee persons' rights. This happens for digital persona and - as the current debate on the Draft GDPR shows – it is even more complicated for profiles.

Moreover, fundamental values such as democracy, rule of law, autonomy and self-determination are jeopardized by the technological developments.

The threat to fundamental rights and values are interrelated, overlap and fuel each other. Profiling may challenge the essence of democracy because it moves to the background the role of human beings in the decision-making process and creates unbalanced distribution of power and knowledge asymmetries among citizens on one side and government and corporate business enterprises on the other side. Decisions based on automated profiling techniques do not allow the

³⁸ Koops, 2008, p.158: "Forensic DNA phenotyping is an interesting new investigation method: crime-scene DNA is analyzed to compose a description of the unknown suspect, including external and behavioral features, geographic origin and perhaps surname. His method is allowed in some countries but prohibited in a few others."

citizens to challenge the reasoning behind the process. This clearly hampers a full and free development and expression of one's personality and his/her effective participation to the democratic life.

Profiling techniques have a broad range of application areas. In most of the domains benefits coexist with risks of violation of fundamental rights. Right to privacy and data protection and right to non-discrimination are the main rights put under risks by profiling techniques.

In some of these domains the clash between the interest of corporations (e.g. insurance companies, banks, etc.) and the rights of the citizens emerge vividly. In other cases the question that arises is: to what extent citizens are willing to allow broad control in order to reduce the risk of a security threat? Are they more willing to give access to sensitive information if this can improve the health services and the possibilities to answer to new health needs?

It is hardly impossible to give a final answer. It is certain that the present level of guarantees given by the legal framework is far from an adequate level of protection.

Three are the possible lines of intervention to increase protection.

The first is to move in the data protection legislation to a goal-oriented approach: the level of protection depends on the goal of data processing and the level of risks. No matter if the data are personal or not. The focus shifts on the purpose. Some traces of this approach can be found in the present debate on the draft GDPR.

The second is to encourage innovation in finding technological solutions to the risks of discrimination and of attacks to privacy and data protection. Time, budget constraints and the cultural approach of public administration, in particular in some EU countries, may hamper the effective implementation of this solutions but it is definitely worth to give a try.

Finally increasing the awareness among citizens is definitely the key issue. Make citizens aware of the value of their own data and of the use of profiling techniques in many areas that directly affect their lives if the only way to make them asking for more transparency in the collection and use of data and so address the issue of the permeability between the public and the private sector in the transfer of data.

References

Benetton A. (2013), Redditometro il ricorso va a segno, in The Fielder, 11 March. Available at: <http://thefielder.net/11/03/2013/redditometro-il-ricorso-va-a-segno/#.UIVIPFN099R>

Bonnici J.P.M. (2013), Exploring the non-absolute nature of the right to data protection, in International Review of Law, Computers & Technology, Vol. 27, n. 3

Bygrave L. A. (2001), Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, in Privacy Law & Policy Reporter, 2000, volume 7, pp. 67–76. Available at: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf

Brause R., Langsdorf T., Hepp M. (1999), Neural Data Mining for Credit Card Fraud Detection, in Proceedings of the 11th IEEE International Conference on Tools with Artificial Intelligence, p. 103, IEEE Computer Society Washington, DC

Canhoto A. (2005), Anti-money laundering profiling, in FIDIS project – Future of Identity in the Information Society, Deliverable 7.2, Descriptive analysis and inventory of profiling practices, pp. 57-58. Available at: <http://www.fidis.net/resources/fidis-deliverables/profiling/#c1764>

Centerstone Research Institute (2010), A Model of Health, IBM, November. Available at: <ftp://public.dhe.ibm.com/common/ssi/ecm/en/yt03158usen/YTC03158USEN.PDF>

Citron, Danielle Keats (2007), Technological Due Process. Washington University Law Review, Vol. 85, pp. 1249-1313.

Clarke R. (1994), The Digital Persona and its Application to Data Surveillance, in The Information Society, vol. 10, no. 2. Available at: <http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html>

Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, Protecting individual Privacy in the Struggle against terrorists. A Framework for Program assessment

Custers B., Calders T., Schermer B., Zarsky T. (Eds.) (2013), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, in Springer-Verlag Berlin Heidelberg

Della Mea V., What is e-Health: The death of telemedicine?, in Journal of Medical Internet Research, 3(2):e22. Available at: <http://www.jmir.org/2001/2/e22/>

ECHR CaseLaw, Case of Amman v. Switzerland, 16 February 2000. Available at: <http://echr.ketse.com/doc/27798.95-en-20000216/view/>

Electronic Frontier Foundation (2009), Report on the Investigative Data Warehouse, April. Available at: <https://www.eff.org/issues/foia/investigative-data-warehouse-report>

Ellis, R. K. (2009), Field Guide to Learning Management System, ASTD Learning Circuits

European Court of Human Rights, Case of Rotaru v. Romania, 4 May 2000, available at: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#%7B%22itemid%22:%5B%22001-58586%22%5D%7D>

European Union Agency for Fundamental Rights (FRA) (2011), Handbook on European non-discrimination law: Case-law update. July 2010 – December 2011, available at: http://fra.europa.eu/sites/default/files/2013-fra-case-law-handbook-update_corr.pdf

Ferraris V., Bosco F., Cafiero G., D'Angelo E., Suloyeva Y. (2013), Defining Profiling, Working Paper 1 of the Profiling project. Available at: http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_definition_0208.pdf

Finn R L., Wright D., Friedewald M. (2013), Seven Types of Privacy, in S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet (eds.) European Data Protection: Coming of Age, pp. 3-32

Fuster G., Gutwirth S., Ellyne E. (2010), Profiling in the European Union: a high-risk practice, in INEX Policy Brief, n.10

Gellert R., de Vries K., de Hert P., Gutwirth P. (2013), A Comparative Analysis of Anti-Discrimination and Data Protection Legislations, in Custers B., Calders T., Schermer B., Zarsky T. (Eds.), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, Springer-Verlag Berlin Heidelberg, pp. 61–89

Goody J. (1997), Representations and contradictions: ambivalence towards images, theatre, fiction, relics and sexuality, Blackwell, Oxford

Greenlaf G., The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?, Research Paper Series, n.2012/12, University of Edinburgh, School of Law

Guagnin D., Hempel L., Jung J. (2013), Evolution of Technologies in Profiling, Working Paper 2 of the Profiling project. Available at: http://profiling-project.eu/wp-content/uploads/2013/08/Evolution-of-Technologies-in-Profiling-08_08.pdf

Gutwirth S., de Hert P. (2008), Regulating profiling in a Democratic Constitutional State, in Hildebrandt, M. Gutwirth S. (Eds.), Profiling the European Citizens, Cross-Disciplinary Perspectives, Springer, pp. 272-293

Gutwirth S., Hildebrandt M. (2010), Some Caveats on Profiling in Gutwirth S., Pouillet Y., de Hert P. (Eds.), Data protection in a profiled world, Springer, Dordrecht, pp. 31-41

Hildebrandt M. (2008b), Profiling and the rule of law, in Identity in the Information Society, vol.1, no.1, pp. 55-70

Hildebrandt M. (2009a), Technology and the End of Law, in Claes E., Devroe W. Keirsbilck B. (Eds.), Facing the Limits of the Law, pp. 443–465

Hildebrandt M. (2009b), Profiling and AML, in Rannenber K., Royer D., Deuker A. (Eds), The Future of Identity in the Information Society. Challenges and Opportunities, Springer, Heidelberg, pp. 273-310

Hildebrandt M (2009c), Who is Profiling Who? Invisible Visibility in Gutwirth S., Pouillet Y., de Hert P., de Terwangne C., Nouwt S. (Eds.), Reinventing Data Protection?, Springer, Dordrecht, pp. 239-252

ICCS (2009), Knowledge-Rich Data Mining in Financial Risk Detection in Computational Science – ICCS, Lecture Notes in Computer Science, Volume 5545, 2009, pp. 534-542

Koops B., Schellekens M. (2008), Forensics DNA Phenotyping: regulatory Issues, in The Columbia Science and Technology Law Review. Available at: <http://www.stlr.org/html/volume9/koops.pdf>

Kuner C., Cate F.H., Millard C., Svantesson D.J.B. (2012), The challenge of 'big data' for data protection, Editorial, International Data Privacy Law (2012) 2 (2): pp. 47-49. Available at: <http://idpl.oxfordjournals.org/content/2/2/47.extract#>

Leenes R. (2008), Do they know me? Deconstructing identifiability, University of Ottawa Law and Technology Journal, 4(1)

Meints M. (2005), Employment, in FIDIS project – Future of Identity in the Information Society, D 7.2, Descriptive analysis and inventory of profiling practices, p.57

Moeckli D., Thurman J. (2008), Counter-terrorism data mining: legal analysis and best practices, in DETECTER project - Detection Technologies, Terrorism, Ethics and Human Rights, Deliverable 8.03

Möller J., Florax B.J. (2002), Kreditwirtschaftliche Scoringverfahren, in Multimedia und Recht (12), pp. 806-811

Nabeth T. (2005), E-learning, in FIDIS project – Future of Identity in the Information Society, D 7.2, Descriptive analysis and inventory of profiling practices pp. 61-63.

OECD (1980), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at:
<http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>

OECD (2013), The OECD Privacy Framework, including the revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Ohm P. (2010), Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, Vol. 57, p.1701

Özden M. (2011), The Right to non-discrimination, in Series of the Human Rights Programme of the CETIM

Pedreschi D., Ruggieri S., Turini F. (2013), The Discovery of Discrimination, in Custers B., Calders T., Schermer B., Zarsky T. (Eds.), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, Springer-Verlag Berlin Heidelberg, pp. 91–108.

Pfutzmann A., Köhntopp M. (2009), Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology, Designing Privacy Enhancing Technologies Lecture Notes in Computer Science Volume 2009, 2001, pp. 1-9

Privacy International (2003), Legal assessment of Communications Data Retention - A violation of the European Convention of Human Rights, 9 September 2003. Available at: <https://www.privacyinternational.org/reports/legal-assessment-of-communications-data-retention-a-violation-of-the-european-convention-of>

Rodotà S. (2009), Data Protection as a Fundamental Right, in Gutwirth S., Pouillet Y., De Hert P., Terwangne C., Nouwt S. (2009), Reinventing Data Protection?, Springer

Romei A., Ruggieri S. (2013), Discrimination Data Analysis: A Multi-disciplinary Bibliography, in Custers B., Calders T., Schermer B., Zarsky T. (Eds.) (2013),

Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, in Springer-Verlag Berlin Heidelberg, pp. 109–135

Roosendaal A. (2010), Digital Personae and Profiles as Representations of Individuals, in Bezzi M., Duquenoy P., Fischer-Hubner S., Hansen M., Zhang G. (Eds.), Privacy and Identity Management for Life. 5th IFIP, WG 9.2, 9.6/11.7, 11.4, 11.6, Prime Life International Summer School Nice, France, September 7-11, 2009, pp. 226-236

Roosendaal A. (2013), Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts, Wolf Legal Publishers, Oisterwijk

Rouvroy A. & Poullet Y. (2009), The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy, in Gutwirth S., Poullet Y., de Hert P., de Terwangne C., Nouwt S. (Eds.), Reinventing Data Protection?, Springer, Dordrecht, p. 45-76

Schermer B. (2013), Risks of profiling and the limits of data protection law, in B. Custers B., Calders T., Schermer B., Zarsky T. (Eds.) (2013), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, in Springer-Verlag Berlin Heidelberg, pp. 137–154

Solove D.J. (2004), Digital Person: Technology and Privacy in the Information Age, New York University Press, New York.

Solove D.J. (2007), 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, San Diego Law Review, Vol. 44, p.745

Steinbock D.J. (2005), Data Matching, Data Mining and due process, in Georgia Law Review, vol. 40, no. 1, pp. 1-84

The Guardian, World News, Edward Snowden. The NSA files. Available at: <http://www.theguardian.com/world/edward-snowden>

Trudel P. (2009), Privacy Protection on the Internet: Risk Management and Networked Normativity, in Gutwirth S., Poullet Y., de Hert P., de Terwangne C., Nouwt S. (Eds.), Reinventing Data Protection?, Springer, Dordrecht, pp. 317-334.

Yi P., Gang K., Yong S. (2009), Knowledge-Rich Data Mining in Financial Risk Detection

WHO (2012), Legal frameworks for e-Health, Global Observatory for e-Health series – volume 5. Available at: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf

Zakaria F. (1997), The rise of illiberal democracy, in Foreign Affairs, vol. 76, no. 6, pp. 22-43

Legal texts

Article 29 Data Protection Working Party, Working Party on Police and Justice, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Adopted on 01 December 2009

Article 29 Data Protection Working Party, Working Party on Police and Justice, Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, Adopted on 5 December 2007 by the Art. 29 Working Party, Adopted on 18 December 2007 by the Working Party on Police and Justice

Article 36 Committee, I/A Item Note to COREPR/ Council, 11858/3/02 REV 3 (Annex), 18.11.2002

Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS n. 108. Available at: <http://conventions.coe.int/Treaty/en/Reports/Html/108.htm>

Council of Europe (1950), European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November, ETS 5. Available at: <http://www.unhcr.org/refworld/docid/3ae6b3b04.html>

Council of Europe (2000), Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, 2000, available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/177.htm>

Council of Europe (2008a), Application of Convention 108 to the profiling mechanism. Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profiling_2008_en.pdf

Council of Europe (2008b), Consultative Committee of the Convention for the protection of Individuals in regard of Automatic Processing of Personal Data, Application of Convention 108 to the Profiling mechanism, Some ideas for the future work of the Consultative Committee (T-PD), 11 January 2008

Council of Europe (2012), The consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data [ETS No. 108], Modernisation of Convention 108: new proposals, DG I Rule of Law and Human Rights

Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27 November 2008. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF>

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, OJ L 281 , 23/11/1995 P. 0031 – 0050

Directive 2000/43/EC of 29 June 2000, implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, Official Journal L 180 , 19/07/2000 P. 0022 – 0026

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) N. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD). Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Committee on Legal Co-operation (CDCJ), (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in

the context of profiling available at:

<https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM>

European Parliament, DRAFT REPORT, with a proposal for a European Parliament recommendation to the Council on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Sarah Ludford.

European Union, Charter of Fundamental Rights of the European Union, 7 December 2000, Official Journal of the European Communities, 18 December 2000 (OJ C 364/01). Available at:

<http://www.unhcr.org/refworld/docid/3ae6b3b70.html>