HAL
archives-ouvertes.fr

Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights

Norberto Andrade

▶ **To cite this version:**

Norberto Andrade. Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. Simone Fischer-Hübner; Penny Duquenoy; Marit Hansen; Ronald Leenes; Ge Zhang. 6th International Summer School (ISS), Aug 2010, Helsingborg, Sweden. Springer, IFIP Advances in Information and Communication Technology, AICT-352, pp.90-107, 2011, Privacy and Identity Management for Life. <10.1007/978-3-642-20769-3_8>. <hal-01559453>

HAL Id: hal-01559453
https://hal.inria.fr/hal-01559453

Submitted on 10 Jul 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Data Protection, Privacy and Identity:
Distinguishing Concepts and Articulating Rights

Norberto Nuno Gomes de Andrade

European University Institute, Law Department, Florence - Italy

Abstract

The purpose of this article is to provide a sound and coherent articulation of the rights to data protection, privacy and identity within the EU legal framework. For this purpose, the paper provides a number of important criteria through which the three different rights in question can be clearly defined, distinguished and articulated. Although intrinsically interrelated, the article draws attention to the importance of keeping the rights and concepts of data protection, privacy and identity explicitly defined and separated.

Based on two proposed dichotomies (procedural/substantive and alethic/non-alethic), the paper makes three fundamental arguments: first, there are crucial and underlying distinctions between data protection, privacy and identity that have been overlooked in EU legislation (as well as by the legal doctrine that has analyzed this topic); second, the current data protection legal framework (and its articulation with the concepts of privacy and identity) presents serious lacunae in the fulfilment of its ultimate goal: the protection of the autonomy, dignity and self-determination of the human person; and, third, the right to identity should be explicitly mentioned in the EU Data Protection Directive.

Profiling is taken as a case study technology to assert the importance of incorporating the right to identity in the EU data protection framework as well to document its current shortcomings.

Keywords: privacy, identity, data protection, EU law, profiling

1. Introduction

The article[1] begins by illustrating the apparently harmonious and coherent manner which the concepts and rights of data protection, privacy and identity have been enshrined and implemented in the European Data Protection Legal Framework, namely in its main instrument: the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data[2] (hereafter: "data protection directive", "DPD" or simply "directive"). The concordant nexus between the concepts of privacy and identity has, moreover, been supported by the legal doctrine that has examined the relationship between these concepts.[3] In this respect, many scholars have pursued a line of reasoning that establishes a harmonious relationship between privacy and identity.

After depicting the current state-of-art of the legislative and doctrinal frameworks concerning the relationship between these three elements, the article then proceeds to its deconstruction and criticism. Therefore, the paper distinguishes the concepts and rights to data protection, privacy and identity. And it does so in two different steps. Firstly, the paper

[1] This paper contains parts of (Andrade, 2010).

[2] 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: see http://eur-lex.europa.eu/LexUriServ/LexUriserv.do?uri=CELEX:31995L0046:EN:NOT

[3] (Agre & Rotenberg, 1997), (Hildebrandt, 2006), (Rouvroy, 2008).

distinguishes data protection, on the one hand, from privacy and identity, on the other. Such distinction underlines the procedural nature of the former in contrast to the substantive character of the latter. Secondly, and relying upon work previously developed by the author, the paper distinguishes privacy from identity based upon the notion of information and through the so-called *alethic* criteria.

Taking into account the fundamental differences between data protection, privacy and identity, the paper then elaborates on the repercussions of such distinctions. For this purpose, the article looks at the use of profiling technologies, focussing in particular on the case of non-distributive group profiling. By taking into account the regulatory challenges that automated profiling processes pose to the directive, the paper puts forward two main arguments: the failure of the EU data protection legal framework to protect the dignity, autonomy and self-determination of the human person (which are at the base of both the right to privacy and the right to identity) and the need to incorporate the right to identity into the data protection directive.

2. The Data Protection, Privacy and Identity "triangle" according to the current EU legislation

The European Union Data Protection legal framework, which is rooted in the data protection directive, presents an apparently harmonious and coherent articulation of the concepts of data protection, privacy and identity. As such, the data protection directive protects the right to privacy by relying upon the notion of identity. In other words, the DPD seeks to achieve privacy protection by regulating the processing of personal data, which is then defined by recourse to the notion of (personal) identity. In what follows, I shall look at how the existing legislation and the legal doctrine currently connect and articulate these three concepts. I will begin by exploring the relationship between privacy and data protection, adding afterwards the identity element.

Privacy and data protection are intimately related. The emergence of the first data protection legislations in the early 1970s, as well as their subsequent developments, were and have been aimed at tackling problems generated by new technologies. Within the broad spectrum of problems to be resolved, the application of those data protection regulatory schemes were – to a great extent – motivated by privacy concerns. In fact, one can say that the incessant development and sophistication of data protection legal frameworks across the last decades has taken place as a result of the fact that individuals' privacy is continuously under threat via increasingly novel means. Poullet describes this phenomenon by distinguishing a series of different generations of data protection legislations,[4] characterizing them as progressive extensions of the legal protection of privacy.

Given this historical background, it comes as no surprise that the underpinning principle of Directive 95/46/EC is the protection of privacy. In fact, the protection of the right to privacy is expressly stated by the EU Data Protection as its main goal. In article 1, the directive states that its objective is:

to protect the fundamental rights and freedoms of natural persons and in particular the right to privacy, with regard to the processing of personal data (Emphasis added)

[4] While the first generation of legislation encompassed a negative conception of privacy, defined as a right to opacity or to seclusion, protecting one's intimacy and linked to specific data, places and exchanges; the second generation, which came into being as a result of the disequilibrium of the balance of informational powers between individuals/citizens and administrations/companies, substituted such negative approach with a more positive one (Poullet, 2010). This new approach is grounded on a set of new principles that correspond to today's data protection principles (such as transparency, legitimacy and the proportionality of the processing of personal data) or, in the United States, to the so-called "fair uses of personal information."

In this manner, the directive, without ever defining the term privacy, seeks to protect it by regulating the processing of personal data.[5] Thus, the interest and the value of privacy are deemed to be protected and sustained through the underlying mechanical procedures of data protection. Therefore, the directive protects privacy by regulating in detail the conditions through which personal data can be collected, processed, accessed, retained and erased.

It is within the definition of personal data, a key concept of the data protection legal framework, that the notion of (personal) identity makes its appearance. Personal data is defined in article 2 of the DPD as:

Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity. (Emphasis added)

In brief, data protection protects privacy by regulating the processing of personal data. The concept of personal data is defined by recourse to the criteria of identifiability, which is then asserted by reference to factors specific to one's identity.

Two important conclusions emerge from this brief analysis. First, the data protection directive seems to be overly oriented to the protection of the right to privacy, neglecting (at least in its wording) other important rights and interests. Second, the notion of identity assumes only a marginal role in this triangle. Identity, in fact, is enshrined in the directive as a secondary notion, placed in the DPD only to facilitate the definition of the concept of personal data and, as such, to ascertain the applicability of the data protection legal framework. In this way, identity is not seen as a right, interest or value to be protected *per se* through data protection, as privacy is, but as a technical criterion that helps to define the concept of personal data. Identity makes its way into the data protection legal framework through the backdoor, as part of the procedural definition of personal data, which – in its turn – is oriented to protect the privacy interests of the data subject. Identity is thus dissolved within the relationship between, and articulation of, privacy and data protection. As a result, the triangle "data protection – privacy – identity" portrayed in the EU legislation is not only a rather static one, but also a profoundly unbalanced one.

Broadly, the right to identity can be defined as the right to have the attributes or the facets of personality which are characteristic of or unique to a particular person (such as appearance, name, character, voice, life history, etc) recognized and respected by others. In other words, the right to identity is the right to be different, that is, the right to be unique.[6] Returning to the analysis of the relationship between privacy and identity, one should note that the marginal role played by the notion of identity and the harmonious relationship between the concepts and rights of privacy and identity does not only transpire from legislation, but it has also been sustained by the legal doctrine.[7] Agre and Rotenberg, in this respect, define the right to privacy as "the freedom from unreasonable constraints on the construction of one's identity."[8] Such perspective is linked to the rationale of data protection and to the idea that the "control over personal information is control over an aspect of the identity one projects in the world."[9] The link between

[5] (McCullagh, 2009).
[6] As we shall see in section 2.2, the right to identity reflects a person's definite and inalienable "interest in the uniqueness of his being" (J. Neethling, Potgieter, & Visser, 1996, p. 39).
[7] (Agre & Rotenberg, 1997), (Hildebrandt, 2006), (Rouvroy, 2008).
[8] (Agre & Rotenberg, 1997, p. 6).
[9] (Agre & Rotenberg, 1997, p. 7).

privacy and the absence of restraints in developing one's identity has been pursued and reconfirmed by other scholars, such as Rouvroy[10] and Hildebrandt.[11]/[12]

As we shall see in the following section, this assumed harmonious connection between "data protection – privacy – identity" is, in reality, deeply flawed and problematic. This triangular relationship is, in fact, much more complex and dynamic than the static and straightforward picture that has been depicted by the current legislation and doctrine. In what follows, I shall deconstruct the accepted position that there is a harmonious web that connects these three elements, proposing new ways and criteria through which to distinguish and articulate such concepts. Firstly, I shall tackle the distinction between data protection, on the one hand, and privacy and identity, on the other. For that purpose, a procedural/substantive dichotomy will be used. Secondly, I will distinguish the scope of the right to privacy and the right to identity through an *alethic* criterion.

2.1 Data Protection vs. Privacy and Identity

A number of studies have been devoted to clarifying the underlying differences between the rights to data protection and privacy, this paper shall focus on those authored by De Hert and Gutwirth.[13] These scholars propose an ingenious way in which to illustrate the differences in scope, rationale and logic between these two rights. They characterize privacy as a "tool of opacity" and data protection as a "tool of transparency." In connecting the invention and elaboration of these legal tools to the development of the democratic constitutional state and its principles, the above mentioned authors state that:

"the development of the democratic constitutional state has led to the invention and elaboration of two complementary sorts of legal tools which both aim at the same end, namely the control and limitation of power. We make a distinction between on the one hand tools that tend to guarantee non-interference in individual matters or the opacity of the individual, and on the other, tools that tend to guarantee the transparency/accountability of the powerful"[14]

In developing the fundamental differences between these tools, the authors explain that:

"The tools of opacity are quite different in nature from the tools of transparency. Opacity tools embody normative choices about the limits of power; transparency tools come into play after these normative choices have been made in order still to channel the normatively accepted exercise of power. While the latter are thus directed towards the control and channelling of legitimate uses of power, the former are protecting the citizens against illegitimate and excessive uses of power."[15]

[10] (Rouvroy, 2008).
[11] (Hildebrandt, 2006).
[12] For a criticism of this conceptualization of privacy, see (Andrade, 2010). In my own view, and as comprehensively developed in the mentioned article, the idea of a right to privacy as "the freedom from unreasonable constraints in developing one's identity" is reductive and one-sided, capturing only one dimension among the many others that compose the spectrum of the intricate relationships between privacy and identity. Furthermore, such proposed concept of (a right to) privacy blurs itself with the one of identity, assuming an overly broad character, claiming some of the definitional and constitutive characteristics that, in truth, pertain to the concept and to the right to identity (Andrade, 2010).
[13] (De Hert & Gutwirth, 2003); (De Hert & Gutwirth, 2006).
[14] (De Hert & Gutwirth, 2006, pp. 66-67).
[15] (De Hert & Gutwirth, 2006, p. 66).

In this way, privacy, as an opacity tool, is designed to ensure non-interference in individual matters, creating a personal zone of non-intrusion. Along these lines, privacy is defined in negative terms,[16] protecting individuals against interference in their autonomy by governments and by private actors. Such protection is enacted through prohibition rules, delimiting the personal and private sphere that is to be excluded from those actors' scope and range of intervention.

Further to this prohibitive feature, the authors also characterize opacity tools as collective and normative in nature. The implementation of these tools, as such, requires a delicate balance of interests with other rights, whose application may supersede the need for individual consent when important societal interests are at stake. In this respect, privacy (as well as identity, I would add) is "a relational, contextual and per se social notion which only acquires substance when it clashes with other private or public interests."[17]

Data protection, on the other hand, is defined as a "tool of transparency." In this way, data protection is described as "a catch-all term for a series of ideas with regard to the processing of personal data. Through the application of these ideas, governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, governmental need for surveillance and taxation, etc."[18] In addition, data protection, contrarily to privacy, has a different rationale. It is not prohibitive by nature. Instead, it operates under the natural presumption that personal information is, in principle, allowed to be processed and used. In this respect, data protection is pragmatic in nature, recognizing that – under democratic principles and for societal reasons – both private and public actors need to be able to process personal information. In this sense, the right to data protection could also be called the right to data processing, as it enables public and private entities to collect and use personal information. Such collection and use are, nonetheless, subject to conditions, procedures, limitations and exceptions. Accordingly, and as De Hert and Gutwirth put it, "[d]ata protection laws were precisely enacted not to prohibit, but to channel power, viz. to promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices."[19] Bearing in mind the societal need to collect, store and process data, along with the relative ease through which entities collecting such data can abuse power and infringe privacy, data protection seems to assume an administrative role. In fact, and as Blume notes, this is one of the functions of traditional administrative law that has been extended to data protection law.[20] Similarly to administrative law, data protection also regulates the activities of other institutions and entities. In the case of data protection, the focus is not only on administrative agencies of government, but

[16] Although De Hert and Gutwirth define privacy as an opacity tool in negative terms, i.e. as rules which prohibit certain acts, the authors also allude to the positive roles of privacy. Regarding the latter, the authors state that "[p]rivacy protects the fundamental political value of a democratic constitutional state as it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards – for example - their sexuality, health, personality building, social appearance and behaviour, and so on. It guarantees each person's uniqueness..." (De Hert & Gutwirth, 2006, p. 72) Nonetheless, and in my view, this positive function of privacy renders the definition of the term too large and overstretched, invading the domains of other specific rights, namely the right to identity.

[17] (De Hert & Gutwirth, 2006, p. 75). The relational and contextual character of the right to privacy, which has been derived from article 8 of the European Convention on Human Rights (ECHR), the right to respect for private and family life, is evident in the wording of article 8.2. Such article, in this respect, is an excellent example of how the respect for privacy is not absolute and can be restricted by other interests, namely by "the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[18] (De Hert & Gutwirth, 2006, p. 77).

[19] (De Hert & Gutwirth, 2006, p. 77).

[20] (Blume, 1998).

on "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[21]

Despite their differences, the tools of opacity and transparency do not exclude each other. On the contrary, "[e]ach tool supplements and pre-supposes the other."[22] The quality of a legal framework depends on the adequate blending of the two approaches, that is, on the balance between a privacy-opacity approach (prohibitive rules that limit power) and a data protection-transparency approach (regulations that channel power).[23] In this way, "[a] blend of the two approaches will generally be preferable, since a solid legal framework should be both flexible (transparency) and firmly anchored in intelligible normative approaches (opacity)."[24]

As a result of these observations, a crucial distinction can be made between data protection, on the one hand, and privacy and identity on the other. Data protection is procedural, while privacy and identity are substantive rights.

While substantive rights are created in order to ensure the protection and promotion of interests that the human individual and society consider important to defend and uphold, procedural rights operate at a different level, setting the rules, methods and conditions through which those substantive rights are effectively enforced and protected.

Privacy and identity, as substantive rights, represent specific interests of the human personality and presuppose the making of normative choices. Those rights and interests (such as, among others, freedom of expression or security) are often in conflict, a fact which requires them to be balanced and measured against each other. It is through the weighing and balancing of these (conflicting) interests and rights that, in the case of privacy, certain intrusions to one's private sphere are deemed to be necessary and acceptable, while others not. In the case of privacy as an opacity tool, its substantive character is reflected in the normative choice and interpretation required to determine what is to be deemed so essentially individual that it must be shielded against public and private interference. Such normative choices, interpretative exercises and balancing processes are exclusive to substantive rights.

Procedural rights, on the other hand, only appear at a later stage. It is only after the weighing and balancing of the substantive interests and rights in question that procedural rights come into play, laying out the legal conditions and procedures through which those substantive rights are to be effectively enforced. In other words, procedural rights lay out the conditions through which substantive rights are to be articulated. Procedural conditions, such as the ones concerning transparency, accessibility and proportionality, function as indispensable conditions for the articulation and coordination between different interests and rights. The data protection directive is an excellent example of such procedural exercise. In order to conciliate the right to privacy, on the one hand, and the free flow of information within the internal market, the directive furnishes a number of procedural guidelines and principles through which to attain such balance.[25] Such

[21] Directive 95/46/EC, article 2(d).

[22] (De Hert & Gutwirth, 2006, p. 94).

[23] In spite of such necessary and welcoming 'mix' of approaches, these tools should not be blurred. In fact, De Hert and Gutwirth call the attention to the importance of not blurring this distinction, as each tool has its proper logic. As an example of the perils that such blurring may cause, the scholars turn their attention to European human rights law and to what they call the "danger of proceduralization", focussing on the article 8 of the European Convention of Human Rights (ECHR). This legal disposition, due to the interpretation made by the European Court of Human Rights in Strasbourg, is shifting from a prohibitive and opacity logic to a channelling one, becoming a transparency-promoting vehicle (De Hert & Gutwirth, 2006, p. 87). The problem we have here is, in brief, the construction of substantive norms through elements of procedural rights. As a result, "[t]he transformation of Article 8 into a source of procedural rights and procedural conditions takes it away from the job it was designed for, viz. to prohibit unreasonable exercises of power and to create zones of opacity" (De Hert & Gutwirth, 2006, p. 91).

[24] (De Hert & Gutwirth, 2006, p. 95)

[25] These basic principles are summarized in article 6 of the Directive, and include the requirements that personal data must be:

procedural conditions, as such, also operate as legitimate restrictions for substantive rights enshrined in the directive.

As a result, and contrary to privacy, data protection is inherently formal and procedural. It is structured and shaped according to the interests and values of other substantive rights and legitimate interests, emerging as a result of the clashes between such different rights and interests. Thereby, "[t]he main aims of data protection consist in providing various specific procedural safeguards to protect individual's privacy and in promoting accountability by government and private record holders"[26] (emphasis added). As such, the goal of data protection is to ensure that personal data is processed in ways that respect or, at least, do not infringe other rights. Or, to put it in a positive way, data protection only exists to serve and pursue the interests and values of other rights. In other words, data protection does not directly represent any value or interest *per se*, it prescribes the procedures[27] and methods for pursuing the respect for values embodied in other rights (such as the right to privacy, identity, freedom of expression, freedom and free flow of information, etc), ensuring their articulation and enforcement. As Poullet clearly states "[d]ata protection is only a tool at the service of our dignity and liberties and not a value as such."[28]

One of the important conclusions to derive from this analysis is that data protection, on the one hand, and privacy on the other, do not fit perfectly into each other. There are important mismatches that need to be acknowledged and underlined. "Data protection explicitly protects values that are not at the core of privacy."[29] This is the case of the requirements of fair processing, consent or legitimacy, which pertain to the specific procedural nature and justice associated with data protection. This is also the case of the protection of rights and liberties such as the freedom of religion, freedom of conscience and the political freedoms. Such rights and liberties are, in effect, protected by the directive through the special regime for "sensitive data," which prohibits the processing of data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, etc.

Data protection protects the value and interest of privacy as it protects the value and interest of identity, security and freedom of information, among others. They do not always overlap. In this respect, data protection is both larger and more restricted than privacy (and vice versa). The

---

(a) processed fairly and lawfully;

(b) collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that member States provide appropriate safeguards;

(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 data; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

[26] (De Hert & Gutwirth, 2006, p. 77). Emphasis added.
[27] In this point, and as De Hert and Gutwirth observe, "[t]he sheer wordings of the data protection principles (the fairness principle, the openness principle and the accountability principle, the individual participation principle, …) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice" (De Hert & Gutwirth, 2006, p. 78).
[28] (Poullet, 2010, p. 9).
[29] (De Hert & Gutwirth, 2006, p. 81).

autonomy and difference between data protection and privacy has, moreover, been acknowledged by the Charter of Fundamental Rights of the European Union which, with the entry into force of the Lisbon Treaty, was given legal binding effect equal to the Treaties. In this way, article 8[30] of the EU Charter now establishes data protection as a separate and autonomous right, distinct from the right to privacy (which is enshrined in article 7).

Furthermore, and looking not at the EU level but at the individual member states, the intricate link between data protection and privacy is not always a given. While Belgium, for instance, has always linked data protection to privacy, France and Germany have based their rights to data protection on the right to liberty and on the right to dignity, respectively. The constitutions of those countries, presenting no explicit right to privacy, have nonetheless provided consolidated legal grounds on which to derive and recognize their data protection rights.[31] In the same way, the United States have not followed the right to privacy as the legal anchor for their data protection regulation, but have based the latter in public law, namely through the so-called fair information practices.[32] All of these facts clearly show that there are several and clearly distinct bases upon which to ground the right to data protection, rendering erroneous the reduction of the latter to a unique dimension of privacy. This demonstrates, in addition, that data protection is an instrument protecting several different values and interests, and that no specific advantage is gained by linking it solely to privacy.

Returning now to the triangle, it is important to remember at this point that data protection can and should be clearly distinguished from privacy and identity. The former is a procedural right while the latter are substantive ones. The next section delves into the substantive nature of the rights to identity and privacy, proposing a criterion through which to distinguish them.

2.2 Privacy vs. Identity [33]

The right to privacy and the right to identity share the same DNA. They are both part of a larger set of rights called personality rights[34] and, as such, they both derive from the fundamental rights to dignity and self-determination. Hence, they both reflect the dignity interest that all of us possess.

Contrary to the right to data protection, the rights to privacy and identity are not procedural but substantive rights. They embed particular values and, as such, protect specific interests of the human personality. Regarding their distinction, only a very restricted number of works have

[30] The article, entitled "Protection of personal data", states that "Everyone has the right to the protection of personal data concerning him or her."

[31] The diversity of approaches followed by different EU member states in the legal anchoring of their respective data protection regulations also constitutes a strong reason supporting the recognition of a constitutional right to data protection in the EU Charter, different and separate from the one of privacy. Such recognition is, in fact, "more respectful of the different European constitutional traditions" (De Hert & Gutwirth, 2006, p. 81).

[32] (De Hert & Gutwirth, 2006, p. 82).

[33] This section includes parts of (Andrade, 2010) Where it is argued that the overly broad definition of privacy has undermined the concept of, and therefore the right to, identity. The relentless inflationary trend in the conceptualization of the right to privacy is presented as the main reason behind the need to articulate in a coherent manner the right to privacy and identity. The article, moreover, specifies the main (and often overlooked) differences between the right to privacy and identity, describing in detail how each of them relate to a different interest of the right to personality.

[34] Following Neethling's study of this particular category of rights: "[t]here is general consensus that personality rights are private law (subjective) rights which are by nature non-patrimonial and highly personal in the sense that they cannot exist independently of a person since they are inseparably bound up with his personality. From the highly personal and patrimonial nature of personality rights it is possible to deduce their juridical characteristics: they are non-transferable; unhereditable; incapable of being relinquished or attached; they cannot prescribe; and they come into existence with the birth and are terminated by death of a human being."(Johann Neethling, 2005, p. 223).

touched upon the underlying differences between these two interests and rights.[35] The tendency, as mentioned before, has been to associate the right to privacy with the value and interest of identity. In addition, the assumption that the right to privacy equates to "the freedom from unreasonable constraints on the construction of one's identity,"[36] has remained unquestioned and undisputed. It is as if privacy is the presupposition of identity and identity is the consequence of privacy.

From an informational perspective, these two concepts also seem to be tied together. As such, the fact that privacy tends to encompass information intimately connected to one's identity has led to the idea that "privacy protects the right of an individual to control information that is intrinsically linked to his or her identity."[37] Following such perspective, privacy and identity seem to act as collaborating partners, defining and contextualizing the type of information that is closely attached to a given person, endowing him or her with the right to exert control over such information. While this view is not incorrect *per se*, it is limited and short sighted.

Despite their common history and background, identity and privacy - as rights - protect different interests. Identity, as an interest of personality, can be defined as a "person's uniqueness or individuality which defines or individualises him as a particular person and thus distinguishes him from others."[38] In this account, identity is manifested in various *indicia* by which that particular person can be recognized. Such *indicia*, in other words, amount to the facets of a person's personality which are characteristic or unique to him or her, such as their life history, character, name, creditworthiness, voice, handwriting, appearance (physical image), and so on.[39] As a result, the right to identity reflects a person's definite and inalienable "interest in the uniqueness of his being."[40] According to such conceptualization, a person's identity is infringed if any of these *indicia* are used without authorization in ways which cannot be reconciled with the identity one wishes to convey.

In order to clearly differentiate the right to privacy from the one of identity, I defend a more delimited conceptualization of the former.[41] I thus argue against the trend of over-stretching the definition and scope of the right to privacy.[42] Following such delimited conceptualization, the right to privacy protects an interest that has been defined as a "personal condition of life characterised by seclusion from, and therefore absence of acquaintance by, the public."[43] In these terms, privacy can only be breached when third parties become acquainted with one's true private facts or affairs without authorization. As we shall see in the following, this distinction bears important consequences once transposed to an informational science dimension and applied to the current EU data protection legal framework. As we shall see, such a distinction

[35] See (J. Neethling, et al., 1996); (Sullivan, 2008); (Pino, 2000).
[36] (Agre & Rotenberg, 1997, p. 6).
[37] (Boussard, 2009, p. 252).
[38] (Johann Neethling, 2005, p. 234).
[39] (Johann Neethling, 2005, p. 234).
[40] (J. Neethling, et al., 1996, p. 39).
[41] This paper, following the same line of thought I have developed in previous works, advocates a more restricted conceptualization of the term privacy. Hence, I lean towards an understanding of privacy along the lines of the classical definition given by Warren and Brandeis, that is, as a "right to be let alone" (Warren & Brandeis, 1890). In this way, I envisage a more negative configuration of privacy, conceptualizing the latter as a right to seclusion. Thereby, and as I shall develop in the following sections, I associate privacy with the control over truthful information regarding oneself, and not with generalist and overstretched understandings of privacy as freedom, self-determination and personality building.
[42] Among the many meanings and purposes that have been attached to the term, the right to privacy has been understood, for example, as providing the conditions to plan and make choices concerning one's private life, as well as forbidding the distortion of one's image. The concept of privacy has also encompassed the freedom of thought, the control over one's body, the misapprehension of one's identity and the protection of one's reputation (among other aspects).
[43] (Johann Neethling, 2005, p. 233).

helps to clarify the articulation between the rights to privacy and identity within the data protection legal framework, as well as to better understand and interpret the concept of personal data.

2.2.1 Identity and Privacy distinguished through an *alethic* criterion

Based upon the different interests of personality pursued by the rights to privacy and identity, and bearing in mind their distinction in terms of harmful breach, the following part of this article seeks to provide a new angle through which to distinguish these two rights. Such distinction is based on the different type of information that each of these rights protect.

As briefly mentioned in the previous section, the right to identity is infringed if person A makes use of person B's identity *indicia* in a way contrary to how that person B perceives his or her identity. This will happen, for instance, when person B's identity is falsified or when an erroneous image of his or her personality is conveyed. The right to privacy, on the contrary, is only infringed if true private facts related to a person are revealed to the public.[44] Neethling summarizes the distinction between identity and privacy in the following manner: "[i]n contrast to identity, privacy is not infringed by the untrue or false use of the indicia of identity, but through an acquaintance with (true) personal facts regarding the holder of the right contrary to his determination and will."[45] In this regard, it is important to stress that while the right to identity concerns all of those personal facts - regardless of being truthful or not – which are capable of falsifying or transmitting a wrong image of one's identity, the right to privacy comprises only those true personal facts that are part of one's private sphere and which, by one reason or the other, spill over to the public sphere.[46]

Applying such important findings to the notion of information and within the context of data protection, I propose a criterion that distinguishes two different kinds of personal information, one concerning privacy interests, and the other related to identity ones. This criterion, which I have termed as '*alethic* criterion' (from *αλήθεια* [*aletheia*]: the Greek word for truth), differentiates between personal information that is truthful and objective from that which is not (or, at least, not necessarily). In this way, and according to such criteria, it is argued that only personal information that qualifies *alethically* (in which there is a correspondence between the concept of personal data and the set of true and objective facts or acts related to the data subject) shall be protected under the right to privacy, whereas personal information that is not necessarily truthful (or that is false or de-contextualized) shall be covered by the right to identity. In other words, it is based upon whether personal information represents or conveys a truth or a non-truth (depending on whether it has an *alethic* value or not) that the processing of personal data will be deemed relevant to identity or privacy (purposes).

It is on the basis of this proposed distinction that I shall develop, in the following section, two important arguments. First, I shall sustain that the current data protection legal framework (and its articulation with the concepts of privacy and identity) presents serious lacunae in the fulfilment of its ultimate goal: the protection of the autonomy, dignity and self-determination of the human person. Second, I shall argue that the right to identity should be explicitly mentioned in the EU Data Protection Directive.

---

[44] In this respect, Pino affirms that: "[t]he first feature of the right to personal identity is that its protection can be invoked only if a false representation of the personality has been offered to the public eye. This feature makes it possible to distinguish the right to personal identity from both reputation and privacy" (Pino, 2000, p. 11).

[45] (Johann Neethling, 2005).

[46] This particular conceptualization, furthermore, corresponds to the notion of privacy advocated by writers such as Archard, who defines privacy as "limited access to personal information", that is, "the set of true facts that uniquely defines each and every individual" (Archard, 2006, p. 16).

3. The lacunae of the current data protection legal framework

As I have observed earlier on, the data protection directive is (at least in its wording) overly oriented to the protection of privacy, downgrading identity to a technical component of the definition of personal data. As a consequence, and looking at the principles that are at the core of both the right to privacy and identity, it can be observed that the directive, in almost exclusive terms, tends to protect the individual's dignity and self-determination from an exclusive privacy point of view. The data protection directive protects privacy through the regulation of the processing of personal data, operating on the basis of an identification procedure. Hence, the rules of data protection will only be applicable if the processing of data allows for the data subject to be identified. Such a construction, as I attempt to demonstrate in the following sections, is deficient and inadequate, failing to protect the individual's autonomy and self-determination when other important personality interests are at stake (namely his or her identity interests). Such failure is particularly evident in the case of profiling technologies.

3.1 Profiling Technologies

In terms of definition, "the term profiling is used to refer to a set of technologies that share at least one common characteristic: the use of algorithms or other mathematical (computer) techniques to create, discover or construct knowledge out of huge sets of data."[47] In a more technical fashion, profiling can be defined as:

"the process of 'discovering' patterns in databases that can be used to identify or represent a human or nonhuman subject (individual or group) and / or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify a subject as a member of a group"[48]

In the case of profiles on human subjects, they can be defined as digital representations[49] that refer to unknown or potential individuals instead of to a known individual. As such, the concerned individuals are not identified in those profiling practices.[50]

Taking into account the several distinctions and categorizations that can be made within the general process of profiling: individual or group, direct or indirect, distributive or non-distributive,[51] we will use as a case-study the most problematic one, that is, group profiling of a non-distributive type. This type of profiling is particularly challenging as a non-distributive profile identifies a group of which not all members share the same characteristics.[52] As such, the link between non-distributive group profiles and the persons to whom it may be applied is opaque.[53] In other words, this specific type of profiling represents a group and reveals attributes that may (or may not) be applicable to the individuals in such group. Accordingly, the profile is not inferred from the personal data of the categorized person but inferred from a large amount of

[47] (Hildebrandt, 2009, p. 275).
[48] (Hildebrandt & Gutwirth, 2008, p. 19).
[49] They are not the only modalities of digital representations. For an analysis of the commonalities and differences between profiles and digital personae as both forms of digital representations, as well as the implications of such distinction to the current data protection directive, see (Roosendaal, 2010)
[50] (Roosendaal, 2010, p. 235).
[51] For a concise explanation of such distinctions, see (Hildebrandt, 2009, pp. 275-278).
[52] (Hildebrandt, 2009).
[53] (Leenes, 2008).

often anonymized data relating to many other people. In this way, one of the major risks linked to these profiling practices lies in the fact that "the process results in attributing certain characteristics to an individual derived from the probability (dogma of statistical truth) that he or she belongs to a group and not from data communicated or collected about him or her."[54]

This is problematic in the sense that the processing of this data is not covered by data protection regulations. Besides the fact that these profiles are built without the awareness of the subject, who has no means to influence how the data set is used to make decisions that will affect him or her, there is no direct connection between the profile and the individual. This means, consequently, that the data corresponding to such profile does not qualify as personal data. In short, data protection is not applicable as tool of protection in these cases, and non-distributive group profiles are excluded from the scope of the data protection legal framework.

Therefore, individuals, in this case, are not only influenced by decisions taken on the basis of such profiles, but are also prevented from making use of the rights given by the data protection directive to protect them. This is the type of situation where there are serious lacunae the legal framework of data protection [55] and where the right to identity may prove to be very useful. In my view, the lessening of one's autonomy and self-determination caused by such profiles (namely by the way they influence how one's identity is represented and projected) cannot be tackled by combining provisions regarding data protection, privacy and personal data. This is, in my opinion, a case to be solved by the right to identity and by the application of the data protection directive to non-personal data.

The problem we have here is that some types of digital representations cannot be connected to a specific individual person. This fact renders the information in question non-personal data, which – consequently – precludes the applicability of the DPD. Nevertheless, the data sets constituting such profiles are used to make decisions that affect the individual person. In order to suppress such a legal gap, which cannot be resolved through the privacy-identification paradigm of the current data protection directive, we need to turn our attention to the right to identity.

In what follows, I thus defend the explicit recognition of the right to identity in the data protection framework.

4. Inserting the right to identity in the EU data protection directive

The use of profiling technologies seen in the previous section does not raise a question of privacy, but of identity. In fact, the application of such technology does not involve the disclosure of true facts regarding the data subject. That technology, on the contrary, involves the processing of information which may not necessary be truthful (or which may even be false). Despite not being retraceable to the individual in the "shape" of personal information, the processing of such information still affects the targeted person, infringing her right not to be misrepresented, that is, her right to identity. In the sense that group profiles are used to infer preferences, habits or other characteristics that the profiled person may be found to have (or not), they do not convey a necessary true-condition, presenting instead the possibility of misrepresenting the profiled individual. Thereby, they should be covered by the right to identity.

Taking into account the rationale of the right to identity, I argue for its explicit inclusion in the data protection framework.[56] In this way, the DPD could be interpreted in the light of the

[54] (Poullet, 2010, p. 16).

[55] In this regard, I am not defending an overall application of the DPD to all data processing, regardless of being personal or not (as that, as Roosendall observes, "might have major, probably undesirable, consequences for the way industry and commerce are organized")

[56] The Data Protection directive mentions the terms "privacy" and "right to privacy" thirteen times, while the term "identity" is only mentioned three times (and either as part of the technical definition of personal data, or as part of

right to identity and therefore also regulate the processing of types of non-personal data[57] involved in the construction of non-distributive group profiles.[58]

In the present state of affairs, the data protection directive is based upon the concept of privacy and constructed under a logic of identification. As such, the directive is only applicable if it processes data that allows for a specific person to be identified. In so doing, the DPD neglects the concept of identity and the logic of representation. According to the latter, what is becoming increasingly important is how data and information are being used to represent someone, and not to merely identify him or her. In other words, the issues raised by the processing of personal information cannot only be about disclosing information involving someone's privacy, but also of using such information to construct and represent someone else's identity.

In addition, it is also important to note that the enshrinement of the right to identity in the data protection directive is not only justified in light of the need to cover the processing of non-personal data in the case of group profiles, but also (and primarily) in light of the need to process personal data in accordance with its most recent understanding.

Taking into account the proposed *alethic* criterion, according to which identity concerns true facts while privacy deals with not-necessarily true data (false or de-contextualized), and bearing in mind that the concept of personal data, enshrined in the DPD, is currently understood as encompassing any information relating to a person, regardless of being objective or subjective, true or false,[59] it is possible to arrive at the following conclusion: a large portion of personal data currently being processed concerns a person's identity, and not necessarily his or her privacy. Moreover, this means that the rules on the protection of personal data (defined as any information, truthful or not, relating to an identified or identifiable person) go clearly beyond the protection of privacy, covering also the protection (and promotion) of one's identity. Therefore, and taking into account the need to protect the individual human person from a representative perspective, and not only from an identifiability standpoint, I argue that it is through the enforcement of both rights to identity and privacy through data protection rules that a more solid and complete protection of an individual's autonomy, dignity and self-determination can be achieved.

5. Conclusion

In this article I have distinguished and articulated the rights to data protection, privacy and identity. In this respect, I have deconstructed and criticized the allegedly harmonious approach through which this triangle of concepts has been depicted in EU legislation and by the legal

---

the information related to the data subject that data controllers are oblige to provide the latter with [namely the identity of the controller]). The term "right to identity" is never mentioned in the directive.

[57] The protection of privacy regardless of personal data being processed or not is, in fact, a trend that can already be observed in EU legislation. This is the case with the E-Privacy Directive and its recent revision. Poullet, in this respect, cites recital 24 (which suggests a comparison between the terminal equipment of a user and a private sphere similar to the domicile), qualifying it as a provision that "clearly focuses on protection against intrusion mechanisms irrespective of the fact that personal data are processed or not through these mechanisms" (Poullet, 2010, p. 25).

[58] Despite not supporting it through a right to identity justification, Roosendaal hints at the same solution. "The key issue is that individuals are affected, even when their names are not known. Because the decisions are applied to individuals, perhaps even without processing personal data in a strict sense, the DPD should apply" (Roosendaal, 2010, p. 234).

[59] In Opinion 4/2007, the Article 29 Data Protection Working Party (Art. 29 WP) advanced the following broad definition of personal data: "From the point of view of the nature of information, the concept of personal data includes any sort of statements about a person. It covers "objective" information, such as the presence of a certain substance in one's blood. It also includes "subjective" information, opinion or assessments" (Art.29 Data Protection WP, 2007, p. 6). Furthermore, Art. 29 WP stated explicitly that "[f]or information to be 'personal data', it is not necessary that it be true or proven" (Art.29 Data Protection WP, 2007, p. 6).

literature. According to such perspective, data protection seeks to achieve privacy protection by regulating the processing of personal data, which is then defined by recourse to the notion of (personal) identity. Privacy, in this line of reasoning, is then defined as the absence of constraints in constructing one's identity.

One of the main conclusions that can be extracted from this brief analysis is that privacy, identity and data protection are clearly undermined if understood as being simple, straightforward and harmonious. In this respect, data protection and privacy do not equate to one another. Data protection does not confine itself solely to the purposes of privacy and the value of privacy is far broader than the mere control of personal data.[60] As Poullet remarks, "[p]rivacy is an issue which goes well beyond data protection."[61] Furthermore, the conceptualization of privacy as the absence of obstacles in constructing identity conflates and blurs the concepts of privacy and identity, overstretching the former and understating the latter.

In order to grasp their underlying differences in scope, nature and rationale, I distinguished data protection, on one side, from privacy and identity, on the other, qualifying one as procedural and the others as substantive. In addition, I differentiated privacy and identity through an alethic criterion, allocating the protection of truthful information to the right to privacy and the not-necessarily truthful information to the right to identity. Such criterion was then tested through the analysis of profiling technologies. I thus examined the impact of automated decisions upon individuals made on the basis of non-distributive group profiles.

By acknowledging these crucial differences between data protection - privacy – identity, and by considering how individuals can be affected by decisions taken on the basis of such profiling practices, I then formulated two important conclusions: the data protection framework presents serious lacunae (1) and, therefore, needs to explicitly recognise the right to identity (2).

Regarding the lacunae, I stressed that the current data protection directive should also operate with the concept of identity and under a logic of representation, and not only with the notion of privacy and through an identification rationale. Consequently, in order to enlarge its *modus operandi*, it is absolutely vital that data protection directive recognizes identity not as a technical term which is part of the definition of personal data, but as a value and interest *per se*, that is, as an explicit and independent right. The recognition of identity as an interest and right is of utmost importance in order to attain and consolidate a complete and flawless protection of human individual autonomy and self determination.

Thereby, I argue that a clear and sound distinction between the rights to data protection, privacy and identity is absolutely crucial. And that is so not only for the sake of the coherence and operability of the legal system, but especially for the sake of attaining a comprehensive and solid protection of all the different aspects related to an individual's personality.

References

Agre, P., & Rotenberg, M. (1997). *Technology and privacy: the new landscape*. Cambridge, Mass. ; London: MIT Press.

Andrade, N. N. G. d. (2010). The Right to Privacy and the Right to Identity in the Age of Ubiquitous Computing: Friends or Foes? A Proposal towards a Legal Articulation In C. Akrivopoulou & A. Psygkas (Eds.), *Personal Data Privacy*

[60] For a criticism of the idea of privacy protection through control of personal data processing, see (McCullagh, 2009)

[61] (Poullet, 2010, p. 17). Poullet, in fact, presents the E-Privacy Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector), and its recent revision, as an example of how privacy can go beyond the parameters of data protection and favour the emergence of new principles that do not find a correspondence in the EU Directive 95/46/EC.

and Protection in a Surveillance Era: Technologies and Practices: Information Science Publishing - Forthcoming.

Archard, D. (2006). The Value of Privacy. In E. Claes, A. Duff & S. Gutwirth (Eds.), *Privacy and the Criminal Law* (pp. 13-31).

Art.29 Data Protection WP. (2007). Opinion 4/2007 on the concept of personal data (pp. 1-26).

Blume, P. (1998). The Citizens' Data Protection. *The Journal of Information, Law and Technology*(1).

Boussard, H. (2009). Individual Human Rights in Genetic Research: Blurring the Line between Collective and Individual Interests. In T. Murphy (Ed.), *New Technologies and human rights*. Oxford ; New York: Oxford University Press.

De Hert, P., & Gutwirth, S. (2003). *Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based servics and the virtual residence*: in Institute for Prospective Technological Studies - Joint Research Centre, Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-Technical Report Series, EUR 20823 EN. 2003. p. 111-162.

De Hert, P., & Gutwirth, S. (2006). Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In E. Claes, A. Duff & S. Gutwirth (Eds.), *Privacy and the Criminal Law* (pp. 61-104). Antwerp: Intersentia.

Hildebrandt, M. (2006). Privacy and Identity. In E. Claes, A. Duff & S. Gutwirth (Eds.), *Privacy and the criminal law* (pp. x, 199 p.). Antwerpen: Intersentia ; Oxford : Hart Pub. [distributor].

Hildebrandt, M. (2009). Profiling and AmI. In K. Rannenberg, D. Royer & A. Deuker (Eds.), *The future of identity in the information society : challenges and opportunities* (pp. 273-313). Berlin ; London: Springer.

Hildebrandt, M., & Gutwirth, S. (2008). *Profiling the European citizen : cross-disciplinary perspectives*. New York: Springer.

Leenes, R. E. (2008). Regulating Profiling in a Democratic Constitutional State. Reply: Addressing the Obscurity of Data Clouds. In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European Citizen: cross-disciplinary perspectives* (pp. 293-300). New York: Springer.

McCullagh, K. (2009). Protecting 'privacy' through control of 'personal' data processing: A flawed approach. *International Review of Law, Computers & Technology, 23*(1), 13-24.

Neethling, J. (2005). Personality rights: a comparative overview. *Comparative and International Law Journal of Southern Africa, 38*(2), 210-245.

Neethling, J., Potgieter, J. M., & Visser, P. J. (1996). *Neethling's law of personality*. Durban: Butterworths.

Pino, G. (2000). The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights. In M. Van Hoecke & F. Ost (Eds.), *The Harmonization of Private Law in Europe* (pp. 225-237). Oxford: Hart Publishing.

Poullet, Y. (2010). About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In S. Gutwirth, Y. Poullet & P. de Hert (Eds.), *Data Protection in a Profiled World* (pp. 3-30). Dordrecht: Springer Science+Business Media B.V.

Roosendaal, A. (2010). Digital Personae and Profiles as Representations of Individuals. In M. Bezzi, P. Duquenoy, S. Fisher-Hübner, M. Hansen & G. Zhang (Eds.), *Privacy and Identity Management for Life* (pp. 226-236). New York: Springer-Verlag.

Rouvroy, A. (2008). Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. *Studies in Ethics, Law, and Technology*, *2*(1), 51.

Sullivan, C. (2008). Privacy or Identity? *Int. J. Intellectual Property Management, Vol. 2*,(No. 3), pp.289-324.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220.