

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### The right to informational self-determination and the value of self-development

Rouvroy, Antoinette; Poulet, Yves

*Published in:*  
Reinventing Data Protection

*Publication date:*  
2009

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

#### [Link to publication](#)

*Citation for published version (HARVARD):*  
Rouvroy, A & Poulet, Y 2009, The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. in *Reinventing Data Protection: Proceedings of the International Conference (Brussels, 12-13 October 2007)*. Springer, Dordrecht, pp. 45-76.

#### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

## Chapter 2

# The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy

Antoinette Rouvroy and Yves Poullet

### 2.1 Introduction

In December of 1983, the German Federal Constitutional Court<sup>1</sup> declared unconstitutional certain provisions of the revised Census Act (Volkszählungsurteil) that had been adopted unanimously by the German Federal Parliament but were nevertheless challenged by diverse associations before the Constitutional Court. That now classical *avant-garde* decision ruled, based on Articles 1 (human dignity) and 2 (personality right) of the Constitution, that the

basic right warrants (...) the capacity of the individual to determine in principle the disclosure and use of his/her personal data.

This was one of the first and most famous articulation of a 'right to informational self-determination', understood by the Court as

the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others.

As we experience a new phase in the development of the information society with, in the technological domain, the advent ubiquitous computing and ambient intelligence and, in the socio-political sphere, the materialization of the shift from a 'control society' to a 'surveillance society'<sup>2</sup>, the purpose of the present paper,

---

A. Rouvroy (✉)

Research associate at the National Fund for Scientific Research (FNRS) and at the IT and Law Research Centre (CRID), University of Namur

<sup>1</sup> BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden.

<sup>2</sup> As Gilles Deleuze powerfully explained (Gilles Deleuze, 'Post-scriptum sur les sociétés de contrôle', *L'autre Journal*, n.1, 1990), the proper of modern norms – and that is what characterizes the gradual shift from the disciplinary society described by Michel Foucault and that presupposed the existence of a multiplicity of 'detention' facilities (psychiatric hospitals, factories, schools, prisons, ...) to the control society that can increasingly do without physical constraint and direct surveillance, is that it is individuals themselves who have to impose themselves not only to respect

twenty-four years after that German *avant-garde* decision, is to elucidate the conceptual relationships existing between the *rights* to privacy and data protection on the one hand, and on the other hand, the fundamental *values* those rights are assumed to protect and which were identified by the German Constitutional Court as human dignity and self-development.<sup>3</sup>

In the present contribution, we argue that privacy, as a legal right, should be conceived essentially as an *instrument* for fostering the specific yet changing *autonomic capabilities* of individuals that are, in a given society at a given time, necessary for sustaining a vivid democracy.<sup>4</sup> What those needed capabilities are is obviously contingent both on the characteristics of the constituency considered<sup>5</sup> and on the state of the technological, economic and social forces that must be weighed against each other through the operation of legislative balancing.<sup>6</sup> Capacity for both reflexive autonomy allowing to resist social pressures to conform with dominant views<sup>7</sup> and for deliberative abilities allowing participation in deliberative processes are arguably among the skills that a vivid democracy needs citizens to have in the circumstances of our times.

Those capabilities are threatened in unprecedented manners by the intensification of observation and monitoring technologies such as CCTV, data mining and profiling, RFID and the 'internet of things', ubiquitous computing and 'ambient intelligence'.<sup>8</sup> The news that Microsoft was filing a patent claim for a spyware

---

but also to adhere to the norms, who have to integrate those norms in their biography, through their own actions and reiterations. Power takes, in modern society, the form of offers of services or of inciting actions much more than of of constraints.

<sup>3</sup> The choice made by the German Constitutional Court to rely on these values instead of others may well be contingent to the German constitutional history and culture. The link established between self-determination and dignity does have normative consequences though, to the extent that the notion of dignity suggests incommensurability and inalienability.

<sup>4</sup> See in the same sense Cass R. Sunstein, *Why Societies Need Dissent*, Harvard University Press, 2003, pp. 157–158: 'The Right to privacy (...) can be illuminated if we see it as an effort to allow people to escape reputation pressures. Suppose, for example, that people are allowed to read whatever they like in the privacy of their own homes, or that actions which are forbidden in public, either by law or by norms, are legally protected if done in private. Or suppose that law creates safeguards against public observation of what is done in certain sanctuaries. If this is so, the privacy right will operate to reduce or to eliminate the pressure imposed by the actual or perceived views of others (...) privacy rights helps to insulate people from conformity.'

<sup>5</sup> Important elements of cultural and epochal incommensurability make the development of a universal theory of privacy most implausible.

<sup>6</sup> The German decision explicitly acknowledges that 'The general personality law (...) gains in importance if one bears in mind modern developments with attendant dangers to the human personality.'

<sup>7</sup> See Cass R. Sunstein, *Why Societies Need Dissent*, Harvard University Press, 2003: 'Well-functioning societies take steps to discourage conformity and to promote dissent. They do this partly to protect the rights of dissenters, but mostly to protect interests of their own.'

<sup>8</sup> For further reflections on how the Internet revolution and more recently the Ambient Intelligence technologies are metamorphosing the risks incurred by the individuals and their basic rights and call for new legislative actions reinforcing the different identified facets of the right to privacy, see Antoinette Rouvroy, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence', *Studies in Ethics, Law, and Technology* 2008, vol. 2, Issue 1. Available at: [http://works.bepress.com/antoinete\\_rouvroy/2](http://works.bepress.com/antoinete_rouvroy/2)

system linking employees to their computers with wireless sensors and enabling employers to monitor their employees' blood pressure, body temperature, heart rate and facial expression throughout the day, exemplifies the phenomenon: under constant, yet most of the time remote, surveillance and subjected to automatic or semi-automatic decisions taken by the 'system' on the basis of constant observation of their choices, behaviours and emotions, individuals may be said increasingly under the influence of those 'normative technologies' and, therefore, decreasingly capable of living by their fully autonomous choices and behaviours.

The German Court acknowledged that self-imposed restrictions on deviant behaviours, or on participation in assembly or civil society initiative by fear that these behaviours and participations be disclosed to others with adverse consequences ensuing

would not only impair his chances of development but would also impair the common good ("Gemeinwohl"), because self-determination is an elementary functional condition of a free democratic community based on citizens' capacity to act and cooperate.

The importance of privacy and data protection regimes today, it will be argued, derives from the support they provide for individuals to keep or develop those autonomic capacities to act and cooperate.

Our contribution will consist in four parts. In the first section, we wish to reassess the need for the type normative inquiry we are engaged in. In the second section, we wish to dispel some misleading interpretations that could be made of the trope 'informational self-determination'. Then, in the third section, the German Federal Constitutional Courts's decision will be commented, as to enlighten the present relevance of its rationales. A fourth section will allow us to clarify certain issues regarding the 'values' or 'basic rights' of dignity and self-determination or autonomy. Finally, we explore various 'facets' of the generic right to privacy and finding how those facets might be articulated around the principle of self-determination.

## 2.2 Why Re-Anchoring the Rights to Privacy and Data Protection in the Fundamental Ethical and Political Values?

Re-anchoring the rights to privacy and data protection in the fundamental ethical and political values from which they derive their normative force and that they are meant to advance has become crucial.

In the United States, the Supreme Court has repeatedly conditioned acknowledgement of the existence of a right of privacy in any given area of human life to the pre-existence of 'reasonable expectations of privacy' of those areas. Scholars have widely criticized the insufficiency of that non-normative assessment in technology-intensive societies. Nicole E. Jacoby, for example, comparing how judges in the US and in Germany identify when and in which circumstances an individual's right to privacy has been violated, showed that, in dealing with new technical surveillance measures the 'expectations of privacy' standard in use in the United States was much less protective of the individual confronted with surveillance than the



German Court's reliance on the principle, anchored in the value of human dignity, that individuals have an inviolable domain in which they may freely develop their personality.<sup>9</sup> Indeed, the obvious disadvantage of the volatile standard of 'expectations of privacy' is that expectations are not, as a matter of fact, independent of the level of surveillance and scrutiny in place. It means that in societies with intense surveillance systems, individuals indeed do not expect to have much privacy left. The scope of privacy, in such a conceptualization, may not extend much beyond the very narrow areas of life that surveillance technologies are not yet able to capture and is inherently dependent on the actual stage of technological development.

A theory of privacy relying on 'expectations of privacy' can not be justified either by saying that what privacy is about is the right individuals have not to be 'surprised' by surveillance devices did not expect to be there. Even where people know they are observed and thus have no expectation of privacy because they have been informed that surveillance devices are in use, surveillance, even overt and not hidden, may cause people harm that they would probably call invasions of their privacy. The most unsophisticated example of this would be an instance where video cameras would have been placed in public toilets. More subtle instances would be, for example, instances where employees would know they are being monitored by their employer and their productivity evaluated in real time. Although they do not have *expectations* of privacy in that case, they still have lost something that very much resembles 'their privacy'.

It is not useless to recall though that although 'expectations of privacy' do not play such an important role for the definition of the scope of privacy in Europe, the decrease of expectations of privacy will necessarily negatively impact on the probability that people will indeed claim respect of their right to privacy in those new areas where they are 'observed', or refuse their consent to being 'observed'. Preserving awareness about issues of privacy might happen to be both of paramount importance and enormously challenging the more we progress in the surveillance society.

Another method, more usual in Europe, for balancing competing interests and establishing whether or not, in each situation, there is a right to privacy or not, and whether or not legitimate and sufficiently compelling reasons exist for allowing interferences with that right, is normative inquiry required by Article 8§2 of the European Convention on Human Rights, among other texts:

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in 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.

<sup>9</sup> Nicole E. Jacoby, 'Redefining the Right to Be Let Alone. Privacy Rights and the Constitutionality of Technological Surveillance Measures in Germany and the United States', *Bepress Working Papers Series*, 2006, No. 1515.

One of the most paradigmatic examples of normative inquiry has been exhibited in the already mentioned German Constitutional Court's (Bundesverfassungsgerichtshof) decision of December 15, 1983<sup>10</sup>, about the constitutional limits to governmental collection of personal data for statistical purposes. The German Constitutional Court traced the foundations of a general 'right to informational self-determination' ('Informationelles selbstbestimmung') and thus of legal data protection regimes and, more broadly, of the right to privacy, to the fundamental right to the 'free development of one's personality'<sup>11</sup> protected by Article 2.1. of the German Constitution:

The value and dignity of the person based on free self-determination as a member of a free society is the focal point of the order established by the Basic Law. The general personality right as laid down in Arts 2 (1) i.c.w 1(1) GG serves to protect these values (...)

The German Constitutional Court's 1983 'census decision' might be an invaluable source of inspiration to address the unprecedented challenges of the advanced information society, where the combined socio-political and technological challenges of the time have made privacy (as well as expectations of privacy) and data protection claims appear relatively weak compared to the systematic normative privileging of transparency ensuing from the absolute logics of security and economic efficiency on the one hand<sup>12</sup> and, on the other hand, the development and dissemination of increasingly sophisticated and ubiquitous surveillance and tracking systems collecting and processing even the most trivial information about individuals.

It appears a reasonable assumption to have that in order to both re-situate the pervasive absolute logics in their relative frame and adapt our legal framework to the nature of the threats exactly are the values we consider threatened in the advanced information society presupposes one knows. Referring the right to privacy to the

<sup>10</sup> Constitutional Court, Dec. 15, 1983, *EuGRZ*, 1983, p. 171 and ff. On this decision, read E.H. Riedl, 'New bearings in German Data Protection', *Human Rights Law Journal*, 1984, Vol. 5, No. 1, pp. 67 and ff.; H. Burkert, 'Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences', *Dr. Inf.*, 1985, pp. 8 and ff. See also E. Brouwer (2007), *Digital Borders and Real Rights*, Nijmegen, Wolf Legal Pub, 501 p.

<sup>11</sup> Although the Court acknowledges that the scope and content of that 'personality right' had not been conclusively settled by case law, it nevertheless indicates that that right 'comprises the authority of the individual to decide for himself based on the idea of self-determination – when and within what limits facts about one's personal life shall be disclosed.' Yet, far from the interpretation of privacy as 'property' advanced by law and economics scholars, one understands from reading the decision through that this 'authority' of the individual is not an end in itself: it prevents situations where inhibition of the individual's 'freedom to plan or to decide freely and without being subject to any pressure/influence (i.e., self-determined). The right to self-determination in relation to information precludes a social order and a legal order enabling it, in which the citizens no longer can know who knows what, when, and on what occasion about them.'

<sup>12</sup> Where by individual transparency is systematically encouraged and reluctance to disclose personal information is often interpreted as meaning that the individual indeed has something (wrong) to hide. On the contrary, businesses are discouraged from being 'transparent' where the market negatively sanctions disclosure of trade secrets.

values in which it finds its roots provides contemporary scholars confronted with the unprecedented and unpredictable developments of information and communication technologies with solid objectives against which to assess the adequacy of current legislation and propose reasoned improvements.

We should note, however, that the recent enactment of Article 8 of the Charter of the European Union and the quasi-constitutional status thereby acknowledged to the right to data protection, instead of clarifying the issue, might, on certain points, further complicate the normative assessment. Indeed, the provision could well be interpreted as ascribing data protection a final, intrinsic value, thereby obscuring what seems to us an important aspect: the rather 'intermediate' or 'instrumental' value of data protection as a 'tool' for the preservation and promotion of more fundamental and basic values (namely the value of autonomic self-development and political participation). Moreover, among the disadvantages of granting a *final* rather than merely an *intermediate* value to the rights to data protection and privacy is the risk of increased rigidity and lack of plasticity of the relevant laws and their ensuing inability to meet the evolving challenges of the contemporary and future information society. In a sense, we wish to explain how privacy and data protection interact to form the immune system of the psychic space and, as any immune system, must evolve to fit the evolutions of the 'informational and societal ecosystem'.

The traditionally individualist conception of human rights may, moreover, inspire misleading interpretations of the recent constitutionalisation of the right to data protection. Especially in an era of possessive individualism such as ours, data protection – or the empowerment of individuals with regard to their personal data – risks being interpreted as making the satisfaction individuals' immediate preferences with regard to their personal data, their choices to keep undisclosed or to commodify personal information a *final value*. It is well-known that those preferences would lead a large part of the population to waive any protection of their personal data provided they receive immediate gratifications or commercial advantages. What would be lost in such an interpretation is the *intermediate value* of data protection as an instrument aimed at fostering the autonomic capabilities of individuals and therefore not something they may dispose of or trade on the market of personal information. Possessive individualism combined with the perception of personal information as a commodity freely exchangeable on the market risks, moreover, to result in a situation where disclosure by some of 'their' personal data unavoidably disadvantages those who would prefer not to disclose 'their' personal information.<sup>13</sup> Reassessing the normative grounds of privacy and data protection are thus, in this regard as well, necessary.

<sup>13</sup> When allowed (by law and/or technology) the transparency of *individuals* is usually rewarded on the short-term, whereas their opacity owes them sanctions. When *enterprises* are considered, the opposite is true: transparency puts them at commercial or industrial disadvantage whereas opacity is more profitable.

### 2.3 The Right to 'Informational Self-Determination': The Subject as Object?

Before turning to the reminder of the German decision which, as will be explained, is highly relevant to discuss the issues just mentioned, we would like to clarify an important conceptual point. The conception of privacy viewed as 'informational self-determination' (where data protection issues are – misleadingly – conceived as exhausting what is at stake when one speaks of privacy) is now often taken to be the fundamental justification ground for data protection regimes, not only in Germany but also in the rest of Europe. Yet, that concept of 'informational self-determination' is often misunderstood.

Our impression is that the right to informational self-determination should not be interpreted as suggesting that controlling and manipulating information and data about oneself is an exercise of 'self-determination'. Information and data are not the pre-existing 'elements' or 'building blocks' of an individual's personality or 'self'. Such a conception would be misleading and unduly reductionistic: the 'self' is not merely irreducible but also essentially different from 'data' and 'information' produced about it. What the expression 'informational self-determination' means is rather that an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said 'self-determined'. This is an important thing to recall today, as personal data (genetic and/or digital) have become *proxies* for persons with the intensification of governmental 'identity projects'. The recent debates in France about the 'offer' to make DNA testing available to immigration applicants to give evidence of family links with persons legally living in France epitomize a current western governmental tendency to make personal and even more so genetic, information a salient feature of individuals' identities and citizenships and to privilege profiles constructed about people in application of non-transparent algorithms over the applicants' biographical narratives.

Such a misunderstanding has had a very ambivalent impact for the protection of privacy. 'Informational self-determination', in a context of pervasive possessive individualism and at a time where private property and the laws of the market are perceived as the most efficient ways to allocate rights, the right to 'informational self-determination' has increasingly been understood as implying a sort of alienable property right of the individual over his personal data and information, perceived as his property (even in cases where personal information relates to that person's identity, the notion of 'identity theft' attests to the transformation of personal information into the status of 'thing' detached from the data subject). Yet 'information' does not pre-exist to its 'expression' or disclosure (information is always somewhat constructed) – no 'natural', ordinary rights could thus logically be held by an individual over information and data relating to him. These considerations have consequences with regard to the current debates about commodification vs. inalienability of personal information and individual privacy, as will be suggested later on.



The originality of the German Court's holdings in this regard is that, relating informational self-determination to the notion of dignity, it suggests a default regime of market inalienability of personal information. Still, one has to acknowledge that the position of the German Court contrasts with other often competing ways of defining and valuing informational self-determination. To say things caricaturally, the libertarian approach for example, would probably consider the right to data protection an alienable, commodifiable right, whereas egalitarian scholars would rather consider inalienability rules to be essential to protect individuals against discrimination and stigma, especially in the socio-economic sphere. For the purpose of the present contribution, we assume we are in a society placing human dignity and personal autonomy high in the hierarchy of fundamental values, as did the German Federal Constitutional Court of 1983.

#### 2.4 The German Federal Constitutional Court's 'Census' Decision of 1983

The German Court came to acknowledge the protection of personal data not as an end in itself or a final or primary value but 'merely' as a tool (though an essential one), making possible the *exercise* of the fundamental and basic individual 'right' to self-development, while being itself distinct from autonomy, self-determination or self-development (depending how one calls the primary values sustaining privacy). The clarification of this 'intermediate' value of privacy is important if only because it avoids the common conflation of the legal concept of privacy with the broad philosophical, political and psychological concepts of autonomy, self-determination or self-development<sup>14</sup> and the ensuing difficulty to figure out how, exactly, the law should intervene to protect those impalpable values. Most interesting to us, in this German decision, is the argumentation of the Court. Those rationales, we wish to show, may be immensely useful to help clarifying conceptual intricacies characterising privacy and data protection in view of the emerging challenges raised by the exponential development of information and communication technologies on the threshold of an 'ambient intelligence era'.

The following excerpt of the decision deserves quotation. Its wording might be considered not only to describe the situation existing in 1983 but to anticipate the more recent developments of the technologies, as we will show later:

This authority (the possibility of the individual to decide for himself) particularly needs protection under present and future conditions of autonomic data processing. It is particularly endangered because in reaching decisions one no longer has to rely on manually collected registries and files, but today the technical means of storing individual statements about personal or factual situations of a certain or verifiable people with the aid

<sup>14</sup> The popular theories of privacy as the 'right to be let alone' (Westin and Brandeis), or, as the 'right of the individual . . . to be free from unwarranted government intrusion' (according to the Judge Brennan's conception in *Eisenstadt v. Baird* (1972)) lead to confusions between privacy and liberty.

of automatic processing are practically unlimited and can be retrieved in a matter of seconds irrespective of distance. Furthermore, they can be pieced together with other data collection – particularly when integrated information systems are built up – to add up to a partial or virtually complete personality profile, the persons controlled having no sufficient means of controlling its truth and application. The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behaviour. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would also impact the common good ("*Gemeinwohl*"), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate.

##### 2.4.1 Data Protection Laws Grounded Directly on Fundamental Constitutional Rights

First, there is the acknowledgement that privacy, or data protection, has an 'intermediate' rather than a 'final' value: they are 'tools' through which more fundamental values, or more 'basic' rights – namely human dignity and individual personality right – are pursued. Earlier in the decision, the German Court held that:

The standard to be applied is the general right to the free development of one's personality. The value and dignity of the person based on free self-determination as a member of the society is the focal point of the order established by the Basic Law (*Grundgesetz*). The general personality right as laid down in Article 2 (1) and Article 1 (2) GG serves to protect these values – apart from other more specific guarantees of freedom – and gains in importance if one bears in mind modern developments with attendant dangers to the Human personality.

By this assertion, the Court establishes a clear and direct link between the Data Protection regime and two basic values enshrined in the Constitution, interpreting legal data protection regimes as mere *implementations* of those fundamental constitutional rights. The first of those fundamental constitutional rights is the right to respect and protection of one's 'dignity' guaranteed by Article 1 of the Constitution<sup>15</sup> and the second one is the right to 'self-development', enacted by Article 2

<sup>15</sup> Article 1 GG: '*The dignity of man shall be inviolable. To respect and protect it shall be the duty of all states and authorities*'.

of the Constitution.<sup>16</sup> The fact that the Court will refer directly to these principles without mentioning the already existing Data Protection Law is noticeable. In its view, the major data protection principles derive *directly* from these two Constitutional provisions that consecrate the value of autonomy (self-determination) and the incommensurability (dignity) of each person in the society. To be more precise, the Data Protection regime is a tool for ensuring those fundamental values and must be interpreted *in light of those values*, a consideration that would logically have important consequences not only, as already mentioned, in the debates relating to the (in)alienability the rights to privacy and data protection but also for the legislative balancing (proportionality test) in the implementation of data protection principles. Additionally, the Court suggests that these two provisions are not on the same level as the other constitutional provisions guaranteeing more specific freedoms like freedom of association, religion, and expression, all presupposing previous acknowledgement and respect of dignity and of the right to self-development.

#### 2.4.2 Fundamental Values Protected by Evolving Laws in a Contingent World

Second, there is the acknowledgement that technological evolution may require legal protections of privacy to evolve, simply because those technological evolutions threaten, in new ways, the fundamental value of personal autonomy: according to the court, the emergence of legal data protections attests and responds to such a need for legal evolution. Self-determination, according to the Court, 'is endangered primarily by the fact that, contrary to former practice, there is no necessity for reaching back to manually compiled cardboard-files and documents, since data concerning the personal or material relations of a specific individual {personal data [cf. Federal Data Protection Act Article 2 Para. 1]} can be stored without any technical restraint with thanks to automatic data processing and can be retrieved any time within seconds, regardless of the distance. Furthermore, in case of information systems integrated with other databases, data can be integrated into a partial or complete picture of an individual, without the informed consent of the subject concerned, regarding the correctness and use of data.' What 'self-determination' presupposes and what it allows in a given society is unavoidably contingent on many evolving factors. Besides the state of technological development – suggested by L. Lessig as the central, if not exclusive, reason to adapt our normative instruments – taking the nature of prevailing institutional arrangements and socio-political structures into

<sup>16</sup> Article 2 GG: 'Everybody shall have the right to the free development of his personality insofar he does not violate the rights of others or offend against the constitutional order or the moral order.'

account is critical in explaining the chronological development of the various and interdependent facets of the right to privacy.

It also means that the laws guaranteeing privacy and enforcing data protection must evolve as to fit the technological and socio-political evolutions generating new threats for the individuals' capacity for 'self-development' of their personality. According to the Constitutional Court's opinion the development of the data processing technologies obliged the State to revise and adapt the guarantees it provides to individuals in order to protect and foster the capabilities needed to implement their right to freely self-determine their personality. In the circumstances of the day, the legal protections offered to the individuals' capabilities for self-development would probably need to address the specific threats accompanying the development of ubiquitous computing and ambient intelligence, as will be further explored in Section 3.

The 'evolutionist' approach of law attested by the Constitutional Court ought to be underlined. In such a perspective, the importance of protecting the individual aptitude to self-determination is not only grounded on the interests of the concerned individuals but also and fundamentally so, in the collective or societal interest in preserving a free and democratic society: individual autonomy and deliberative democracy presuppose a series of rights and liberties allowing individuals to live a life characterized as (partly at least) self-determined, self-authored or self-created, following plans and ideals – a conception of the good – that they have chosen for themselves.<sup>17</sup> In that sense, the right to privacy is not something citizens are entitled to barter. Privacy is rather a social structural imperative in a democracy, since a precondition to democratic deliberation is that individuals feel free and are free to express themselves without fear of being judged out of context or by public and/or private bureaucracies interpreting their expressed thoughts and behaviours from a distance, on the basis of information collected and processed by them. Maintaining and fostering private *and public* expression of individuals' thoughts, preferences, opinions and behaviours is among the obligations of the State in democratic societies.<sup>18</sup> The German Constitutional Court therefore explicitly acknowledged that

<sup>17</sup> See Onora O'Neill, *Autonomy and Trust in Bioethics (Gifford Lectures, 2001)*, Cambridge University Press, 2002, recalling the wide variety of notions that have been associated to the concept of autonomy by scholars such as Gerald DWORKIN, *The Theory and Practice of Autonomy*, Cambridge University Press, 1988, listing liberty (positive or negative), dignity, integrity, individuality, independence, responsibility and self-knowledge, self-assertion, critical reflection, freedom from obligation, absence of external causation and knowledge of one's own interest as concepts that have been equated to the concept of autonomy, or as Ruth Faiden and Thomas Beauchamps, *A History and Theory of Informed Consent*, Oxford University Press, 1986, according to whom autonomy may also be defined as privacy, voluntariness, self-mastery, choosing freely, choosing one's own moral position and accepting responsibility for one's choices.

<sup>18</sup> 'From it follows that it is a prerequisite of free development of the personality under modern conditions of data processing; the individual needs protection against unlimited collection, storage and transmission of his personal data.'



it is a prerequisite of free development of the personality under modern conditions of data processing; the individual needs protection against unlimited collection, storage and transmission of his personal data.

The basic right to informational self-determination (based on the fundamental principles of dignity and self-development) provides individuals the power to decide themselves about issues of collection, disclosure and use of their personal data.

The right to informational self-determination is not absolute though, as the Court explicitly acknowledges that

The individual does not possess a right in a sense of an absolute, unlimitable mastery of "his" data; rather he is a personality dependant on communication developing within the social community. Information, even if personality based, is a reflection of social reality and cannot be associated purely with the individual concerned. The Basic Law has decided the tension between the individual and society in favour of the individual being community related and community bound.

As already mentioned above, due to this conception of the individual who needs interactions with others, the (individual, private businesses, governmental) stakeholders' respective interests must be balanced against each other.<sup>19</sup> Therefore, the Court recalls the importance of the 'proportionality principle' as a constitutional principle that 'follows from the essence of basic rights, as an expression of the citizens' claim to freedom (. . .). Considering the dangers of utilizing automatic data processing outlined above, the legislator more than previously is under the duty to institute organisational and procedural safeguards which counteract the dangers of infringements of the personality rights.'

Interferences with the right to informational self-determination are allowed only when 'predominant public (or private) interests' outweigh the individual interest founding the right to self-development and that no alternative solutions less intrusive might be found to achieve these interests. Clarity and transparency of legal rules and principles ('Normenklarheit') following the more general principle of the rule of law ('Rechtsstaat') must also be respected according to the Court decision.

<sup>19</sup> According to P.De Hert and S.Gutwirth ('Privacy, Data Protection and law enforcement. Opacity of the individuals and transparency of the power', in *Privacy and the Criminal Law*, E. Claes et alii (ed.), Interscientia, Antwerpen-Oxford, 2006, p.74): 'Never does an individual have an absolute control over an aspect of his or her privacy. If individuals do have freedom to organise life as they please, this will only remain self-evident up to the point that it causes social or inter-subjective friction. At that stage, the rights, freedoms and interests of others, as well as the prerogatives of the authorities come into play. The friction, tension areas and conflicts create the need for a careful balancing of the rights and interests that give privacy its meaning and relevance. This shows clearly that, although quintessential for a democratic constitutional state, because it refers to liberty, privacy is a relational, contextual and per se social notion which only requires substance when it clashes with other private or public interests.'

### 2.4.3 Privacy as a Social-Structural Tool for Preserving a Free and Democratic Society: The Co-Originality of Private and Public Autonomy

Third, there is the acknowledgement that privacy and data protection are social-structural tools for preserving a free and democratic society. The right to self-development attaches to the members of a free society. In other words, privacy and data protection regimes are not there merely to protect the best right holders interests of the (and, indeed, as has been widely discussed in debates about the commodification of personal information, those best interests many sometimes be better promoted by disclosing personal information than by maintaining 'secrecy') but are necessary, in a democratic society, to sustain a vivid democracy. There, the German decision is crystal clear in its consideration that 'if one cannot with sufficient surety be aware of who knows what about them. Those who are unsure if differing attitudes and actions are ubiquitously noted and permanently stored, processed or distributed will try not to stand out with their behaviour. Those who count with the possibility that their presence at a meeting or participation in a civil initiation be registered by the authority, will be incited to abandon practising their basic rights (Basic Law, Article 8 §. 9).'

As a matter of fact, the 1983 German Constitutional Court decision considers individual autonomy not as a radical seclusion and independence of the person vis-à-vis his social environment but as the autonomy of a person radically inserted in society and living and communicating with others. On that point, the decision reiterates the point of view already expressed in 1954<sup>20</sup> by the same Supreme Court:

L'image de l'Homme qui sous-tend la Loi fondamentale n'est pas celle d'un individu solitaire et souverain. Dans la tension existant entre l'individu et la collectivité, la Loi fondamentale a au contraire voulu privilégier les liens de relation et solidarité entre la personne et la Communauté.<sup>21</sup>

The liberty protected by the Constitution is in no way comparable with 'Robinson Crusoe's liberty, German scholars acknowledged.<sup>22</sup> The right to self-development is not conceived as a liberty held in isolation by an individual living secluded from the rest of society but, on the contrary, as a right enjoyed as member of a free society. The Constitutional Court refers to the Kantian concept of freedom that presupposes individuals to have the possibility to develop their personalities through interactions and conversations they have with others and which, thus, is circumscribed by the

<sup>20</sup> BVerfG July 20, 1954, *BVerfGE*, 4, 7, 15-16.

<sup>21</sup> Translation suggested by M.T. Meulders-klein, 'L'irrésistible ascension de la 'vie privée' au sein des droits de l'homme', in F. Sudre (ed.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Collection Droit et Justice 63, Bruxelles, Nemesis, Bruylant, 2005.

<sup>22</sup> Besides the authors already mentioned, one may also refer to Mainz, Dürig, Herzog, *Grundgesetz Kommentar*, München, C.H.Beck, under Article 2.



legitimate demands of society.<sup>23</sup> This justifies the fact that, because individuals need interactions and cooperation with others and with the State in order to self-develop, data protection organises a system of *disclosure* of personal data respectful of the individual's right to self-determination, as both opacity and transparency therefore contribute to sustaining the individual's self-development.

Self-determination, it may even be argued, is not an independent value but a tool for guaranteeing the democratic functioning of society.

Human rights and liberties not only restrict the power of the State but also empower citizens to participate in the political system. These rights and liberties enable citizens to develop and exercise their moral powers informing, revising and in rationally pursuing their conceptions of the good.<sup>24</sup>

Inspiration for thinking about the mutual reinforcement of private and public autonomy (the idea that they are 'co-originated') can be found in Habermas's discourse theory of law according to which 'Just those action norms are valid to which all possibly affected persons could agree as participants in rational discourses'. In such a perspective, the right to self-development constitutes a precondition to real democratic discussion. This idea of the 'co-originality' of private and public autonomy also transpires, implicitly, in most defences of privacy based on its structural value for society by authors like Schwartz and Treanor, Flemming and others.<sup>25</sup>

## 2.5 'Dignity' and 'Autonomy': A Few Words of Conceptual Clarification

The Karlsruhe judges anchored their approach of the right to privacy in two distinct constitutional provisions reflecting the primacy, in the German constitutional order, of two fundamental values: human dignity on the one hand and individual

<sup>23</sup> Let us note here that theoretically, on Kantian grounds, on the condition that the State is legitimate, there are no reasons to think of the individual's and the State's interests as conflicting with each other (see the Kantian ideal of universalisable reason according to which an autonomous individual cannot reasonably wish something that is not, at the same time, something that all his community, thus the State, would wish. In this regard, Rawls's conception that the State's unique justification is the guarantee of the maximum liberty for each individual is somewhat radically alien to Kant's lessons, as taken over by Habermas among others).

<sup>24</sup> P. De Hert and S. Gutwirth already quoted, p. 64. These authors are referring to Rawls', Dworkin's and Habermas's conceptions of Human Rights.

<sup>25</sup> Jürgen Habermas, *Between Facts and Norms*, MIT Press, 1996; P.M. Schwartz, and W.M. Treanor, 'The New Privacy', *Michigan Law Review*, 101, 2003, p.216; James E. Flemming, 'Securing Deliberative Autonomy', *Stanford Law Review*, Vol. 48, No. 1, 1995, pp. 1–71, arguing that the bedrock structure of deliberative autonomy secures basic liberties that are significant preconditions for persons' ability to deliberate about and make certain fundamental decisions affecting their destiny, identity, or way of life. On deliberative democracy, see James E. Flemming, 'Securing Deliberative Democracy', *Fordham Law Review*, Vol. 72, p. 1435, 2004. On the concept of co-originality, see Rainer Nickel, 'Jürgen Habermas' concept of co-originality in times of globalisation and the militant security state', IUE Working Paper Law, 2006/27.

self-development in a free society on the other hand. The combination of those values inspired the Court's acknowledgement that a 'generic right to personhood' ('An Allgemeines Persönlichkeitsrecht'), existed as the hardest core of the legal constitutional order of the German Republic. That right, transposed in the technological context of 1983, was to be understood as a right to informational self-determination that justified the adoption of the Data Protection Act. Reference to its constitutional inspiration guides the interpretation to be given of that Data Protection Act.

Reference to the value of human dignity places the legal regime of data protection in a human-centred perspective and in a vision of society requiring technological developments to be developed at the service of the development of human personality, which is, 'the attributes of an individual which are irreducible in his selfhood.'<sup>26</sup> According to the German Constitutional Court, 'the right to privacy protects the individual's interest in becoming, being and remaining a person.'<sup>27</sup> Dignity, unlike autonomy, is unconditionally 'attached' to each human being. A person who, as a matter of fact, is not 'autonomous' has, nevertheless, 'dignity'. In a Kantian sense, human dignity is a condition of human beings that they are acknowledged because of their theoretical or generic capacity to exhibit autonomy, without regard to whether they actually develop that capacity for autonomy or not.

Privacy is thus a legal concept, or an 'intermediate value' for the fostering of the socio-political ideals (or 'final values') of liberty, autonomy and self-determination. Autonomy and self-determination (exhibited for example when individuals hold ideas or have lifestyles that might be politically and socially unpopular) cannot be characterized as legal 'rights', 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.<sup>28</sup> Like happiness, autonomy or self-determination, is a matter of degree. The conditions for individual autonomy are so diverse, so subjective in a sense, that no law could really ensure the genuine effectuation of a 'right to autonomy'.<sup>29</sup>

They are capabilities that not all individuals wish and/or have the aptitude to develop. Individual autonomy, not more than musical talent, artistic gifts of happiness, is something that the State, through the law, could never 'provide' to

<sup>26</sup> P. Freund, quoted by D. Solove, 'Conceptualizing Privacy', 90 *Cal. Law Rev.*, 2002, 1090.

<sup>27</sup> J.H. Reiman, 'Privacy, Intimacy, and personhood', in *Philosophical dimensions of Privacy*, F.D. Schoeman (ed.), p. 314. See also, J. Rubinfeld, 'The Right of Privacy', 102 *Harv. Law Rev.*, 1989, pp. 737–807.

<sup>28</sup> Sustaining that mere immunity from intrusion or interference from state or from others with my 'personal' affairs makes me an autonomous person amounts to confusion between the concepts of autonomy and of *negative liberty*. To give a paradigmatic example: a left alone child under the age of five is indeed enjoying the *negative liberty* that non interference in one's private affairs provides but he is certainly not enjoying *autonomy* and may moreover be assumed to be deprived from *real liberty*, subjected as he will probably be to hunger and all other threats that children left alone endure.

<sup>29</sup> Considering the 'right to autonomy' as a fundamental human right would require justification for any restriction on that 'right' imposed by the parents to their child.

individuals. A 'right to be autonomous' would not make more sense for the law than a 'right to be happy'. What does exist is a right to the pursuit of happiness (e.g., the American Declaration of Independence of 1776 proclamation: 'We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness') and, arguably, a right to the pursuit of autonomy.

However, despite the law's inability to 'create' or 'guarantee' individual autonomy, showing *respect* for individual autonomy<sup>30</sup> and, as far as possible, providing some of the conditions necessary for individuals to develop their capacity for individual deliberative autonomy (the individual process of self-governance) and for collective deliberative democracy (the group-oriented process for critical discourse indispensable to a vivid democracy) have become the most fundamental and basic ethical and legal imperatives in contemporary western societies, where respecting those imperatives is perceived as a precondition to the legality and legitimacy of the law. Individual autonomy and deliberative democracy presuppose a series of rights and liberties allowing individuals to spend a life characterized as (in part at least) self-determined, self-authored or self-created, following plans and ideals – a conception of the good – that they have chosen for themselves.

An important lesson derived from the German Constitutional Court's approach, is, as previously said, the fact that privacy is not considered merely as an individualistic value. As P. Regan<sup>31</sup> expressed it, 'Privacy has value beyond its usefulness in helping the individual to maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize the individual is better off if privacy exists. I maintain that the society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public and collective purposes.'

<sup>30</sup> Respect for individual autonomy of persons and thus for the choices they make, is contingent, in law, to the consideration that the subject is *indeed* autonomous in the choices he makes. That condition of autonomy implies the absence of either physical, mental or economic coercion. Legal interference with lawful, fully conscious and unforced choices of capable individuals is considered unacceptable, even if interference arises for the sake of the subject's own good, in which case one speaks of unacceptable legal paternalism.

<sup>31</sup> P. M. Regan, *Legislating Privacy, Technology, Social Values and Public Policy*, New York, 1995, pp. 321. See also D. Solove 'The Digital person, Technology and privacy in an Information Age', New York University Press, 2004, pp. 57 and ff. and Schwartz, 'Beyond Code for Internet Privacy: Cyberspace Filters, Privacy control, and Fair Information Practice', *Wisconsin Law Rev.*, 2000, p.787.): 'In place of Lessig's idea that privacy protects a right of individual control, this Article has developed a concept of constitutive privacy. Information Privacy is a constitutive value that safeguards participation and association in a free society. Rather than simply seeking to allow more and more individual control of personal data, we should view the normative function of information privacy as inhering in its relation to participatory democracy and individual self determination. Information Privacy rules should carry out a constitutive function by normally defining multi-dimensional information territories that insulate personal data from the observation of different parties.'

As expressed by Burkert<sup>32</sup>, privacy may be considered a '*fundamentally fundamental right*'. Privacy is not a freedom on the same rank than the others: essential to human dignity and individual autonomy and translating these moral principles in the legal sphere, privacy is a necessary precondition to the enjoyment of most other fundamental rights and freedoms.

However, one may but acknowledge the quintessential indeterminacy of privacy. Awkward as it may appear, this indeterminacy is unavoidable, as what one understands as being in the scope of privacy is 'fundamentally' contingent on the societal context in which our autonomic capabilities as individuals have to be protected. In that sense, one may only agree with Burkert's view that privacy is also a 'fundamentally relative right.'<sup>33</sup> What is meant by privacy and how it is protected must evolve to face the changing threats to human dignity and individual autonomy and must be found taking fully into account the context in which our liberties have to express themselves, as Solove argued.<sup>34</sup> The enactment of data protection legislations should be seen in that light as an attempt, certainly not the last one, to face the unprecedented challenges of the already elapsed time when those data protection regimes were set.

## 2.6 The 'Facets' of Privacy and How They Can Be Articulated to Protect and Promote Autonomous Self-Development

Exploring what 'self-development' would mean in a society such as ours and identifying the legal instruments susceptible to contribute to the protection of such a capability in the circumstances of our times, will amount to analyse the different aspects or conceptions of the generic right to 'privacy', in the chronological order of their surfacing in jurisprudence and scholarship.

Privacy has first been conceptualized as 'seclusion' (opacity, or privacy as solitude)<sup>35</sup>, before being understood as also encompassing a dimension of

<sup>32</sup> H. Burkert, 'Dualities of Privacy – An Introduction to 'Personal Data Protection and Fundamental Rights'', in *Privacy- New visions*, M.V. Perez, A. Palazzi, Y. Pouillet (eds.), Cahier du Crid, to be published in 2008.

<sup>33</sup> 'This is not an attempt to reconstruct a ranking of fundamental rights, an exercise that would only undermine the legitimacy of all fundamental rights including those, which might end up on a 'higher' rank. The term 'fundamentally fundamental' is only meant as a pointer to the functional importance of 'privacy' as a fundamental right. This importance, however, seems to clash with what we have already observed before when speculating on this fundamentalism and what I would call here the factual unimportance of 'privacy' due to its relativity: 'Privacy' is being regarded as a 'relatively fundamental' right which has to – it seems – reconstitute itself anew in a balancing of interests in each and every new informational conflict.'

<sup>34</sup> D.J. Solove, 'Conceptualizing Privacy', 90 *California Law Review*, 2002, 1085 et s. ; P.Blok, *Het recht op privacy*, Boom Juridische uitgevers, 2003.

<sup>35</sup> See Ruth Gavison, 'Privacy and the Limits of the Law', 89 *Yale Law Journal*, 1980, pp. 421–471. See also Judith W. Decew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, Cornell University Press, 1997.



'non-interference' (decisional privacy, or privacy as liberty)<sup>36</sup> and, finally, of individual informational control or empowerment ('the ability of an individual to control the terms under which their personal information is acquired and used'<sup>37</sup>, formalised through fair information practices).<sup>38</sup>

Those 'facets' of privacy have emerged from competing theoretical constructions that have long struggled against each other to gain the monopoly in defining what privacy is about. Our aim here will be to attempt reconciling those 'visions' or 'theories' of privacy, insisting on their common roots and their complementarity. Of particular interest to us will be the question how the 'data protection branch' of privacy would benefit from reassessing its connectedness with the other traditional branch of privacy sometimes simply defined as 'the right to be let alone' but implying both a notion of seclusion and a notion of decisional autonomy, as attested by the evolution in this regard of both the Strasbourg Human Rights jurisprudence giving effect to Article 8 of the European Convention of Human Rights and the US Supreme Court decisions relating to privacy.

### 2.6.1 The Right to Privacy as 'Seclusion', 'Opacity' or 'Solitude'

The scholarly genesis of the right to 'informational privacy' may be traced back to Warren and Brandeis' classical 1890 Harvard Law Review article of 1890. Already then, privacy was presented as an adaptation of, or as an adjunction to, pre-existing legal rights, that technological and social evolution had rendered necessary: 'Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.' And already then, it was acknowledged that '[T]he principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality' that Warren and Brandeis equated with the 'right to be left alone' when writing that '(...) the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone'. That 'principle' was conceived to protect 'the privacy of the individual from invasion

<sup>36</sup> See *Griswold v. Connecticut*, 281 US 479 (1965), a case taken to be the first judicial acknowledgement of the right of privacy by the US Supreme Court, in which it invalidated a law forbidding married people from using contraceptives.

<sup>37</sup> M.J. Culnan, 'Protecting Privacy online: Is self-regulation working?', 19 *Journal of Public Policy Market*, 2000, 1, pp. 20 and ff.

<sup>38</sup> See for instance Charles Fried, 'Privacy: A Rational Context.', in M. David Ermann, Mary B. Williams and Claudio Guitierrez, *Computers, Ethics, and Society*, Oxford University Press, 1990; Arthur Miller, *The Assault on Privacy*, Harvard University Press, 1971.

either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds.'<sup>39</sup>

In Europe, the right to privacy is explicitly acknowledged by Article 8 of the European Convention of Human Rights. The initial interpretation of that right resembled the American 'right to be left alone', in the intimacy of one's private and family life, home and correspondence, but – and this is quite paradoxical in view of the subsequent evolutions in this regard – contrary to the American doctrine of privacy, the European right was not primarily directed against interferences by other individuals (journalists) but against intrusions by the State in the sanctity of home and of correspondence. The early version of the right to privacy was, in the context of traditional society, not merely seen as ensuing from the principle of human dignity but also as a precondition to the free development of personality. It means that each individual must have a physical place where to express him or herself and the possibility to exchange views or to reveal his intimate convictions to others through private communications means without being observed from outside or by third parties.<sup>40</sup>

As a matter of fact, total transparency would impair the possibility for individuals to freely develop their personality. They need some 'secrecy, anonymity and solitude', 'withdrawal and concealment'<sup>41</sup> in order to reflect on their own preferences and attitudes, or, in other words, to reflexively make and revise choices in life, as well as to develop meaningful relationships with others. Friendship and love do not easily develop in a crowd; they necessitate selective retreat and seclusion. Even in the traditional villages, the role played by the walls of the private home included the protection of a sphere of intimacy where individuals felt allowed to give up, for the time of the private encounter, the role he or she endorses in public. In that sense, the 'right to opacity' is a precondition to the very existence of the 'authenticity' of the self and to the implementation of the ability we have, as human beings, to develop our personal identity. Our 'inviolable personality' may only grow in the shadow of partial opacity.<sup>42</sup> The 'right to opacity' protects the individual from others watching, scrutinizing or spying on his or her private realm. It protects against public and

<sup>39</sup> S. Warren and L. Brandeis, 'The Right to Privacy', *Harvard Law Review*, 4(5), 1890. See also D. Solove, 'Conceptualizing Privacy', 90 *California Law Rev.*, 2001, pp. 1041–1043.

<sup>40</sup> About the history of the privacy concept, read notably D.J. Solove, 'Conceptualizing Privacy', 90 *California Law Review*, 2002, 1085 et s.; P.BLOK, *Het recht op privacy*. Boom Juridische uitgevers, 2003.

<sup>41</sup> R.Gavison, 'Privacy and the limits of Law', 89 *Yale Law Journal*, 1980, pp. 433 and ff.

<sup>42</sup> See on that issue, the reflections proposed by J. Rayman ('Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway of the Future', 11 *Santa Clara Computer & Techn. Law Journal*, 1995, pp. 22 and ff.), J. Cohen ('Examined Lives: Informational Privacy and the Subject as Object', 52 *Stanford Law Rev.*, 2000, pp. 1373 and ff.) and H.Nissenbaum ('Privacy as contextual Integrity', 79 *George Washington Law Rev.*, 2004, pp. 150 and ff.), who asserts that 'the freedom from scrutiny and zones of 'relative insularity' are necessary conditions for formulating goals, values, conceptions of self and principles of action because they provide venues in which people are free to experiment, act and decide without giving account to others or being fearful of retribution'.



private global surveillance. As will be suggested later on, this 'right to seclusion' might well be even more vital today in our modern society than ever before, justifying the new legal tools put into place in order to protect 'opacity' against the new technological and socio-political challenges of the day. What characterizes the present Internet world is precisely the unprecedented possibility that surveillance be exercised over each of us through the multiple traces we leave in cyberspace and through the gradual invasion of our private sphere by terminals of multiple and ubiquitous nature (from personal computers, GPS, mobile phones, RFID, etc.), dissolving the traditional separation between public and private spaces.

Privacy as 'seclusion' or as the 'right to be left alone' suggested a geographical scope of application: the 'private sphere' to which the right to privacy applied was bordered by the house's walls or by the private letter's material envelope. As such, the right to privacy as 'seclusion' has attracted much criticism from feminist scholars like Catherine MacKinnon who demonstrated that because privacy prevented the State to interfere in the protected area of family life, it allowed domestic violence to occur and left its victims helpless.<sup>43</sup> The feminist critique of privacy makes it clear that the right to privacy, originally, was not a protection for the individual subject as much as a protection of the familial structure, understood as the basic institution in society.

### 2.6.2 Privacy as 'Decisional Autonomy'

In *Griswold v. Connecticut*<sup>44</sup>, a case usually taken to be the starting point of the jurisprudential trajectory of the American constitutional right to privacy as 'decisional autonomy', the Supreme Court voided a State criminal law prohibiting the use or distribution of any contraception drug or instrument to married persons on the ground that a protection from State intrusion into marital privacy was a constitutional right, one that was a 'penumbra' emanating from the specific guarantees of the constitution. The nature and scope of this 'penumbral' right to privacy remained uncertain though. Judge Douglas, who spoke for the Court, appeared concerned not only by the intrusion by the police into the private marital bedroom necessary to investigate breaches of the prohibition but also by the special relationship that constitutes marriage and which should not be intruded or controlled by the State. As a result from this dual justification, conservative interpreters of *Griswold* perceive the decision as protective of the institution of marriage, while other commentators consider that concerns with policy access to the marital bedroom are peripheral to the Court's central concern to provide autonomy with respect to intimate decisions. These alternative rationales make it unclear whether the Court's intention was to protect the institution of marriage per se or whether it intended to protect marriage

<sup>43</sup> C. MacKinnon, *Towards a Feminist Theory of the State*, Cambridge: Harvard University Press, 1989.

<sup>44</sup> *Griswold v. Connecticut*, 381 US 479, 493 (1965).

not for its own sake but because this special relationship provides individuals with a context that fosters autonomous choices on fundamental and existential issues of life such as the choice whether to conceive a child or not. Despite the uncertainties of interpretations, this 'penumbral' right of privacy has been one of the main foundations of the later Supreme Court decision in *Roe v. Wade*<sup>45</sup> to overturn State abortion statutes. From there on, privacy acquired its truly individual character as a right protecting freedom of choice in intimate issues such as the decision, for a woman, whether to bear or beget a child. 'Decisional privacy', encompasses 'the rights of individuals to make certain kinds of fundamental choices with respect to their personal and reproductive autonomy'.<sup>46</sup> In *Planned Parenthood v. Casey*<sup>47</sup>, the Supreme Court expressed the consideration that

At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State.<sup>48</sup>

Notwithstanding the different legal strategies to cope with it, autonomy as self-determination or as autonomous construction of one's personality is, in US<sup>49</sup> like in Europe, the crucial value behind privacy.

In Europe, the explicit acknowledgement of privacy in the European Convention on Human Rights made its individualistic orientation indisputable from the start. Moreover, from an initially 'negative' undertone suggesting that the right to privacy merely implied the obligation for the State to abstain from interfering in the private matters of the individuals, the European Court of Human Rights soon interpreted the obligations held by the State quite extensively. Although, according to Konvitz, the essence of privacy is merely 'the claim that there is a sphere of space that has not been dedicated to public use of control'<sup>50</sup>, the notions of 'private and family life' has been interpreted extensively by the ECHR, to the effect that the right to privacy protects individuals against invasions of privacy by public authorities or, through the Convention's *horizontal effect*, by other individuals.<sup>51</sup> According to the

<sup>45</sup> *Roe v. Wade*, 410 US 113 (1973).

<sup>46</sup> N.M. Richards, 'The Information Privacy Law Project', *Georgetown Law Journal*, 2006, p.

<sup>47</sup> 505 US 833 (1992).

<sup>48</sup> On the American conception of Privacy and its link with the 'Autonomy' concept, read A.J. Rappaport, 'Beyond Personhood and Autonomy: Theory and Premises of Privacy', *Utah Law Review*, 2001, pp.442 and ff.

<sup>49</sup> On that point particularly, J.S. Mill, *On Liberty*, G.Himmelfarb (ed.), 1984.

<sup>50</sup> Konvitz, 'Privacy and the Law: A Philosophical Prelude', *Law and Contemporary Problems*, 1966, 31, 272, 279-280.

<sup>51</sup> Since the 1981 judgement in *Young, James and Webster v. United Kingdom* (Eur.Ct.H.R., 13 August 1981, Series A No.44) the European Court on Human Rights acknowledges an *horizontal effect* to the Convention, extending the scope of protections to relations between private parties: §49: 'Although the proximate cause of the events giving rise to this case was [an agreement between an employer and trade unions], it was the domestic law in force at the relevant time that made lawful the treatment of which the applicants complained. The responsibility of the respondent State for any resultant breach of the Convention is thus engaged on this basis.' Through this horizontal effect of the Convention, the fundamental rights seem to gain positive effectiveness. The matter is highly

Strasbourg jurisprudence the State is not merely under the obligation to abstain from interfering with individuals' privacy but also to provide individuals with the material conditions needed to allow them to effectively implement their right to private and family life.<sup>52</sup> In other words, according to the theories of the 'positive duties' of the State combined with that of the 'horizontal effect' of the ECHR broadly applied by the European Court of Human rights, States are under the obligation to take all appropriate measures in order to protect fundamental rights of the individuals including against infringements by other non-state parties.

As to the 'scope' of privacy, it has been interpreted by the European Court of Human Rights as encompassing all the domains in which individuals are confronted with the need to make fundamental choices in their life, including their sexual life and sexual preferences<sup>53</sup>, their personal and social life<sup>54</sup>, their relationships with other human beings<sup>55</sup>, the choice of their residence in full knowledge of the environment etc.<sup>56</sup>

Interestingly, the inclusion, in the scope of the right to privacy, of the choice of one's residence in full knowledge of the environment attests to the fact that access to essential information is indeed a precondition to the free development of one's personality. This has justified a number of legislative initiatives in our countries to

controversial, however, just as controversial as the question of the conception of privacy either as a mere *privilege* or as a (subjective) *right*. See also *X and Y v. Netherlands*, 8978/80 (1985) ECHR 4 (26 March 1985), Series A, Vol. 91: 'although the object of Article 8 (Art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see the *Airey* judgment of 9 October 1979, Series A No. 32, p. 17, para. 32). These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.'

<sup>52</sup> The positive duty of the State to provide the means necessary in order to allow effective enjoyment of rights is not as such recognised in the United States, neither by the law, nor by the jurisprudence. This might be only superficially coherent with classical liberalism. Mill's assertion that 'The only freedom which deserves that name is that of pursuing our own good is our own way... each is the proper guardian of his own health, whether bodily or mental and spiritual. Mankind are greater gainers by suffering each other to live as seems good to themselves than by compelling each to live as seems good to rest.' (J.S. MILL, *op.cit.*, p. 72, does not necessarily imply that the State should not provide the individuals with the resources they need to pursue their own good.

<sup>53</sup> *X and Y v. Netherlands*, 8978/80 (1985) ECHR 4 (26 March 1985), Series A, Vol. 91.

<sup>54</sup> *Beldjoudi v. France*, 12084/86 (1992) ECHR 42 (29 March 1992).

<sup>55</sup> *Niemietz v. Germany*, 13710/88 ECHR 80 (18 December 1992) Series I, Vol. 251 B.: 'The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.'

<sup>56</sup> On all these issues, read the different articles published in F.SUDRE (ed.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Collection Droit et Justice 63, Bruxelles, Nemesis, Bruylant, 2005.

develop what has been called Universal access to the Information infrastructure and guaranteed access to public informational resources, etc.<sup>57</sup> The *Guerra* case judged by EHRC<sup>58</sup> is in that perspective and illustrates this movement. In that decision, on the basis of the Article 8 of the EHRC, the Strasbourg judges have asserted the governmental obligation to deliver information about environmental risks to Italian families, which had planned to install their home close to a polluting industrial complex. The Court held that the choice of residence, which is essential to family life, implies, in our Information Society, that the information required for exercising that choice be available to the families.<sup>59</sup>

Besides the development of a right to autonomous and informed decision making in existential matters, the Strasbourg jurisprudence also understood the right to privacy as encompassing informational issues, understanding Article 8 of the European Convention on Human Rights as guaranteeing the individual right to control personal information, including in the workplace<sup>60</sup> (the scope of the right to privacy and of the right to data protection may intersect with regards to 'informational privacy'), the right to access one's personal records.<sup>61</sup>

<sup>57</sup> This idea of a 'Public Domain Content' has been clearly promoted by the UNESCO. See, Point 15 of the 'Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace', adopted by the UNESCO General Conference at its 32nd session (Oct. 2003): 'Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation.'

<sup>58</sup> *Guerra v. Italy* Case, February 19, 1998.

<sup>59</sup> About this question of the link between Privacy and the different facets of a new Right of access to Public Information resources, read C. de Terwangne, *Société de l'information et mission publique d'information*, Doctoral thesis, Namur, 2000, available at [http://www.crid.be/pdf/public/These\\_cdeterwangne.pdf](http://www.crid.be/pdf/public/These_cdeterwangne.pdf).

<sup>60</sup> See the recent decision by the European Court on Human Rights, in *Copland v. United Kingdom*, 62617/00 [2007] ECHR 253 (3 April 2007), in which the Court held that monitoring of an employee's emails, Internet usage and telephone calls had breached the employee's right to privacy. The Court held that even monitoring the date and length of telephone conversations and the number dialled could give rise to a breach of privacy. The arguments of the court included the fact that the employee had not been informed that her telephone calls might be subject to monitoring and that, at the time, no law existed in the UK that allowed employers to monitor their employees communications. Indeed, the Regulation of Investigatory Power Act of 2000 was not yet in force at that time. The Court does not investigate whether that Act might be inconsistent with the Human Rights Act however.

<sup>61</sup> *Gaskin v. United Kingdom*, 10454/83 (1989) ECHR 13 (7 July 1989), Series A No. 160. See also *Odièvre v. France*, 42326/98 (2003) ECHR 86 (13 February 2003), where the ECHR acknowledged that the right to privacy (Article 8 of the European Convention on Human Rights) protects, among other interests, the right to personal development and acknowledged that matters relevant to personal development included details of a person's identity as a human being and the vital interest in obtaining information necessary to discover the truth concerning important aspects of one's personal identity.



### 2.6.3 Privacy as 'Informational Self-Determination': Reinventing Data Protection?

#### 2.6.3.1 The Rationales of Data Protection

The fundamental principles of data protection (fair processing, performed for specific purpose, on the basis of the subject's consent or of other legitimate basis laid down by law, subjective rights of the data subject to access and rectify collected data) had been formalized in the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe<sup>62</sup> and reiterated in the fair information principles formalised in the European directive on the protection of individuals with regard to the automatic processing of personal data<sup>63</sup> and in the European directive concerning the processing of personal data and the protection of privacy in the electronic communication sector.<sup>64</sup> 'The ability of an individual to control the terms under which their personal information is acquired and used'<sup>65</sup> is often presented as the hallmark of data protection.

The rationale behind the data protection regimes relates to the risks to individual self-determination carried by the early development of the Information technologies infrastructures. The use of Information Technologies has been considered, from the beginning, as worsening power asymmetries between data subjects (the individuals whose data are processed) and the data controllers (in charge of the collection, storage, processing, use and dissemination of data). Technological developments gradually brought about a situation where (a) there is virtually no limit to the amount of Information that can be recorded, (b) there is virtually no limit to the scope of analysis that can be done – bounded only by human ingenuity and (c) the information may be stored virtually forever.<sup>66</sup>

These developments had of course direct impact on the autonomy of the data subjects: vast collections and intensive processing of data enable data controllers such as governmental authorities or private companies to take decisions about individual subjects on the basis of these collected and processed personal information without allowing for any possibility for the data subjects to know exactly which data would be used, for which purposes, for which duration and overall without control of the necessity of these processings in consideration of the purposes pursued by the

<sup>62</sup> Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe, ETS No. 108, Strasbourg, 28 January 1981.

<sup>63</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23 November 1995.

<sup>64</sup> European Directive 2002/58/EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.

<sup>65</sup> M.J. Culnan, 'Protecting Privacy online: Is self-regulation working?', 19 *Journal of Public Policy Market*, 2000, 1, pp. 20 and ff.

<sup>66</sup> H. Nissenbaum, 'Protecting Privacy in a Information Age: the Problem of Privacy in Public', 17 *Law and Phil.*, 1998, pp. 576.

public or private bureaucracies. Data Protection regimes were thus designed (and, in some countries, translated into self-regulatory measures) in order to better balance 'informational power'. This resulted in a widening of the protection previously limited and centred on intimate and sensitive data, which now included all personal data defined as 'information about identified or identifiable individuals' and in the attribution of new rights to the data subjects, including an 'access right' allowing a better control over the uses and dissemination of personal data and, finally, the imposition of limitations to the permissible processing by data controllers, especially through the requirements that data processing will be fair, legitimate (another word for proportionate both as regards the existence of the processing and its content) and secure.<sup>67</sup>

These main principles might be viewed as a development of the self-determination principle in the area of the personal data flows. 'Informational privacy' had been defined traditionally by the U.S scholars following the A. Westin wording<sup>68</sup>, as the 'claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated through others'. That American definition inspires some scholars to use the argument that there was a sort of 'intangible property right' held by each individual over his or her personal data<sup>69</sup> and that individuals could legally 'sell' their personal information on the market and, in that way, 'choose their optimal mix of privacy without parental intervention from the State'. We will come back on this issue later in the discussion of the recent EU Constitutional or quasi constitutional acknowledgement of the right to Data Protection.

#### 2.6.3.2 'Classical Privacy' and Data Protection: Complementarities and Interactions

The legal protections offered by Article 8 of the European Convention of Human Rights (and taken over in Article 7 of the Charter of Fundamental Rights of the European Union) and by the right to data protection now acknowledged by Article 8 of the Charter of Fundamental Rights of the European Union and implemented by the two data protection directives, interact in a variety of ways. The European Court of Human Rights has acknowledged that 'informational privacy' is among what Article 8 of the ECHR protects. In this regard, data protection directives are

<sup>67</sup> Security is envisaged in its broadest sense, meaning both integrity, confidentiality, accountability and availability.

<sup>68</sup> A. Westin, *Privacy and Freedom*, New York, Ateneum, 1967, p. 7. For other similar definitions, read D. Solove, 'Conceptualizing Privacy', article already quoted, pp. 1110 and ff.

<sup>69</sup> The theoretical approach of the Privacy viewed as a 'property right' has been developed particularly by the author defending the economic analysis of the Law. See on this approach, among numerous authors, R.A. Posner, *Economic Analysis of the Law*, New York, 1998, pp. 46 and ff (considering Data Privacy law functionally as 'a branch of property Law'); E.J. Jagger, 'Privacy, Property, Intangible Costs and the Commons', 54 *Hastings Law Rev.*, 2003, pp. 899; J. Rule and L. Hunter, 'Towards a property right in personal Data,' in *Visions of Privacy, Policy Choices for the Digital Age*, C.J. Bennett and R. Grant (ed.), 1999, p. 168.



among the *tools* through which the individual exercises his right to privacy. More generally, having the guarantee that personal information (personal data) will not be collected and used in manners that totally escape from the individual's control is indeed a precondition for the individual to feel genuinely free from unreasonable constraints on the construction of his identity.

Yet, data protection is also a tool for protecting other rights than the right to privacy: preventing the processing of information relating to the individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and concerning the individual's health or sexual life, the data protection directives prevent potential discriminations on those grounds. On the other side, the right to privacy is irreducible to the right to data protection: it guarantees the inviolability of the home (spatial privacy), has to do with the inviolability of the human body and protects the individual's emotions and relationships with others. What privacy protects is irreducible to personal information. Privacy and data protection intersect but are also different tools for enabling individual reflexive autonomy and, as a consequence, also collective deliberative democracy. These tools are not to be put on the same footing though. Whereas the concept of privacy refers to the double aspects of the guarantees the State has to provide to the citizens in order to ensure their capabilities of self-development; the concept of data protection appears in a second step, taking fully into account the new risks threatening the two 'aspects' of privacy (the right to seclusion and the right of decisional autonomy), ensuing from the development of the information and communication technologies. It thus appears obvious from there that data protection regimes are intended both, with regard to the 'seclusion' aspect of privacy, to protect our 'private sphere' (for instance by forbidding the processing of certain sensitive data or by enlarging the secrecy of the correspondence to electronic mails) on the one hand and, on the other hand, with regard to the 'decisional autonomy' aspect of privacy, to increase the transparency of information flows and to limit them in order to prevent disproportionate informational power relationships to be developed or perpetuated between public and private data controllers and citizens.

### 2.6.3.3 Data Protection and Its 'Constitutionalization': Opportunities and Ambiguities

The role played by the European Union, particularly through 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<sup>70</sup> and Directive 2002/58/EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector<sup>71</sup>, could make believe

<sup>70</sup> Official Journal L 281, 23 November 1995.

<sup>71</sup> Official Journal L 201, 31 July 2002. See also the 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 communication services or of public

that the 'right to data protection' is above all the result of the need, for the European single market, to harmonize data protection regimes as to ease the free circulation of goods and services. But the European Data Protection regime has its roots in the European human rights regime and more particularly, in Article 8 of the European Convention on Human Rights and in the Convention No. 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data enacted in 1981 (before that, data protection had already been enacted in the Swedish Law of 1973). The Charter of Fundamental Rights of the European Union<sup>72</sup>, in its Article 7, §1 reasserts the existence of the right to private and family life, home and communication, whereas Article 8 of the same Charter acknowledges, as already noted, that the right to data protection has the status of a fundamental right:

1. Everyone has the right to the protection of personal data concerning him or herself.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or herself and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

This acknowledgement of the right to Data Protection as a fundamental right, distinct from the traditional fundamental right to privacy, enacted in Article 7 of the Charter is questionable and invites some comments. This 'constitutionalization' of data protection might be considered 'an added' to the extent that it enlarges the application of the main principles of the Directive to all processing of personal data, including those that are not covered by the Directives but processed in the context of EU second and third pillars. The constitutional status given to Data Protection provides data protection regime with a sort of constitutional privilege over competing legislative texts and allows for Constitutional control of its implementation respect by the Constitutional Courts. To this well intentioned acknowledgement of the fundamental importance of the right to data protection, two critiques may be raised: the first one relates to the wording of the second paragraph, which seems to suggest that consent would provide *per se* a legitimate ground for any processing. The second critique is more fundamental: by placing the right to data protection' at the same level as privacy, the European text carries the risk that the fundamental anchoring of data protection regimes in the fundamental values of dignity and autonomy will soon be forgotten by lawyers and that legislators will soon forget to refer to these fundamental values in order to continuously assess data protection legislations, taking into account the evolution of the Information Society.

communications networks and amending the Directive 2002/58/EC, Official Journal, L 105, 14 April 2006 P. 0054-0063.

<sup>72</sup> 2000/C 364/01.

### The Limited Value of the Consent as Legitimate Ground for Data Processing

One may but regret some of the dangers raised by the wording of Article 8. In situations other than those where the legitimacy of processing is grounded in a legislative text, Article 8 explicitly acknowledges consent by the data subject as a necessary and sufficient condition legitimizing data processing, whereas consent is often derived from the simple interaction in the networks. Growing conflation of consent and interaction makes the condition of consent less and less demanding. Most websites include, as part of the transactional process with their customers, specific steps aimed at collecting consents to various processing they find profitable, including the possibility to share any obtained data with third parties, to create users' profiles and to use those profiles for individualized marketing (operated by themselves or by others) purposes. In some cases, consumers are driven to consent through financial incentives (fees or price reductions; gratuitous participation in a lottery, etc.). The use of some services may be dependent on such express consent to processing of the data obtained through the operation of those services.<sup>73</sup>

This approach is advocated using the argument that the 'right to data protection' is the right for the individual to decide about the dissemination of his or her own information. And as nobody is better placed to judge if he or she wants to disseminate data about his or her self, individual consent is necessarily a legitimate ground for the processing of personal data. The argument, making of personal data the alienable property or commodity of the data subject, is disputable<sup>74</sup>: medical data, for example, may arguably be said to belong to the medical practitioner in charge of the patient and who 'produced' the information contained in the medical file, as much as to the patient himself.<sup>75</sup> In the 'property approach', personal data

<sup>73</sup> Margaret Jane Radin, 'Justice and the Market Domain', in John Chapman, J. Roland Pennock, *Markets and Justice*, New York University Press, 1989, p. 168: 'the domino theory asserts that market evaluations of objects and activities are imperialistic, diving out other and better ways of perceiving and evaluating objects and activities. Once some individuals attach a price at a given object, relation or activity, they and others tend to lose their capacity to perceive or evaluate that object, relation or activity as anything but a commodity with a specific market price. Moreover, the theory asserts, once certain objects or activities are commodified, there is a tendency for other objects or activities of the same sort or even of other sorts also to be seen and evaluated merely in terms of their actual or potential market value.'

<sup>74</sup> The context of the Internet creates new possibilities for Internet users to express his or her consent. In a first version of P 3 P (Platform for Privacy Preferences), the Internet's user had the possibility to negotiate his or her privacy preferences against financial advantages. This possibility has been discussed extensively in the American literature, see P.M. Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace, Filters, Privacy control and Fair Information Practices', *Wisconsin Law Review*, 2000, p. 749 et s.; M. Rotenberg, 'What Larry doesn't Get the Truth', *Stan. Techn. L. Rev.*, 2001,1, disponible sur le site: [http://www.sth.Stanford.edu/STLR/Articles/01\\_STLR\\_1](http://www.sth.Stanford.edu/STLR/Articles/01_STLR_1).

<sup>75</sup> As Kang & Butner observed: 'But Economist, merely creating property rights in personal data says nothing about to whom property is initially assigned, correct? So let's say a citizen bought prodigious amounts of St John's herb from a vendor last Friday. Which of them owns the 'property', that is the knowledge of the citizen's purchase? And what precisely would such ownership entail' (J.Kang & B. Buchner, 'Privacy in Atlantis', 18 *Harv. Journal Law &*

is considered a valuable commodity that may be the object of bargains and transactions with other people through licenses.<sup>76</sup> Closely connected with the property approach, the contract approach puts party agreement at the heart of personal data processing. Regardless of whether personal data are viewed entirely as property, the contractual approach allows parties to make promises regarding personal data and their processing'.<sup>77</sup> As observed by Schoeman<sup>78</sup>, 'One difficulty with regarding Privacy as a claim or entitlement to determine what information about one self is to be available to others is that it begs the question about the moral status of privacy. It presumes privacy is something to be protected at the discretion of the individual to whom the information relates.'

Much more objections than one could report in the present contribution exist against considering consent as a sufficient condition of legitimacy of the processing of personal data. For our purpose here, it suffices to recall that under the EU Directive, consent, as defined by Article 2.h) of the Directive<sup>79</sup> is not presented as a completely sufficient basis for legitimating processing. In any case – even in case of unambiguous consent – it may be possible to declare the processing illegitimate if that processing is disproportionate. The control of proportionality clearly suggests the need for societal control or monitoring of the legitimacy of the processing.

Other, more classical, arguments might be advanced for justifying the insufficiency of the consent.<sup>80</sup> The information asymmetry and power inequality, disadvantageous to the data subject or, as argued by D. Solove<sup>81</sup> among others, the fact that a large portion of 'personal data' may in fact be relevant not only to the individual but also to others with whom the individual entertains or has entertained relationships. Another line of argument refers to the difficulty, for the consenting

*Techn.*, 2004, p.9. This article is written in the form of a Socratic discussion between protagonists of different thesis and representatives of different functions in a Society in order to build up a consensus about the main principles of a future Privacy legislation). This assignation might be justified following a market-based approach by the greater efficiency of this solution.

<sup>76</sup> As regards the similarities between this kind of contract and the Licensing contracts about works protected by the Intellectual Property, read P. Samuelson, 'Privacy as Intellectual Property', 52 *Stanford Law Rev.*, 2000, pp. 1125 and ff.; J. Litman, 'Information Privacy/Information Property', 52 *Stanford Law Rev.*, 2000, pp. 1250; K. BASHO, 'The Licensing of the personal information. Is that a solution to Internet Privacy?', 88 *California Law Rev.*, 2000, pp. 1507.

<sup>77</sup> J.Kang & B. Buchner, 'Privacy in Atlantis', 18 *Harv. Journal Law & Techn.*, 2004, p.4.

<sup>78</sup> F. Schoeman, 'Privacy Philosophical Dimensions of the Literature', in *Philosophical Dimensions of the Privacy*, F.D. Schoeman (ed.), 1984, p. 3.

<sup>79</sup> Article 2 h defines the data subject's consent as 'any freely, given specific and informed indication of his or her wishes by which the data subject signifies his agreement to personal data relating to him being processed.' This consent implies that the data controllers have given the relevant information about the mode and the extent of the data processing for which consent is given.

<sup>80</sup> See particularly, M.A. Froomkin, 'Regulation and Computing and Information Technology'. Flood control on the Information Ocean: Living with Anonymity, Digital Cash and 'distributed Databases', 15, *Jour Law & Com.*, 1996, pp.395 and ff. (this author speaks about a 'myopic, imperfectly informed consumer'); J.Cohen, 'Examined Lives: Informational Privacy and the subject as object', 52 *Stanford Law Journ.*, 2000, pp. 1373 and ff.

<sup>81</sup> D.J. Solove, 'Conceptualizing Privacy', 90 *Calif. Law Rev.*, 2002, p. 1113.



data subject, to keep track of personal data in secondary transfers and to verify in what measure these secondary transfers are respecting the conditions of the initial license given by the data subject.<sup>82</sup>

Some of those 'weaknesses of consent' could be remedied, as has been done in the context of the consumer protection, by reinforcing the right to be informed and affording new rights to the consumer including class action, when appropriate, in order to decrease power and information inequalities and asymmetries in the Information market (information technology<sup>83</sup> may be of great help in this regard, allowing for example the digital 'marking' of each bit thereby empowering the data subjects with regard to the control and limitation of their transfers. Others – especially those ensuing from socio-economic and other structural inequalities among stakeholders may be more challenging.

#### The Anchorage of Data Protection Legislation in the Protection of Fundamental Human Values

Another inconvenience of making the 'right to data protection' a distinct fundamental right is that it risks obscuring the essential relation existing between privacy and data protection and further estrange data protection from the fundamental values of human dignity and individual autonomy, foundational to the concept of privacy and in which data protection regimes have their roots, as has already been argued. Keeping in mind those fundamental values and the 'instrumental' value of data protection in this regard is crucial if one is to adapt the legal regime to the changing technological circumstances of the time. Moreover, acknowledging the fundamental values behind the right to data protection makes it clear that, contrary to certain interpretations of that right, it is not amenable to a kind of individual alienable property right over personal data. Finally, taking the fundamental roots of data protection seriously justifies that one should not content ourselves with the current tendency to consider individual consent as sufficient criterion for establishing the legitimacy of whatever processing is considered useful by public or private bureaucracies.

This 'return to the basics' approach provides powerful arguments to refuse the 'information market' approach advocated by some. It goes without saying that those basic values will be immensely useful in showing the direction for the revisions of our data protection regimes<sup>84</sup>, arguably necessary due to the unprecedented

<sup>82</sup> Already in 1989, P. Samuelson, 'Information as Property: Do Ruckelshause and Carpenter Signal a changing Direction in Intellectual Property Law?', 18 *Cath. U.L. Rev.*, 1989, pp. 365 and ff.

<sup>83</sup> DRM technologies developed for protecting works covered or not by intellectual Property Rights might be also used here. On that issue, J. Zittrain, 'When the publisher can teach the Patient: Intellectual Property and Privacy in an era of Trusted Protection', 52 *Stanford Law Rev.*, 2000, p.1201 insisting about the fact that in both cases, it is about protecting the data, whether it is a brilliant article protected by Intellectual Property Rights or my shopping habits considered as personal data.

<sup>84</sup> About the need to have a third generation of Data Protection legislation in order to face the new challenges of ICT recent developments and about new principles to enact in that context,

challenges raised by the recent and future developments of the global Information Society on the threshold of the 'ambient intelligence era'.<sup>85</sup>

## 2.7 Conclusion: Privacy as a Bidirectional Principle Fostering the Autonomic Capabilities of Individuals

Agre, reflecting on privacy, commented that

... control over personal information is control over an aspect of the identity one projects to the world, and ... the freedom from unreasonable constraints on the construction of one's own identity.<sup>86</sup>

The two aspects – freedom from unreasonable constraints (from the State or from others) in the construction of one's identity and control over (some) aspects of the identity one projects to the world – are at the heart of what the various 'facets' of privacy are all about. Yet, more fundamentally and against the common view that the 'freedom in the construction of one's personality' and 'control over information about oneself one projects on the world' pursue different, though complementary, normative goals, we would like to argue that their common normative justification and objective, or, to say it more plainly, the final value they are meant to advance, is the capacity of the human subject to keep and develop his personality in a manner that allows him to fully participate in society without however being induced to conform his thoughts, beliefs, behaviours and preferences to those thoughts, beliefs, behaviours and preferences held by the majority. Privacy and data protection regimes should thus be understood as 'mere' tools (evolving

Y.Pouillet, 'Pour une troisième génération de législations de protection des données', *JusLetter*, No. 3, October 2005), we tried to show the extent to which directive 2002/58 when it regulates the traffic and location data generated by the use of communication services pays little attention to the fact that these data are data of a personal nature. 'The very definition of the 'data', whose protection is at the very heart of the recent directive does not follow that of 1995 exactly. The definitions of 'traffic in data' and 'localization' listed in article 2 carefully avoid expressions like 'data of a personal nature' which, however, circumscribe the field of application of the directive 95/46/EC, of which the 2002 directive would be just one application. Both articles 2 c) and preamble 14 of the Directive define localization data via simple reference to the user's terminal equipment. When it is a question of commenting on the concept of traffic in data, preamble 15 talks 'about information consisting of a denomination, a number or an address, provided by he who sends an electronic message or he who uses a connection to send an electronic message. What are we to say? These data may not be data of a personal nature, in other words the search for a link with an identified or identifiable person is no longer necessary'.

<sup>85</sup> Antoinette Rouvroy, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence', *Studies in Ethics, Law, and Technology* 2008, vol. 2, Issue 1, Available at: [http://works.bepress.com/antoinette\\_rouvroy/2](http://works.bepress.com/antoinette_rouvroy/2) (forthcoming, 2008). See, also about the new techniques of RFID body implants, the Opinion of the European Group on the Ethics of the Sciences and New Technologies of the European Commission, 'Aspects éthiques des implants TIC dans le corps humain', March 16th, 2005.

<sup>86</sup> Philip E. Agre, Marc Rotenberg (eds.), *Technology and Privacy. The New Landscape*, MIT Press, 1998, p. 3.



when required by the new threats that socio-economic, cultural and technological changes impose on individual and democratic self-determination), meant to pursue that one single common goal: sustaining the uniquely human capacity for individual reflexive self-determination and for collective deliberative decision making regarding the rules of social cooperation. We consider this as one unique, rather than two separate, goal given the mutual 'production' or reinforcement of public and private autonomy.<sup>87</sup> Privacy, as a principle catalyzing the tension inherent in individual existence between the need for retreat from others and the need for participation and interaction with others, is, depending on the context and circumstances, constantly requiring the adaptation of the legal instruments that find, in that principle, both their roots and horizon. It is not, as has been suggested by other scholars, that the 'classical' privacy regime is there to protect the facets of human life that need 'opacity' to best develop and that data protection regimes are there to organize the partial disclosures that social life and interactions require. Rather, both facets – 'seclusion' and 'inclusion and participation', are, depending on the circumstances, best preserved by a combination of legal tools protecting against undue interference in existential matters, or protecting personal data against a series of illegitimate collections and misuses.

Thus, 'classical' privacy regimes and data protection should be conceived together as forming the evolving bundle of legal protections of the fundamental individual and social structural value of the autonomic capabilities of individuals in a free and democratic society. Guaranteeing the generic right to privacy (or the principle of privacy, should we maybe say), given the crucial role it plays in enabling the autonomic capabilities of the individual legal subject, is a precondition to any meaningful exercise of all other rights and freedoms acknowledged by the Council of Europe. This is particularly explicit in the case of freedom of expression but is also true regarding all other fundamental rights and freedoms, including, crucially, those social and economic rights<sup>88</sup> that guarantee the full participation of the individual in the social and political fabric of society.

---

<sup>87</sup> See above, notes 24 and 25, and accompanying text.

<sup>88</sup> As Burkert (quoted *supra* footnote 33) asserts it: 'Even in their passive state fundamental rights need economic and social framework conditions which make the use of such rights meaningful. This observation is reflected in the (still heavily contested) extension of fundamental rights into the area of economic and social rights. Some of the discussions at the World Summit of the Information Society, already mentioned above, might well be seen as a tentative connection of 'privacy' to such social and economic rights in the information society'.