Privacy

Poullet, Yves

Published in:
Proceedings of the XXXI International Conference on Data protection and Privacy

Publication date:
2009

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

Privacy: Conditions for its survival in our I.S.

© Yves Poullet
Professor Faculties of Law Namur and Liège (Belgique)
Director of the CRID (University of Namur)[1]

http://www.crid.be

Summary

New Internet applications are characterized by some features: ubiquity of terminals, opacity of their functioning and of the data flows generated, maximization of individual's participation (Web 2.0 applications) and limitless capacity of computer analysis which permits use of profiling methods. These characteristics lead to the emergence of an "Observation society", functioning with the implicit understanding and interpretation of the data as valid and privileged source of « truth » about the persons, their preferences, intentions, etc. Decisions are taken a priori on the basis of this data and profiles rather than on information by the data subjects (risks of reductionism and de-contextualisation) with all the additional risks created by the increasing power asymmetries between data subjects and data controllers.

It must be underlined that these developments are undermining not only what we do consider traditionally as our "right to privacy" but also all our fundamental liberties (especially our freedoms of expression or of movements) and are multiplying the risks of discrimination.

At our opinion, firstly, as it has been asserted in the recent EU Commission recommendation on RFID and Privacy, a societal control (including from a social, psychological and ethical point of view) measuring the impact of the ICT applications on the individuals' autonomy is needed. Secondly, as the design of the terminal equipment influences many processing operations, certain security responsibilities should be imposed on producers or designers so as to prevent operations to be carried out in unfair or illicit manner, In conclusion, it is at the roots of the Technology where we should find the solutions to risks created by the use of that Technology.

Introductory remarks

1. ICTs with their ubiquitous and universal character drastically are modifying our environment and our economic and social relationships. This trend will increase in the future in a way only partially predictable For example who would have predicted that RFID conceived in a first moment to re- emplace the bar code would served as a way to detect at distance the health state of human being. They are more and more everywhere and offering to each of us a place without limits where we express ourselves, where we might access to more and more personal services but also where

[1] Our gratitude to my colleagues: Claire Lobet and Antoinette Rouvroy for their valuable inputs.

we meet front to front with multiple visions of the world which were previously maintained separated behind physical or social barriers. So they create an unique opportunity to develop ourselves and to enter into dialog founded on the recognizance of a large diversity of opinions and might contribute to an cultural, economic, intellectual, democratic and human enrichment of the global society.

2. This dream inherent to the potential development of the Information Society might lead, if we are not cautious, to a nightmare. It is not obvious that the way the technologies are presently designed and applied will contribute to the development of our liberties and of our democracies. Privacy concept has been, traditionally but now more than never, designated as the appropriate concept to defend these values in our Society. The reasons why certain concerns are growing on that point are the following.

3. The development of ICT can be firstly described in a continuous and tremendous growth of computer and communication systems capacities. The so called Moore's Law predicts that every 18 months the storage capacity of a computer is multiplied by two for the same price, which implies the multiplication by 1,000 in fifteen years. It is becoming possible to store on a personal computer the record of all the events of my life and certain imagine to set-up a central GRID collecting the basic identification data of all people around the world. This capacity of storage doubled by an increasing capacity of processing and transmission explains how Google can validate your request, scanning in less than 10 seconds more than a thousand million sites worldwide. It explains also the development of what we call the Web 2.0 multimedia applications like YouTube, Daily motion, etc. and in the next future the new "cloud computing applications".

4. The Internet revolution might be described from different point of view. The global character of this network of network has a double meaning. It means not only the universal dimension of this infrastructure and the interoperability norms but also the convergence of all networks traditionally clearly separated like TV channels and mobile infrastructure and thus the possibility to cross match the data created by all these communication activities. In order to have a better interoperability between computers, to dialog among themselves or to be able to understand automatically the messages we are sending, the Web is becoming semantic: it does mean that, without necessarily human intervention, the computer can create itself meta data from the data it stores or sends in such a way that people even computers can easily have an access to their data and process them.

5. Ambient Intelligence[2] is perhaps the more recent outcome of the ICT evolution. With the miniaturization of the terminals to a "smart dust" and their implantation in objects, clothes even in our own bodies, wireless, sensors and networking technologies, it is now possible to conceive interaction between human and their physical environment in new ways and things might now interact together send information about themselves and their users through electronic networking to data bases. If gains of convenience, efficiency and safety undoubtedly are linked with these developments, in the same time, concerns are raised as regards the increasing traceability these technologies are offering and which might be tempting not only for marketers but also for law enforcement

[2] "The central idea of these networks is to create environments in which people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects. It is an environment that is capable of recognizing and responding to the presence and actions of different individuals in a seamless, unobtrusive and, often, invisible way using several senses"

authorities and companies to ensure security. So, TV sets will know which programmes we are interested in; the fridge would like to tell us what kind of beverages we would like to re-order or to reorder by their own. Our mobile will indicate us the closest restaurant that meets our appetites and tastes. The employer might follow the movements of our employees during the whole day and any deviation from their normal way. The police will follow suspected people by invisible tags embedded in identity card or elsewhere.

The technology is becoming ubiquitous covering all the events of our everyday life. We speak also of a learning technology insofar they are able to adapt their functioning to data obtained through their use. So, the RFID system installed in a large store will learn progressively apart from my different moving, purchases and from other sources my preferred wine and cheese, when I use to come, the amount of money I am usually spending, etc. This learning process have as result the possibility to predict my future behaviour and so to influence my conduct

These technological developments all denote a progressive shift away from PCs and desktop configurations well located even is not fully mastered by their users to devices embedded in the physical environment functioning following unknown rules. Things and people are interacting. At the heart of these networks created by the dialogue between things, among things or between things and people, human being can become a "thing" itself inserted into a relation with other things which react to its or his/her presence.

6. "Digital identities" linked to individuals or to be more precise with his or her bodies (biometric data) or with objects under their use (cookies or IP as regards the personal computer or the communication mean; tag number as regards RFID enshrined in clothes or…) or simply with works or objects[3]. One underlines the double role of these "digital identities". They firstly might be used as "authentication" tool, especially to control the access to certain resources. Secondly they are essential for reconstructing information about a person identified or not apart from pieces of information scattered in data bases geographically dispersed through the network and that without limit of national borders. Let us notice that biometric data precisely because there are directly linked with the body are available during the entire life of the individual, without possibilities of modifications and therefore creating new privacy risks.

7. The different uses or presences of all these technologies surrounding our daily life the web, mobile phones, electronic financial systems, biometric identification systems, RFIDs, GPS, ambient intelligence are generating data. All these data might be processed for still more pervasive and powerful data mining and tracking systems. These processing will lead through extensive data mining and profiling to real-time and autonomic applications which impact upon ongoing actions and their environment. What characterizes the profiling definitively is its use of pure aleatory statistical methods permitting to discover correlations between *a priori* not logically linked elements. The profiles established through these methods are considered in itself as pertinent information and applied to persons.

[3] See the Object Names System put into place by EPC Global in the context of a large development of RFID. ONS will permit to trace a product to know exactly the producer, distributor, the ingredients, etc. Placed at a certain distance of a reader which might be the mobile, it permits to a consumer to know exactly the product he or she is purchasing.

I. Why our privacy is at stake?

8. Indeed, ubiquitous computing is creating a new environment and the central question that needs to be addressed now is: "How to make this new environment sustainable from both individual and societal points of view and how to redefine the position of human beings in this new environment? Till now, the predominant view, at least in Europe, is to consider privacy as the most adequate and relevant concept to ensure an appropriate protection of human dignity, of fundamental rights and liberties. According to the ECHR case law, Privacy is viewed as a pre-condition not only for the self-development of human beings but also for their ability to take an active role as citizens within a democratic state. However, one must admit that the concept of privacy is subject to a variety of interpretations and its protection is more and more difficult to ensure in the new information and communication era. In fact, the challenge posed by new technologies is more serious than weakening the effectiveness of privacy protection instruments: we have reached a state where new technologies call into question the very foundations of privacy and ultimately the position of the subject in the new information era.

A. The imbalance of information powers

9. First, perhaps we have to remind that the first Data Protection legislations have been enacted to remedy the imbalance of respective powers of those responsible for data processing on one hand and the person concerned on the other. This imbalance can lead to all kinds of discriminations and introduces a deep disequilibrium between the "Information-have" and the "Information-have not". The situation today multiplies the information at the disposal of certain intermediaries whose intervention does represent *de facto* a mandatory passage for getting the resources available on the Net. Information and communication technologies (ICT) allow the collection and processing on a large scale of data, including personal data even biometric data. Furthermore, the continuous development of technologies poses new challenges as regards collection and further processing of data. Particularly, this collection may use in particular the processing of traffic data and user queries on the Internet, the recording of consumer purchasing habits and activity, the processing of geo-location data concerning mobile telephone users, the data collected by video surveillance cameras and by RFID systems, foreshadowing the "internet of things". In other terms, the data subjects are more and more transparent whereas in the same time, the data controllers might act with opacity and maximizing through more and more powerful and sophisticated software the knowledge he has about people. This knowledge creates major risks of discriminations and attempts to social justice requirements. The sharpening of power inequalities between those that have that knowledge and those that are being traced, surveyed even tracked have to be considered as threat to privacy as personal autonomy but also raises questions as regards fairness and due process, taking into account the potential manipulation, by companies or administrations, about individuals, manipulations inherent in knowledge asymmetries

B. The "decontextualisation" of data processing

10. Our **second** point underlines the variety of data which might be collected by certain actors especially the gatekeepers or intermediaries like web 2.0 platforms, search engines' providers, internet access providers or telecom operators including mobile or payment systems ones. Their intervention is needed for accessing to services which

might be deemed as essential services in our Communication Society. Through their channels, indeed, we are exchanging with a large number of persons in all the aspects of our social, family, professional life, we are interacting for multiple purposes including for medical, political, philosophical reasons, we are accessing to a large range of information and services useful or not. In other terms, these gatekeepers are collecting data revealing more less all the facets of our personality, our various identities. All these "identities" traditionally were carefully separated following the context of the exchange of data. So for instance the data exchanged with my healthcare practitioner were limited to the information presumed important for detecting diseases and when I was at my office, my employer was supposed to use information only related to my job.

The Data protection legislation has enacted this obligation to maintain that "contextualisation" principle both through the prohibition to use data for not compatible purposes and by the proportionality principle. This principle of data contextualisation precisely is now put into question by the fact that intermediaries are collecting the data generated in a lot of different context. Social networks platform are collecting data of all the aspects of my life and sometimes disseminating them if as user, I have not taken adequate protection by multiplying different identities and activating the appropriate privacy settings. This "decontextualisation" raises certain concerns since it creates major risks for being judged "out of context". The example of the employer having at look at the Facebook's pages of the candidate employee is a clear demonstration of this risk. The fact that Google might store all the keywords I have typed and the web pages visited starting from the search engines web sites gives to this company the possibility to have a comprehensive view of most of my subject of interest whatever that concerns my social, family, or professional lives, my health status, my cooking preferences or my travelling habits. The use of search engines reveals the multiple facets of personalities that we are looking after through their names as keyword.

C. From individuals' tracking towards their anticipatory conformism

11. The introduction pinpoints a **third** challenge: the frequent opacity of the functioning as much of terminals. The information systems' opacity carries the fear of unsolicited and unwanted information processing, and the motivation henceforth is to conform to a behaviour believed to be expected in these new invisible places of surveillance. The data are often collected and merged without the subject's notice, based on different technical devices such as cookies, IP addresses or RFID tags playing a role of "silent and continuous trackers" of the users' habits. These systems raise obvious questions regarding personal data protection and question one of its key principles, the informed consent. But they also raise controversies about the empowerment and capabilities. These controversies concern the self-determination of the individuals and their capabilities to build their own past and present personality and social life by personal learning, seclusion and reflexive experiences and the shaping of their proper history and images. With these systems, the personal and social experiences are to some extent perverted by external silent rationalities and logics characterized by their opacity and fuzziness which do not allow individuals to impact on the "informational image" compiled on themselves nor on the interpretation thereof. To some extent, these systems question the vitality and the diversity of our society because they foster **social anticipatory conformism** and therefore undermine our democracies, as clearly asserted by the first German Constitutional Court decision asserting the right to informational self determination in 1983.

D. A double reductionist approach

12. **Fourthly,** the use of modern data processing technologies leads to two forms of reductionism. From one part, reductionism means that persons are no more identified by their data but by their "**profiles**". As previously explained, collected data are concerning events, even the most trivial in our lives. The generation of these data by our increasing use of terminals of all kinds, their storage within huge datawarehouses and the application of data mining software makes possible the definition of profiles which might be applied in real time to people though automated pattern recognition. By mining of machine-readable data, profiling leads to the identification of patterns in data of the past which can develop into probabilistic knowledge about individuals, groups of humans and non-humans in the present and in the future. The difference between that autonomic profiling and what we might call the human profiling (when spontaneously, I compare the behaviour of a person to other ones and so try to deduce certain characteristics of his or her behaviour) has deep impacts on the relationships between the profiler and profiled people. The probability construed on the basis of the data mining techniques is considered as a "norm" and even if statistically they are some risks of errors, is applied without human interaction with the people to whom the norm is applied. The information systems analyse us via these profiles and by applying them automatically reduce the choices of human beings or take decision about them according not to their personalities but to their profiles. In that context, it remains to the individual (if he has the chance to know that he has been submitted to profiling methods) to contest *a posteriori* the application of the profile by showing that it does not belong to the profile. Profiling constitutes a sort of reversal of the "*onus probandi".* If traditional data protection legislations which took into consideration the risk linked to the reduction of the individuals to their data but now with profiling this risk definitively is higher. The person is no more judged as regards his or her own data but automatically and seamlessly by his or her belonging to a profile generated not by his or her data but by probabilities calculated on data collected from other persons.

13. From another part, reductionism has a second significance. It underlines the trend to use the **body as a source of truth** and to disqualify the information given by the persons about themselves. This reductionism is striking in the case of technologies assuming some kind of causal and deterministic link between facial and physical expressions and emotions or intentions. These systems combine a multimodal capture of data "extracted" from human bodies (facial expressions, eye gaze, postures and motions) with an implicit interpretation of these data as valid and privileged sources of "truth" about the persons, their preferences and intentions following the assumption according to which the "body does not lie" whereas, *a contrario* anything transiting through the prism of individuals' consciousness is *a priori* suspect and unreliable. That idea is well expressed by CEYHAN who underlines that this type of surveillance systems "*moves the site of identity from the Self (in relation to the Other) to the body itself* ".This form of very basic behaviourism puts into question the emotional privacy and the self-determination of the subject. In addition, this kind of intrusive surveillance has per formative effects on the subject's perceptions of what is expected in terms of attitudes, behaviours and preferences, with the result to increase a sort of detrimental anticipative conformity in society. This growing presence and sophistication of multimodal surveillance systems collecting data about our bodies can in part be legitimated by what certain authors have called "the advanced modernity". This modernity is characterized by a radical dislocation between time and space and this dislocation, also gives raise to a

"strangers society" where social control and governance traditionally based on intimacy and face-to-face knowledge, are less and less viable. This context of low social normativity explains one of the major features of the advanced surveillance systems, such as biometry, body tracking or facial emotion recognition which permits to detect automatically abnormal situation or behaviour and to take security measures including preventive ones.

14. Furthermore since Data protection is an expression of personal freedom and dignity, it ought not to be tolerated that data processing are exploited in such a manner as to "turn an individual into an object under continuous surveillance". Nowadays with body's implant, with ubiquitous tracking including through biometric technologies, and by the continuous on-line addressing of advertisements or of all kinds' messages, our anthropological conception of the human body is evolving. The individuals transmitting and receiving messages they are not controlling, are becoming "networked persons" (RODOTA) permanently manipulated little by little as regards their choices, opinions, movements and even their emotions or brains' functioning, putting into question their autonomy in the deepest sense. This pervasiveness of our modern ICT applications does represent a huge challenge for our privacy.

E. The blotting out of the distinction between public and private spheres

15. Finally, **last challenge** for our privacy in the broadest sense, our Information Society might be characterized by the blotting out of the distinction between the public sphere and the private sphere. Man, lost in the crowd, can be spied, followed and traced. Inversely, even in his home, doubly locked in, he/she can be followed spied, followed and his intimate secrets pierced. in his behaviours via the GMS (global monitoring system) in his pocket, through the RFID which he/she can carry, via his/her use of interactive TV, and thank to his/her computer connected to Internet. That factual statement leads to come back to the initial conception of privacy defined as the "right to be left alone". Anonymity in public space and seclusion inside our home are pre-conditions for the free development of our personality, In other words, each individual must have a physical place where to express him or her self 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. In other words it means that in public spaces, the individual must feel free to express him or herself without being continuously placed under surveillance.

II. Are there solutions?

16. Could all these new features and the involved privacy risks be adequately addressed by our current data protection legislation? Definitively Data Protection Authorities particularly are trying in certain cases through audacious reasoning to demonstrate that Directive 95/46 on data protection might bring solutions to these new challenges, but certain of their assertions raise legal objections from the courts and create doubts which might prejudice the market and, at the same time, the protection of the citizens. What we have in mind is to analyse the solutions in two steps. The first one would be dedicated to a deepening of the protection afforded by a constructive interpretation of certain provisions of the traditional data protection legislations; the second one goes a step further and definitively suggests to enlarge the privacy protection beyond its present limits and to address new issues. Certain of these suggestions will lean on

certain texts recently adopted or still in drafting process at the European level (Council of Europe or European Union).

A. First step: How to better our data protection legislation through a constructive interpretation?

a. The need to redefine and enlarge the concept of personal data and of sensitive personal data

17. Indeed, in the context of the present functioning of Internet's application, different remarks have to be proposed as regards the **central concept of personal data**. Traditionally, the personal data we had in mind were what we might call "*bibliographical data"*. It means data directly linked with past or present events of individuals' life: their home address, their health problems, the shopping basket, their precise location at a certain moment, etc. We are used to classify these data according to their sensitivity and, on that basis, to distinguish the applicable rules. As regards this category of data, the ubiquitous character of information systems, coupled with the fact that storage capacity is increasing tremendously and is cheaper and cheaper, induces the collection of more and more trivial data and instantaneous slices of our lives. The risk is no longer linked with the very nature of the data but with the multiplication of the data collected and cross-matched permitting the definition of individual profiles.

18. Apart from this first category of data, the Internet (r)evolution leads to take fully into account two new kinds of data. The **first** ones have been (see supra 3) described as *identifiers* or, more precisely, as "**matching identifiers**", since these data have as main role to permit the cross matching of data belonging to various databases in order notably to profile the individual behind the data collected. Furthermore, we need to underline the dangers of using the same digital identity in several areas of our online life. It is clear that, most often, the same identification method or access key is used in different databases with as a result that our data can be cross-referenced more easily. From that point of view, these matching identifiers might be considered as quite sensitive data even if they are not always linked with an identified or identifiable individual, but with an object, like e.g. cookies which are linked with a session at our hard disks or like a tag number which is connected with the thing wherein the tag is embedded. Overall, the sharing of this identifying data by those who collect it, raises the question of how to handle correctly the data within a given context (see supra 10). Furthermore these data permit to their users to trace individuals even if not identified. They make possible to follow their movements and contributes to a continuous observation of the people.

    Another kind of data seems more and more relevant in our information society. **Contact data** are used in order to allow data controllers to enter into contact with the data subjects. On that point it might be interesting to underline how mobile phones will be more and more used in connection with ambient intelligence systems for sending appropriate messages like advertisement but also, at their customers' request, services linked with their precise location. So, contact data authorize their data processors to take immediate decisions against the person identified by this contact data. Definitively the nature of personal data might be discussed and we know that certain jurisdictions are reluctant to consider certain of these data as personal data since for instance IP addresses might not be linked *a priori* or *a posteriori* to an individual characterized by his name or by other traditional signs of identity. Let us take another example. In a large

supermarket, a customer is walking along the shelves with his or her trolley equipped with both a RFID tag (sender and reader) and a small video screen. Combined with the presence of products equipped also with RFID tags, the RFID system reveals at each moment the products purchased by the customer, as well as his or her precise location in the store, and is able to send the appropriate advertisement according to these data. If the RFID is embedded not in a shopping card but directly in the trolley, the store has no indication as regards the name of the person who is conducting the trolley but does not need anyway this knowledge in order to elect the "adequate" advertisement. Definitively, as it is the case with cookies, the information system is conceived in such a way to take decisions towards individuals.

19. The simple fact that these data are used to take decisions against an individual in function of his/her profile or his/her belonging of a thing seems sufficient to require a specific protection against their use. In its famous opinion on the concept of personal data[4], Article 29 Working Party makes a distinction between data related to individuals by their content, by their purpose and by the result of their processing. The last category seems to match with the problem at stake. We quote the Working Party: "*Despite the absence of a "content" or "purpose" element, data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. It should be noted that it is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data*". This third category does represent a shift as regards the notion of personal data since it does not refer to the nature of the data, as it was the case under Directive 95/46/EC, but only to the potential impact that the use of data collected about an object in possession of an individual not necessarily identifiable might have towards an individual, through the characteristics of the information system in use. So what is at stake is no longer the data but the technical possibility to contact a person X in order to have an impact on his or her rights or interests. Definitively to identify a person is not anymore a prerequisite for data processing affecting him or her. A single identifier and a contact point are sufficient. .
20. To be complete, it must be added that these two new categories: identifiers and contact data are not separated, but that certain overlapping might exist between both categories. So, data like an e-mail address or a RFID tag number belong to the three categories, since they might reveal our name, but also serve as identifiers, and finally they might be used in order to send messages to the individual in possession of the e-mail address or the RFID tag. What becomes obvious in our modern societies is that the data of the two last categories must be considered in many contexts as sensitive, since as regards the "matching identifiers" they permit to a large scale to aggregate data belonging to the same individuals and thus to "profile" them very precisely and must be regulated as such on the same basis than our data protection legislation are regulating medical, sexual, philosophical or political data.

b. Compatibility means the absolute respect of the context

21. As previously said (supra 10), one of the most problematic issues of the development of new infrastructures and platforms offering services of all kinds is the question of

[4] Working Paper 4/2007 on the concept of personal data, WP n° 136 (June 20, 2007).

compatible uses of all the data generated by their use. That statement calls for the development of adequate solutions including through self- or public regulatory measures as regards the possibility for gatekeepers to collect the different uses of their services. On that point, it might be recalled the severe limitations imposed under e-Privacy Directive to public e-communications services providers as regards the processing of location and traffic data. Perhaps certain limitations of that kind could be envisaged as regards these gatekeepers in order to limit their use of the data there are collecting through their services.

c. Consent never might be a panacea for legitimating all kinds of processing.

22. 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. 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.

23. The argument, making of personal data the alienable property or commodity of the data subject or subject to contract (sort of licensing contract) is disputable. It suffices to recall that under the EU Directive, consent, as defined by the article 2.h) of the Directive is not presented as a completely sufficient basis for legitimating processing. In any case - even in case of unambiguous consent - it may still 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. The information asymmetry and thus power inequality (see point 9), are disadvantageous to the data subject or 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 arguments refers to the difficulty, for the consenting data subject, to keep track of personal data in secondary transfers and to verify to what extent these secondary transfers are respecting the conditions of the initial license given by the data subject.

24. Some of those 'weaknesses of consent' could be remedied, as it 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 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. Another suggestion might be found by placing the consent in the

context of a **collective negotiation** between data subjects and the data controllers. Recently a web 2.0 platform has initiated a discussion about its "terms of use" and "privacy policy" with their users and has modified certain provisions according with the outcomes of the discussion. This collective negotiation seems to be a more legitimate ground than an individual consent. The e-commerce Directive dated from June 2000 might be given as a support to this collective discussion insofar it promotes codes of conduct negotiated with consumers, when their interest is at stake. Why not to extend this statement derived from consumer's protection to privacy protection (see infra)?

d. Reciprocal benefits' principle ought to lead to more effective rights for the data subjects

25. This principle would make it a statutory obligation, wherever possible, for those who use new technologies to develop their professional activities in order to accept certain additional requirements to re-establish the traditional balance between the parties concerned. The justification is simple – if technology increases the capacity to accumulate, process and communicate information on others and facilitates transactions and administrative operations, it is essential that it should also be configured and used to ensure that data subjects, whether as citizens or consumers, enjoy a proportionate benefit from these advances. Several recent provisions have drawn on the proportionality requirement to oblige those who use technologies to make them available for users to enforce their interests and rights. . It is even possible to imagine that certain of the rights associated with data protection, such as the right to information, the rights of access and rectification and the right to appeal, might soon be enforced electronically. In most of interactive Internet applications, a right to access might be provided through the same electronic devices than that used for collecting data including with a priori non personal data like cookies or Tag number. Many applications could be proposed: so, it should be possible to apply data subjects' right to information at any time through a simple click (or more generally a simple electronic and immediate action) offering access to the privacy policy, which should be mandatory placed and accessible through user-friendly means on the website and must be as detailed and complete as the greatly reduced cost of electronic dissemination allows. Such a step must be anonymous as far as the page server is concerned, to avoid any risk of creating files on "privacy concerned" users. We might think also to the data controller's obligation to provide a hyperlink to the notification of his processing to the Data Protection authority. Another application of this principle might be found in the obligation for companies who are using "profiles" to provide an automated access for data subjects to the profile they are deemed to comply with (see infra,).

B. Second step: Beyond data protection – New actors and new objects to be regulated.

a. Terminals must be privacy compliant and, by default, must be privacy friendly. Their functioning must be transparent

26. Directive 95/46/EC takes only into account the relationship between data controller and data subjects and has no consideration at all about the technical features embedded into the functioning of our modern networks and the risks linked with them. This functioning leads to new privacy threats, for instance through invisible hyperlinks, cookies or spyware, automated generation of identifiers or "transclusive" links like

those provided by Google analytics. The intervention of not trusted third parties during the communication sessions between data subjects and data controllers are another reality we definitively ought to consider. Progressively, the Data Protection Authorities became conscious of these threats entailed by Internet communications hardware and software. Since its Recommendation 1/99, Article 29 Working Party has clearly established the principle that software and hardware industry products should provide the necessary tools to comply with EU data protection rules. These considerations plead in favour of granting a new privacy right:: the "right to a privacy compliant terminal" including the "right to a terminal with a transparent and mastered functioning by its user". That new right encompasses different facets, such as the right to have at disposal a terminal programmed by default to minimize the data sent and received to the strict minimum needed for achieving the purposes pursued by its user is a first facet. It includes that the data generated, stored and transmitted by the terminal will be reduced to what is technically necessary for ensuring the telecommunication services used (data minimization).

The transparent functioning of the terminal equipment imposes that the terminal may not initiate a communication unless required by the user to do so, or unless it is strictly necessary for the adequate functioning of the communication networks or services (suppression of data chattering). The user ought to know what is entering into, and what is going out from his or her terminal. In this way, the user should be able to know, through a clear and easy method, the extent to which his computer chatters on about him, what information is sent or received, who is doing his sending and receiving, and what use will be made of this information. To this end, a data log would seem to be a technique that is both appropriate and relatively easy to implement. Terminal equipments' interfaces must clearly and permanently indicate if its user is currently identified or identifiable by another party. In order to minimize the risk linked with common identifiers and contact points, it would be desirable that the identifiers generated by the terminal would be both as less persistent as possible and, if possible, independent from each other towards the different data controllers. The rights of the user not to be submitted to unsolicited communications and advertisements, to refuse any intrusion into his or her terminal and finally to have the means to personally audit the privacy compliant functioning of his or her terminal are other facets contributing to ensure the right of self-determination of the citizens.

27. This assertion will progressively be extended through different steps. The first one is the support the EU Commission gave by its Recommendation dated from 2007 to Privacy Enhancing Technologies (PETs). As we know, PETs include all kinds of information and communication technologies that strengthen the protection of individuals' private life in an information system by preventing unnecessary or unlawful processing of personal data, or by offering tools and controls to enhance the individual's control over his/her personal data. As progressively asserted, PETs should be part of the architecture of the information system, right from the start. In this phase, the functional design is further elaborated and detailed in a more technical sense. An important aspect is that the technical design of the PETs option must be integrated in the complete technical design of the information system.

b. New liabilities for new actors: from PETS to Privacy Impact assessment

28. The second one might be characterized by the increasing demand of Data Protection Authorities to impose certain liability on terminal equipment manufacturers and

information systems designers, as the RFID case illustrates. How can the data be properly protected if technical solutions do not take into account present-day constraints and do not transpose them efficiently into regulation? For instance, regarding the case of RFID again, do we agree with the Article 29 Working Party[5] and with the EU Commission Recommendations that a person carrying a chip should be duly informed about the presence of these tags and be able to deactivate them easily, and that transmissions should be protected cryptographically? This approach, called "Privacy by Design", is based on some early thinking in the area first framed in French law in 1978 and recalled by the Recital 2 of the EU Directive 95/46: "*Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties*". Based on this text, Data Protection Authorities have consistently confirmed the principle that the responsibility for protecting the data of any users lies with the suppliers of terminal equipment and those creating the infrastructures, as they are responsible for the risk they are creating. In that context and precisely to measure the risks linked with the dissemination of RFID and its use, the RFID Commission's recommendations are going a step ahead by imposing on the operators an obligation to "*conduct systematically an assessment of the applications, implementation for the protection of privacy* ***and*** *data protection, including whether the application could be used to monitor an individual. The level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application; take appropriate technical and organisational measures to ensure the protection of personal data* ***and*** *privacy; designate a person or group of persons responsible for a continuous assessment…; make available the assessment to the competent authority at least six weeks before the deployment of the application; (…)*". This obligation to produce a 'Technology Assessment' on privacy risks and to make this assessment publicly and individually available constitutes, in our opinion, the first regulatory assertion of the necessity to take fully into account, as of the early stage of conception of an equipment, the privacy risks linked with the deployment of information systems. It is quite interesting to see how this obligation will be enlarged to all invasive and ubiquitous technologies which will characterize our future Information Society.

c. Profiling methods must be regulated according to the specific risks they are raising

29. The risks linked with these activities might be identified as follows. Firstly, the process results in attributing certain characteristics to an individual derived from the probability (dogma of statistical truth) that he or she belongs to a group and not from data communicated or collected about him or her. Secondly, the process is to a large extent unknown for the individual, who never might imagine the logic behind the decision taken towards him or her. Thirdly, the use of profiling for detecting potential infringers induces a reversal of the burden of the proof. Fourthly, it creates some risks of discrimination, and even threats to social justice, since certain consequences are attached to the meaning of the profile. Amazon's "adaptive pricing" system is often quoted in that perspective. This system permitted to adapt prices in function of certain *a priori* characteristics of the detected profile of the customers. Opportunities are so offered to the processor to have an automated judgment by considering not the

[5] *Working paper on the questions of data protection posed by RFID technology*, January 19, 2005, WP No. 105 available on the European Commission website: http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf.

individual but the profile that person belongs to. "*Profiling burdens those in the proxy class when the social meaning of the profile expresses denigration of the group defined by the proxy trait but the persons in the proxy group need to prove either that they are actually injured psychologically by the stigmatizing meaning or that they individually interpret the social meaning of the profile denigrates those in the proxy class. This requires them to show that the reasonable person familiar with our culture and traditions would understand the practice to have this meaning*".[6]

30. Article 15 of the 95/46 Data Protection Directive is applicable only to certain profiling systems. It grants to everyone "*a right not to be subject to a decision which produces legal effects concerning him or significantly and which is based only on automated processing of data intended to evaluate certain personal aspects relating to him*".[7] Definitively, this article is not applicable to all the profiling systems as most of them are not affecting our legal rights and have no significant legal or financial consequences. Furthermore, it is not applicable to systems functioning without identifying or making identifiable people. Nevertheless, we do consider that liberties would be jeopardized if there were no regulation at all as regards these methods of processing. Privacy is an issue which goes broadly beyond data protection. This concept means to provide the conditions of informational self determination. In our ubiquitous Information Society functioning on opaque profiling systems notably with ambient intelligence systems, privacy ought to mean equality of arms and due process and imposes that the person to whom profiling systems are applied must be aware of the existence of these systems, must have knowledge of their logic and must have the possibility to contest the accuracy and the applicability of these profiles. Privacy, except in cases where there are other prominent public or private interests, implies in our opinion the right not to be profiled without consent. On that point, as regards marketing profiling at least, an additional argument might be the found in the regulation of spam. By prohibiting illegitimate sending of unsolicited e-mails, the public authorities intend to limit undue influence on the individuals by those who have knowledge and make exercise undue influence through that knowledge and the facilities linked to the use of ICT.. This argument used for justifying the spamming opt-in system might be taken again to submit to authorisation the on-line behavioural advertising, what GONSALEZ and GUTWIRTH call "unsolicited adjustments".

31. Which rules might be developed as regards profiling techniques? I indicate just certain avenues for regulating without pretending to be exhaustive. The first right to be asserted definitively ought to be the right to be informed about the fact that certain messages have been sent according to a profile. Recently, Google has launched a new marketing approach construed on profiling methods. It is interesting to underline that this company has meanwhile recognised an automated and seamless right for people to refuse that this method will be applied to them and provided a right to access to the criteria used in that context, allowing to each user the possibility to correct the profile, to suppress or to add certain criteria of his or her profile. We are convinced that these rights must be extended for all marketing systems using profiling techniques. Another point must be the refusal to process sensitive data as criteria of profiling or as result of the profiling.

---

[6] D.HELLMAN, « Classification and fair treatment : an essay on the Moral and Legal Permissibility of Profiling », *Univ. of Maryland School of Law, Working Research Paper n° 2003-04,* available at: http://www.ssrn.com/abstract=456460

[7] This article needs to be interpreted in regard of Article 12 about the right of access. This article provides that the data subject has the right to obtain from the data controller the logic involved into any automatic system referred to in Article 15 (1).

III. Two additional reflections

32. Curiously the concerns expressed by the huge and unlimited development of our Information Society might found an answer in two traditional Human rights enacted by the article 8 of the EHCR and closely linked with or even embedded into the right to privacy: the inviolability of the domicile and the secrecy of correspondence. Beyond that, second reflection, it has to be asserted that more and more Privacy protection might be easily obtained by developing synergies with other fields of the legal system. In that perspective I will consider how consumers' protection legislation and criminal law might be allies for privacy advocates.

a. The protection of virtual domicile and correspondence: flying back to the initial sense of the Article 8 EHCR.

33. A regards a modern version of the inviolability of the domicile, the argument might be derived directly from Article 5.3 of the E-Privacy Directive, which considers our terminal equipment as a kind of virtual "domicile" to be protected like a physical one and submits to authorisation any intrusion in the user's terminal equipment. A recent German Constitutional Court decision interprets in a same quite revolutionary way the Article 8 of the Council of Europe Convention. Shortly, it might be asserted that starting from the Recitals of the E-Privacy Directive and a recent German Constitutional Court decision dated from February the 27th of 2009[8], new privacy principles as regards the functioning of our terminal equipments might be proposed. Indeed, Recital 24 does suggest an interesting comparison between the terminal equipment of a user and a private sphere similar to the domicile requiring protection under the European Convention for the Protection of Human Rights and fundamental freedoms. Any intrusion into the electronic domicile through spyware, web bugs, hidden identifiers like cookies or other similar devices, ought to be considered a violation of the private electronic space (virtual domicile), that could even be viewed as a form of hacking punished by criminal provisions. The provision clearly focuses on protection against intrusion mechanisms irrespective of the fact that personal data are processed or not through these mechanisms. This legitimate expectation of not being observed through opaque systems of surveillance has to be ensured by a new right to confidentiality and integrity of information systems, which more or less translates in our modern Information Society the right of inviolability of the home enacted also by the same Council of Europe Convention's provision, although "*the interests protected by this traditional fundamental right are constituted by the spatial sphere in which private life takes place*". This new right is indeed independent of all precise physical location and is not limited, as the traditional one, to a physical space, but its enactment does correspond to the same philosophy as the inviolability of the home.

---

[8] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html. About this decision, see G. HORNUNG, „Ein neues Gründrecht", *Computer und Recht*,2008, pp. 299 and ff. and G. HORNUNG and C. SCHNABEL, „Data protection in Germany II: Recent decisions on on-line searching of computers, automatic number plate recognition and data retention", *CL&SR*, 2009, pp. 114 and ff. See also on that decision, in the present book the contribution signed by R. BENDRATH, G. HORNUNG and A. PFITZMANN, "Surveillance in Germany: strategies and Counterstrategies".

34. The second point consists of asserting that the secrecy of electronic communications must be placed on equal footing with the secrecy of traditional correspondence, like postal mails. Whilst nobody does contest the fact that our correspondence might not be intercepted or read by third party except the designated recipient, it is curious that our electronic communications through for example Web 2.0 platforms, going through electronic mail service providers or simply created by our visits to web sites might be analysed, used and even transferred by these platforms, these service providers or by these web sites without our explicit consent.

b. Calling for new synergies.

35. Secrecy of correspondence is traditionally protected by criminal law. In the same time, identity theft constitutes an infringement of diverse criminal provisions. Intrusion into terminal equipment constitutes an illegal access to a computer systems punished as "hacking" by criminal sanctions. How not to see there opportunities for privacy advocates of additional legal ways for protecting privacy? Undoubtedly it is a matter of fact that synergies with specialists of criminal law might be developed in a time where a global consensus seems to be found around the 2001 Council of Europe Convention about cybercrime ratified notably by Japan and US. Furthermore the Convention sets up an international cooperation between law enforcement agencies which might of certain help for the effectiveness of our privacy regulations.

36. The same synergy might be elaborated with Consumer's protection legislations and associations. As already demonstrated, besides Human rights questions, the development of numerous ICT applications raises serious concerns as regards the consumers' interests. The economy of Internet broadly is based on publicity resources and the technologies in action do maximise the impact of that publicity by giving the advertisers the means of one to one advertising by using the automated analysis of consumers' behaviours. The profiling methods already described, the multiplication of traces created by our use of interactive and highly personalized services and finally the size of certain companies working into different domains of activities and thus able to cross data generated in different contexts justify these concerns and creates the fear of an exploitation more and more acute of the consumers' choices and of their data put on the web (list of friends, hobbies, holiday pictures, etc.). Consumer protection legislations might offer in that context to privacy advocates additional ways to get solutions to a certain extent more effective than those derived from the data protection legislations. So on line behavioural advertising might constitute in certain cases unfair commercial practices. The non respect of a privacy policy might be judged as a deceptive statement making the company liable. Class actions traditional in the consumer protection world are unknown by the data protection legislation. Spamming does constitute an infringement to consumer law as also to data protection. Statutory damages might be obtained under consumer legislation, etc. The interest of that convergence is demonstrated by the noticeable action of the US Federal Trade Commission. Despite the fact that no US data protection exist, this jurisdiction has developed important actions as regards privacy protection and its recommendations or decisions about RFID, on line behavioural advertising and in general non respect of privacy statements have to be considered as models even in European Union. That is why synergy between data Protection authorities and consumer's associations has to be encouraged.

Conclusions

37. Until now, as asserted supra n°8, the predominant view, at least in Europe, is to consider privacy as the most adequate and relevant concept to ensure an appropriate protection of human dignity, of fundamental rights and liberties. In fact, the challenge posed by new technologies is more serious than the weakening the effectiveness of privacy protection instruments: we have reached a stage where new technologies call into question the very foundations of privacy and ultimately the position of the subject in the new information era. What we need is definitively to renew our approach by considering more intensively the anthropologic and societal impacts of technologies. On that basis, we might conclude by two fundamental observations as regards the relationships between Privacy and Data Protection.

    - The first one is that the development of technologies have conducted to unprecedented privacy challenges, that our traditional data protection legislation are unable to face. Definitively we have to enlarge our considerations and take fully into considerations the values which are enacted by the privacy concept. It is quite interesting to see how the German Constitutional Court repeatedly refers directly to the Dignity and self-development principles to justify the recognition of new rights. **Definitively, (personal) data protection in the sense of the article 8 of the EU Charter on fundamental rights does not exhaust the privacy values.**
    - In that context we have already criticized the risk we take by distinguishing, as does the EU Charter, the right to privacy from the right to data protection without seeing that the second one is just a tool for ensuring the first one. If we are not doing that, we will be unable to cover the risks linked with profiling activities and the use of non-personal data. We will be unable to ground regulations of operators which are not data controllers and thus not under the obligations imposed by Directive 95/46/EC, and we will miss what is fundamental, meaning the regulation of the infrastructure and of terminal equipment.

    On these two aspects, the E-Privacy Directive in course of revision indicates the right way by not hesitating to propose new objects, new data and new actors to be regulated. Moreover, as an indication of the need to come back to the very fundamental roots and values of privacy, it is not astonishing that our reflections have led us to come back to an interpretation of the wording used in 1950 when we have spoken about electronic communication as correspondence and home as "virtual" home designating so our terminal equipments. In other words, we have to come back to the Privacy concept as construed by the courageous and quite innovative interpretation of the Court of Strasbourg (see notably the Pretty case).

38. If Technology is viewed as the major challenge for our privacy, it might also be the solution. The role of technology must be reassessed and new research efforts should be devoted in computer science to the design of future "privacy aware systems". With traditional Privacy Enhancing Tools (PETs), technologies are used to enhance "user empowerment", for example by providing means to ensure that the subject can hide his personal data (or encrypt them) or by offering guarantees for the express consent of the user through computer facilities such as software agents. But technologies might also be used in direct or indirect relationships with law, either by enforcing or facilitating the compliance of controllers with their legal commitments, by developing a policy for the standardisation of terminal equipments which takes into consideration privacy requirements, by providing auditing techniques for labelling authorities, by facilitating

the attribution of liabilities in case of litigation and, finally, in relationship with social uses, by defining architectures for reinforcing negotiation or for adopting collective privacy statements, notably in the context of Web 2.0 platforms, what we call P5P (Peer to Peer Platforms for Privacy Preferences).

39. In conclusion, we see that the law cannot attempt to solve all the problems. As far as data protection is concerned, the law must look to other methods of regulation, more particularly to the place of regulation through the technology itself. As we noted in the conclusions of the MIAUCE Report[9]: *"Time has come for the law to also seek the help of technology to ensure that the same instruments aimed at observing persons and events (for purposes ranging from safety or security, to marketing and entertainment; through technologies involving observation and/or interaction and/or profiling) do not disproportionately and illegitimately deny individuals' adequate protection of their fundamental rights and liberties"*. The above-described RFID case has demonstrated the importance to assign new duties and obligations for terminal equipment providers, the obligation to conduct a 'privacy technology assessment' and a new role for the State; i.e. a duty to create the conditions for a public debate on the technologies and their impact on our citizenship. **One major question we have to address, considering the way in which our society is definitively and deeply transformed by all these surrounding technological applications and their inherent normativities, is how to conciliate the individualistic approach inherent to human rights and their collective dimension in a democratic state.** Along the same lines, one may analyse to what extent democracy is at stake when we are speaking about privacy protection. On that point, perhaps the parallel with environmental laws (precaution principle, multi-stakeholders' discussion, governance, need for technology assessment) would be appropriate. How far can this comparison be pushed forward? How to ground this parallelism? And what practical lessons can be drawn for privacy protection? There are many questions to be solved rapidly if we want to renew in an appropriate way our reflections on Privacy in our modern Information Society.

40. All these considerations lead to a last point but definitively not the least one; we urge data protection authority to reconsider their role. They are not acting only as a jurisdiction by applying a specific legislation which would be considered as a dogma for them. Such an attitude would mean a closure vis-à-vis any other analysis. At the contrary, it is asked to these authorities to courageously face the reality, to enter into contact with all stakeholders and to take fully their responsibilities by creating discussions about the new features of our constantly evolving Information Society and their impact about our liberties including beyond the legislation at the basis of their setting-up. The answer they and we jointly have to address is not only: "Where Internet is going to?" but rather "We, citizens or rather netizens, where are we going to?"

[9] M. CORNELIS, D.DARQUENNES, N.GRANDJEAN, C.LOBET-MARIS, Y. POULLET, A. ROUVROY, *Miauce, Deliverable D5.1.2. Ethical, legal and social issues,* available online on the MIAUCE website: www.miauce.org.