Data protection legislation

Poullet, Yves

Published in:
Computer Law and Security Review

Publication date:
2009

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

available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Data protection legislation: What is at stake for our society and democracy?☆

Yves Poullet

Centre for Information and Law (CRID), University of Namur, Belgium

Keywords:
Privacy
Data protection
Social networks
Web 2.0
Profiling
Terminal equipment
Proportionality
Opacity
Informational self-determination
Semantic Web
Digital identities
Ubiquitous computing
Ambient intelligence
Data Protection Authority

ABSTRACT

The author starts by questioning the main privacy challenges raised by our present and future information society viewed as a "global village". Apart from a comparison with the traditional village of our parents, he identifies the two complementary and not dissociable facets of our privacy: the right to seclusion and the right to participate fully in our society. According to the first German Constitutional Court recognizing the right to informational self-determination as a new constitutional right, he underlines the need to analyse the data protection as a tool for ensuring both the citizens' dignity and our democracy.

The second part describes the three major changes of our technological environment: firstly, the tremendous and continuous growth of capacity of our information and communication systems; secondly, the Internet revolution with Web 2.0, the multiplication of digital identities and the convergence of all infrastructures and, finally, the ubiquitous computing. That evolution generates new privacy threats. In order to face correctly these new privacy risks, the author suggests the adaptation of our privacy legislation. Most notably, he proposes the adoption of certain principles available in environmental regulation, viz. the strong liability both of terminal equipment producers and of the infrastructure operators.

The final chapter addresses three caveats to the data protection lawyers. Please, stop acting only like a lawyer. Open your mind. The information society needs a 'Technology Assessment' approach and better attention to the solution the technology itself might offer. Finally, the author underlines the absolute need to come back to the two keywords of the data protection legislation: transparency and proportionality and to take fully into consideration the way by which the technology might enhance the efficiency of those principles.

1. Introduction

1.1. *The information society: some questions*

Information about us is circulating everywhere on the web of today's communication network. More than 1.5 billion people use e-mail. Mobile phone use is surging forward and tomorrow's technology will combine mobile phones, computers and televisions. The average single European is listed in around 500 different data files. Seeing these numbers raises a certain number of questions.

- **What information is circulating about us?** We can guess some of it, but some we know nothing about! The methods

☆ This article has been written in the context of the MIAUCE project (Multi-modal Interactions Analysis and exploration of Users within a Controlled Environment (www.miauce.org) IST Call 5, FP6-2005-IST-5).

0267-3649/$ – see front matter © 2009 Prof Yves Poullet. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2009.03.008

of collecting data have multiplied – CCTV, Radio Frequency Identifiers (RFIDs) which can be read at distance, through mobile phones[1] for example; other information we ourselves supply such as what I place in FACEBOOK, traffic and tracking information, my fingerprints, the DNA of my dog, my keyword searches on my preferred search engine, and how my eyes move.[2]

- **Who processes this information?** We immediately think of our banker, insurer, our employer, or the various levels of government and their departments; this is obvious, but how many others are spying on us? One company keeping an eye on us is Cyber Click, a cyber marketing company that operates by placing cookies on your computer when you visit one of their client's sites. This company, recently purchased by Google, collects information through the cookies placed on the hard disk and establishes a consumer profile and then adapts and personalizes the publicity banners.[3]

  Simple membership in social networks like LINKELDEN, MY SPACE or FACEBOOK permits far removed ''friends'' to use the information available on us in unsuspected ways or for companies to see our chain of friendships and use this to unanticipated commercial ends.
- … **and to do what?** Here too, some of the uses of the information are clear, or perhaps only apparently so; in other cases, it is less clear. Who would have thought that Amazon, the well-known American online bookseller, would create programs for ''adaptive pricing'', that is, book prices that change automatically depending on the demand of their clients, calculated by sophisticated formulas incorporating client profiles. RFID technology[4] in employees clothing can certainly help to easily and accurately ''clock in'' workers, but the same technology can also be used to follow the movements of employees throughout the day and underline where and when the movements are not ideal from the employer's point of view – long breaks in the cafeteria…

1.2. *From paranoia to the global village*

Do not these questions lead inevitably certain a malaise or even paranoia? To this frightening thought, some will answer: openness is a virtue; in any case, what does an honest man have to fear. They compare the Internet to a traditional village. Don't we all live in a ''global village'',[5] surely an image to calm and reassure! Traditional village life was where everyone knew (almost) everyone else's business, and this was all to the good – wasn't it?

1.3. *The plan*

The first part of this paper will compare the two types of villages mentioned. It will be seen that it is a misleading comparison. The examination will find it difficult to blindly support the supposed universal benefits of transparency, proudly proclaimed by social networks such as LINKELDEN, MY SPACE or FACEBOOK.

Starting from this comparison, we can examine two aspects of private life and the dangers it encounters. Ideas borrowed from the American author Solove[6] regarding ''Big Brother'' and ''The Trial'' will help us in this.

The second part will describe some characteristics of the ongoing changes in ICT (information and

[1] It is possible to combine these different collecting methods. So apart from readers installed within mobiles, it is possible to detect the presence of a person close to an object where an RFID tag is enshrined. On the experiences developed in US and the debates raised by these combined technologies, read N. KING, «Direct Marketing, Mobile Phones and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices», *Federal Communications Law Journal*, March 2008, 2, Vol. 60, p. 229 and ff.

[2] In the context of the MIAUCE project, an application analysed precisely consists in the automated analysis of the face's expressions and emotions in order to detect the individual's reactions regarding TV programs collected through a webcam installed on an interactive WebTV.

[3] On that point, see 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, p. 395 et seq. (this author evokes a ''consumer myopia and badly informed''); J. COHEN, «Examined Lives: Informational Privacy and the Subject as Object», 52 *Stanford Law J.*, 2000, p. 1373 and ff.

[4] About that technology of the infinitively small, Y. POULLET, A. ROUVROY and D. DARQUENNES, The Law encounters communication and information technologies: the case of RFIDs, in *Identity, Privacy and New Technologies*, Special Issue, *International Journal of Intellectual Property Management*, 2008, pp. 372–395. Thanks to nanotechnologies, terminal equipment, i.e. the micro-processor which, depending on the occasion, collects, processes, emits or receives data or external communications, and sometimes is limited to one or the other of these operations, may see its size reduced to the breadth of a pinhead or a grain of sand, so much so that one can speak of «Smart Dust». These developments lead to the possibility of largely invisible interactions between 'things' (the computer mouse, goods, clothing, etc.) or people on whom these microprocessors and information systems have been implanted, based on information so collected and other information. This interaction will help the individuals carrying these devices in their everyday lives in doing their work or surveying their activities. All of these applications by which ''people will be surrounded by intelligent and interactive interfaces embedded in the everyday objects around us and an environment recognizing and responding to the presence of individuals in an invisible way'' has been described as ''ambient intelligence'' by the European Union.

[5] The «Global village» is a wording invented by Marshall McLuhan in his book: ''*The medium is the Message*'' in order to qualify the impact of the globalisation, the media and the ICT.

[6] D.J. SOLOVE, *The Digital Person*, New York University Press, New York and London, 2004.

communication technology). The global and convergent nature of these technologies and the almost infinite capacity of the networks raise questions about two other kinds of evolution.

The first arises from new programs and uses of the web that we find in the so-called Web 2.0, and in what is called the Semantic Web. The second underlines how information systems are ubiquitous, what some identify as the birth of ''ambient intelligence''. Two trends arise from this evolution: the first is the loss of the boundary between private and public space; the second is the supposed ''overall responsibility'' of each individual, which leads us to think about integrating some of the principles and concepts from environmental law into the law concerning ICT.

These reflections bring us to a third question regarding the necessity to rethink and perhaps reinvent our legislation to protect personal information if we want our liberties protected. We will see that the protection of our private lives is a necessary condition to secure our liberty, and even the survival of our democracy.

2. What does privacy mean? – lessons from Kafka and Orwell

2.1. *A misleading comparison to the traditional village*

2.1.1. *'Un'openness or opacity as a virtue*

Look at the comparison sketched out in the introduction. Does the global village function like a traditional village? We see that in a traditional village, the knowledge we have of one another is limited, a man's home is his castle. This private space is sacred. It is vital to allow me a place to recharge my batteries, away from prying eyes. In the same way, the law must protect my private communication with others. This preoccupation justifies the primary concept of our right to a private life, as inscribed in article 8 of European Convention of Human Rights in 1950.[7]

Moments of ''discretion, anonymity and solitude'' or ''escape and withdrawal''[8] are necessary for an individual to think about or to question their life, or to develop relationships with others. Love and friendship are not easily expressed in public; they require certain discretion and a selective privacy. In the traditional village, the role of the walls is to protect intimacy, to allow individuals the freedom to abandon their public personas and to be free in their private life. It is for this reason that the ''right to opacity'' is a necessary condition to find authenticity within oneself or in contact with others. The necessity to provide this opaqueness or reticence is explained by the need of people to have a place where their personality and person can develop.[9]

As we will see in the text that follows, this ''right to isolation'' is more necessary now than ever before in our contemporary society and fully justifies the need to put in place new legislative safeguards to protect this ''right to isolation'' given the technological and socio-political challenges of today.

2.1.2. *The virtue of opacity – bad mouthed and badly manhandled*

The need of each of us, to have a certain opaqueness to the information society when safely behind the walls of our home, is sorely tested today. Our walls no longer hide us.

We could cite the infrared surveillance equipment used by the police and military to detect movement inside buildings, but of much greater concern are ICTs that are much more invasive. For example, RFID chips, in our clothing, our consumer goods, and appliances (the smart fridge) or even our own bodies,[10] inform observers far removed from our homes. They use the network to detect the messages these chips send out, and can detect our actions: simply drinking our favourite juice, our level of stress waking up, or our movements. Another example, that is a little more obvious, is that any use of your web browser is logged by your ISP (Internet Service Provider). They can know which pages we visit, what information we looked for, or what products or services we are now or shortly planning to use.[11]

Finally, the example of Gmail, their server can identify all the keywords inside all our e-mails. In sum, we are constantly watched and spied upon in ways and in places that were previously inviolate.

[7] The original conception of the ''right to privacy'' deeply is linked with the principle of dignity and was considered as a condition of the free development of the personality: the protection and leads to protect the family and home intimacy and of the correspondence.

[8] R. GAVISON, «Privacy and the limits of Law», 89 *Yale Law Journal*, 1980, p. 433 and ff.

[9] On that point, read 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, p. 22 et seq.), J. COHEN («Examined Lives: Informational Privacy and the Subject as Object», 52 *Stanford Law Rev.*, 2000, p. 1373 and ff.) and H. NISSENBAUM («Privacy as contextual Integrity», 79 *George Washington Law Rev.*, 2004, p. 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*''.

[10] About RFID implant's body and medical applications, read the Opinion expressed by the European Group on Ethics and Science dated from March 5, 2005: ''*Ethical Aspects of ICT implants in human body*''.

[11] The question of consumers' surveillance and of their online behaviours' follow-up has been commented and analysed by the FTC (US Federal Trade Commission) in different reports: «*Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-regulatory Principles*», available on the FTC website: http://www.ftc.gov.bcp/ with the debate held on November 1 and 2, 2007 on the theme: «*Behavioral Advertising: Tracking, Targeting and Technology*». Voir également World Privacy Forum, *The Network Advertising Initiative: Falling at Consumer Protection and Self-regulation*, publié le 2 Nov. 2007 sur le site: http://www.worldprivacyforum.org. See also very recently (Jan. 13, 2009) the complaint addressed by the Center for Digital Democracy before the FTC. The FTC complaint provides valuable insight into the developing business practices of mobile advertising and who the industry players are in the U.S., and to some extent, internationally.

2.1.3. … the need to master our environment

A second difference from our traditional village is whether we control our image in daily life. We know, or suspect, that our comings and goings, late nights or early mornings, change of clothing or car, new job or job loss, are in the public domain and that the disagreeable neighbour or the friend who calls to congratulate us or to tell us of their problems are all ''in the know''. We can, based on this daily feedback, adapt and adjust our behaviour, play this role or that and hide certain choices. To this extent, we master our environment. However, what about in our global village? Do we have the same control? Absolutely not! Look for example at technologies such as ''one-to-one marketing'' or ''adaptive pricing''. Here the company based on our profile adjusts the price in line with their expectation of our interest to buy (adaptive pricing) or in the case of banner publicity change it (one-to-one marketing) in line with our buying behaviour. These systems are based on the use of profiling techniques that we look at next.

2.1.4. Profiling techniques

These techniques use statistical methods which cross-indexing randomly selected information from large databases (data warehouses) and deduce an individual's behaviour based on his membership in a group or, more precisely, his profile.[12]

In this way, collections of information from various sources and databases allow us to deduce with a certainty of 89% that purchases by such and such a consumer, at this or that grocery store, at that time, on that particular day, clearly indicates that the person is single, likes long distance travel, and may engage in fraud. The profile of the terrorist is deduced by cross-indexing information from various databases, the population roll, the use of credit cards, movements detected through use of mobile phones, brand name discount cards, use of medications, etc.[13] The drop in the cost of storing information, the level of sophistication of the analytical tools and the sheer processing power available on modern computers means that sorts and searches can find the correct profile (at least statistically) that can then be compared with the real information about the real individual. In short, the ''man in the street'' finds his profile based on data that has little connection to him and even less connection to the use made of this information and of whose existence he is largely ignorant.[14]

Worse still, this information provides the profiler a better understanding of the person concerned then the person has of themselves. If the person concerned rejects the profile or indicates that a decision based on it about him is wrong, it is up to the profiled person to prove the mistake.[15]

2.1.5. Social networks

After having read the 'privacy settings' of FACEBOOK or other social networks and understood the restrictions on the flow of information about us to our close friends we think we control our Internet profile. A quick reading of the 'privacy notices' on these sites will end our illusions. Advertising we receive because we are the friend of so and so, that we are supposed be interested in too, keeping our personal information on file after we have cancelled our contract; these are examples of how in fact we do not master the personal data out there about us.

2.1.6. Two sides or facets of privacy[16]

We see that the individual is more and more transparent and operates in the virtual world that is more and more opaque. In fact, this is how the Internet operates. It undermines our privacy which legislation is trying to protect. If legislation provides new rights of protection, it is because personal data protection is founded on our existing ideas of privacy. This legislation looks, firstly, to establish the right to intimacy or more generally the right to withdraw from society and, secondly, at the possibility to develop our capacities to choose. These two aspects of privacy are not incompatible, quite the opposite in fact. They both establish a common objective: to allow the individual fully to participate in social life. To reach this objective means that either the right to seclusion or rather the freedom not to be exposed (the right not to participate in the information society) is a necessary condition for the development of the individual.[17] This is in the sense that it allows independent thought and the right to choose a way of life and relationships with others and at the same time

[12] About these practices and the need to regulate them, J.M. DINANT, C. LAZARO, Y. POULLET, A. ROUVROY, ''*Profiling and Data Protection*'', Report addressed to the Convention 108 Consultative Committee, September 2008, available on the Council of Europe website. Voir également, l'excellent ouvrage rassemblant des articles sur le thème du profilage, édité par M. HILDEBRANDT et S. GUTWIRTH, *Profiling the European Citizen, Cross disciplinary Perspectives*, Springer Science, Dordrecht, 2008, pp. 303–344.

[13] On ''data mining'' applications developed by the public administrations especially for public security purposes, read D.J. SOLOVE, «Data Mining and The Security vs. Liberty Debate», 75 *University Chicago Law Review*, 2008, p. 343 and ff. The author pinpoints in particular the US MATRIX (*Multistate Anti-Terrorism Information Exchange*) program.

[14] M. HILDEBRANT, «Profiling and the Identity of the European Citizens», in *Profiling the European Citizens, Crossdisciplinary Perspectives*, M. HILDEBRANT and S. GUTWIRTH (eds), Dordrecht, Springer, 303–344.

[15] About the reversal of the evidence in profiling applications cases, D.J. STEINBOCK, Data Matching, Data Mining and Due Process, 40 *GA Law Rev* (2005), 1, p. 82 and ff.

[16] About that distinction between the two facets and their intrinsic linkage, A. ROUVROY and Y. POULLET, 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 Colloquium held at Brussels, Nov. 2007, Springer Verlag, 2009. See also but grounding the first facet on privacy and the second one on Data Protection, 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 al. (ed.), Interscientia, Antwerpen–Oxford, 2006, p. 74.

[17] See, in the same sense, 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.»

assures the right to fully participate in the information society while maintaining control of one's data profile and the manner in which it can be used.[18]

We see that the two possibilities are intimately linked – necessary and complementary – one to the other. The first is necessary to the second, in as much as it allows the individual to create both independence and identity so that his place in society (''privacy'' as a condition of liberty of expression) can be established as well as the respect of his rights. This is done by controlling the information flow (the control of information that others have) and assuring one's right to be secluded and anonymous – a feedback mechanism of the second right which reinforces the first. In other words, we can only be part of the information society in all serenity if we are able to have a minimum of opacity, a ''secret garden'', as a condition of our liberty (for example the possibility of remaining anonymous or use a screen name, or to have the capacity to simply to turn off the machine through which we can be located).

Both rights are at present suffering problems. Solove[6] uses two fictional characters from well-known novels to illustrate how technologies weaken our right of privacy and profoundly influence the relationship between the people who hold the information and the people who the information concerns.

2.2. *The information society: between Kafka's 'The Trial' and Orwell's 'Big Brother'*

2.2.1. *Big Brother*

The first character we will look at is Orwell's 'Big Brother' from the famous book ''1984''. This first reference shows the extent that those that control information have power over those concerned, whether they are citizens, employees or consumers; we are each more and more transparent to 'Big Brother' who looks to regulate our behaviour for our own good. For those who hold it, information is power. Whoever has information about others can adapt their decisions and actions in line with what they know or have deduced about them. He knows what to expect and can better respond to any expressed need or even reshape this if needed.

It is no doubt urgent to establish some new rights (we will come back to this point later); a certain balance of information control must be re-established if we do not wish to see those about whom this information is known reduced to mere objects. We are rightly concerned about the power that Google, or its affiliates, have or could have, in diverse domains.

We hesitate to imagine the knowledge Google, today's 'Big Brother', has already collected about each of us, collated, cross-referenced, and deduced from the combined use or non-use of their products and services. These include the search engine (Google Search Engine); e-mail service (Gmail); their online news services (Google News); their geographic service (Google Earth) and their online publicity services, developed by their subsidiary '.Double-click'. The latter, thanks to their invisible hyperlink technology, collect information about millions of users surfing on millions of sites connected to Double-click.

2.2.2. *The Trial*

The second case we can look at is 'The Trial' written by Franz Kafka in the sixties. The story concerns a character on trial for unspecified crimes, with nameless accusers, for unknown reasons. Here we can see how the systems surrounding us are completely opaque and obscure. We do not know what information is collected, for what purpose, who it is for, or how much there is of it. This situation of concealment can lead to certain fears and adopting normative behaviour in line with what we think 'others' expect of us. Psychologists have shown that behaviours are adaptive and when we know or think we know we are being watched, we no longer dare to express our natural joy or anger – no doubt suppressed to be expressed at another time and place, though not necessarily for the better.

2.3. *The decision of the German Constitutional Court regarding the 1983 census: the fundamental importance of privacy in our democracies*

2.3.1. *From the confirmation of the right to informational self-determination*

As with the case that Kafka denounces, one of the first decisions of the German Constitutional Court of 1983[19] asserts the right to data protection regarding personal data collected through the census, while unanimously approving the legislation organising the census arrangements. According to the Karlsruhe judges, the law contained serious errors and omissions: no clear definition of the objectives, no clear or transparent procedure for following or identifying inaccurate information regarding German citizens. These deficiencies constituted an attack on human dignity and the proper development of the person.[20] The German Court underlined the dangerous consequences to democracy if a closed and obscure system handles the information. In particular, it raised the point that individuals automatically and perhaps unconsciously self-censor their

[18] About this debate, A. ROUVROY, Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence, in *Studies in Ethics, Law, and Technology*, 2008, available at SSRN: http://ssrn.com/abstract=101.3984.

[19] BVerfG, Karlsruhe, Dec. 15, 1983, *EuGRZ*, 1983, p. 171 and ff. See comments by E.H. RIEDL, «New bearings in German Data Protection», *Human Rights Law Journal*, 1984, Vol. 5, no. 1, p. 67 and ff.; H. BURKERT, «Le judgement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses consequences», *Dr. Inf.*, 1985, p. 8 and ff. See also, E. BROUWER, *Digital Borders and Real Rights*, Nijmegen, Wolf Legal Pub., 2007, 501 pp.

[20] ''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 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.''

behaviour for fear of being considered as deviant or even simply eccentric by others.[21]

The court underlined the fear people have of the unfavourable consequences, should others know their behaviour. The court decided that (information) technology might "might destroy not only our chance to develop, but also the common good, because self-determination is a necessary condition to a free democratic society built on the capacity of its citizens to act and cooperate".

2.3.2. … on to democracy

In light of the preceding points, we must establish regulations to protect privacy and guarantee the protection of information. These measures are in fact necessary because they help individuals to keep and to develop the capacity to act independently or cooperate with others within society so that it can remain democratic, based on the mutual respect of differences and the free development of each individual.[22]

This decision of the German Constitutional Court has been followed, point for point, by another decision[23] taken by the same court, regarding a Lander's legislation, which allowed police entry into computers at distance. These two decisions show how the protection of privacy is a fundamental and necessary condition to the democratic process. What it implies is that a state that respects the development of each individual is a necessary condition for other democratic freedoms.[24] Can we imagine real freedom of expression if everyone feels that each of his or her actions and choices is observed? Can we imagine freedom of movement in a world where our mobile, with some help from RFID, follows our every move and constantly informs us of various events? Privacy, now protected through personal data protection legislation, thus becomes 'the' fundamental freedom, and the necessary condition for all other freedoms.

3. Some characteristics of recent new uses of information and communication technologies

3.1. *New technologies…new risks to privacy*

Asserting the importance of our private life leads us to look at characteristics of the new technology itself, to better understand the implications on our behaviour, our life, and our capacity for self-realization. The European Data Protection directives are intended to deal with the problems of processing, as we understood them in 1995.

Far be it for us to suggest that ideas established at the dawn of the Internet revolution, no longer provide a proper base to protect our liberties; however, the Internet revolution, convergence of communication technologies, increasing storage, computer capacity and ambient intelligence lead us to think about new approach or at least to examine additional possibilities to protect our privacy in today's world, which are both effective and adequate. No doubt, changes in technology are not the only considerations to take into account when looking at present-day risks. Contrary to what Lessig[25] suggests, changes in technology are not the only reason to revise our laws. Changes in socio-political circumstances, for example the horror of 9/11 and its aftermath, also create new

[21] "The possibility of inspection and of gaining influence has 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 citizen's 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 have 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.*"

[22] On that point, S. GUTWIRTH and P. DE HERT, "Regulating Profiling in a democratic constitutional State" in M. HILDEBRANT and S. GUTWIRTH, *Profiling the European Citizen, Cross disciplinary Perspectives*, Springer Science, Dordrecht, 2008.

[23] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1-333): http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (*MMR*, 2008, 303, annotated by Th. HOEREN, p. 366 and ff). That decision grants to the individual a new Constitutional right to the security and integrity in the use of Information System and does consider the respect to the integrity of the virtual home what constitutes the terminal equipment on the same footing than the physical home.

[24] The link between privacy as a condition for an expression free, original and full of respect of the differences, from one part, and the democracy, from the other part, is developed by number of authors. See notably, 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.

[25] L. LESSIG, *Code and other Laws of Cyberspace*, New York, Basic Book, 2000. For more reflection about the way by which new technologies, especially technologies of ambient intelligence, modify drastically our way of life and creates new risks of privacy threats, read A. ROUVROY, Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence, in *Studies in Ethics, Law, and Technology*, 2008, available at SSRN: http://ssrn.com/abstract=101.3984.

dangers for the self-determination of people,[26] and adapting legislation to protect personal information and the many facets of personal life can be critical in this regard. The laws respecting personal privacy and protecting personal data needs to be adapted to technological and social–political changes that threaten the conditions necessary for an individual to freely develop their personality.

3.2. *Three important changes*[27]

The development of information technology can be described chronologically along three aspects. Firstly, there is Moore's law. This describes the constant growth of the capacity of computers, user terminals and the communication infrastructure to which is added the seemingly limitless capacity of computer analysis. Secondly, we have the Internet revolution, which we can look at in three ways: the convergence of the network around a single interoperable platform, the appearance of the 'Semantic Web' and Web 2.0 and lastly, the changes in identification and authentication techniques. Thirdly, is a still more profound change, the emergence of ambient intelligence that takes technology and the network and puts that technology into our everyday life, the things around us, the places we go, the body we inhabit.

3.3. *Two induced tendencies*

These technological changes have created two important tendencies as regards our use of the web. The first underlines the privatisation of cyberspace where private corporations establish the technical norms but, equally, where access is only possible to those who have the necessary knowledge, and raising thus the question of access to the needed knowledge. The second observation concerns the global aspect of our actions on the Internet, and the way in which the functioning of our web access points and web infrastructure shape our behaviour and interactions. With this second point we see that service providers and computer manufacturers have some responsibility as concerns our communication environment and require our consideration if we wish to introduce or import into data protection legislation certain principles of environmental law.[28]

4. Three major changes[29]

4.1. *Improvements in the ability to store data, the raw power of calculation and transmission, as well as the user terminals themselves*

4.1.1. *Moore's law*

The first evolution concerns storage media. It is usual on that point to quote Moore's law, which states that memory capacity will double every 18 months [1000 times improvement in 15 years], while at the same time, cost for this improved capacity is reduced by 50%. In a study done for the Council of Europe,[30] regarding the problems associated with data protection we see: ''[it] has become and will continue to be easier and easier to record the life of every individual on the planet (our own and that of others…)''.

For example, we could look at the feasibility of recording every telephone call from Europe to the entire world. No small task as it would mean stocking the equivalent of 15 billion minutes of telephone conversation on an annual basis.[31] If we realize that we need approximately 10,000 bits per second to digitalize the voice, that we can compress the information by a factor of two (which is typical), we see that we need something like five terabytes to store 24 h of telephone traffic, easily feasible today with a system of disk arrays where each disk can store around 400 GB.

Furthermore, the average volume of these hundreds of thousands of simultaneous telephone communications equals approximately 0.5 GB per second, and can be carried easily on a single optical fibre the thickness of a human hair. Put another way it is entirely possible to have ALL telephone communications pass through a single tube of glass a few microns across.

At present, we find systems like the old ''Walkman'' but which are perfectly capable of recording the equivalent of several hundred CDs in MP3 format. Digital cameras today allow us to record hundreds even thousands of photos, cameras in the past were limited to 36 shots. This increase in storage capacity, the capacity of calculation and transmission simply is demonstrated each time Google works scanning in just a few seconds more than 500,000 sites in the world to answer your request.

4.1.2. *The users' terminals: from multifunction to miniaturisation*

A second evolution can be noted in user terminals. This change is on several fronts. Of course technical and functional, but it also concerns their regulation.

[26] So Judge POSNER justifies the multiple legislative attempts to Privacy by the necessity of the fight against terrorists and the imperatives of the public security (E.A. POSNER and A. VERMEULE, *Terror in the Balance: Security, Liberty and the Courts*, Oxford University Press, 2007).

[27] More on these evolutions might be found in Y. POULLET (with the cooperation of J.M. DINANT), ''The Internet and private Life in Europe: Risks and aspirations'', in A.T. KENYON and M. RICHARDSON (eds), *New dimensions in Privacy law, International and Comparative Perspectives*, Cambridge Univ. Press, p. 60 and ff.

[28] The interest to introduce the principle of the environmental law into the Internet law is developed *infra*, no. 5.2.1.

[29] For a more complete view on these trends, see Y. POULLET, A. ROUVROY, ''Introductory Remarks, General report'', *European Conference on Ethics and human rights in a Information Society*, Conference organized by UNESCO and Council of Europe, Strasbourg, 13–14 Sept., 2007 available at the UNESCO website.

[30] Y. POULLET and J.M. DINANT, «*Self-determination at Internet era. Some reflections on the Convention 108 regarding the future work of the Consultative Committee (T-PD)*», Report available on the Council of Europe website: http://www.coe.int.

[31] The figures have been calculated on the basis of an extrapolation of figures given by the International Telecommunication Union as regards the year 1999 (see: http://www.itu.int/ITU-D/ict/statistics/atglance/Eurostat 2001.pdf).

The term ''telecommunications terminal equipment'' (in this paper referred to as ''user terminal'') is defined in the European Directive on telecommunications terminal equipment[32] as ''a product enabling communication or a relevant component thereof which is intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks (that is to say, telecommunications networks used wholly or partly for the provision of publicly available telecommunications services)''. This broad definition includes not only personal computers, or other typical user terminals such as telephones (mobile or fixed), faxes, but equally RFID,[33] chip cards, and in the future, ''intelligent molecules''[34] implanted in people themselves.

What is interesting about the RFID, whose use is presently growing exponentially, is as much the miniaturisation, as the fact that it sticks to and associates the owner with an object and indirectly the behaviour of its owner. This raises the question of whether legislation on the protection of ''identifiable'' personal data is applicable.[35]

In addition to the point raised above, two others of interest can be raised relative to user terminals. Firstly, concerning the nature of the equipment, the technology has moved from electromechanical to programmable electronics. In other words, the operation of the user terminal is not dictated by the user,[36] but by the manufacturer of the terminal or by a third party that has inserted programs in the terminal to operate it from a distance (for example spyware or updates for programs in the computer system).[37] In fact, the user of the terminal only partially controls the computer; he does not initiate all the changes.

This lack of control by the user reflects a similar loss of control by the state in terms of control of production norms for these user terminals. Where previously the functioning and the design of the old ''voice telephony apparatus'' were entirely regulated, this is no longer the case as concerns the

[32] European Parliament and Council Directive 1999/5/EC of March 9 1999, on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, O.J., l 091, 4 April, 1999, p. 10 and ff.

[33] We in fact distinguish three types of RFIDs or tags and this according to the passivity or not of the device installed:

- *active* tags are equipped with an autonomous energy source (a battery or solar collector) and with a chip; they are only able to signal their presence and/or establish more elaborate dialogues with reading devices which are designed to receive the radio signals emitted by a tag; the cost of these tags is high ($20) even if their cost is constantly going down. Their lifespan is limited by the use of a battery;
- *semi-passive* tags do not establish communication with the reader but are nevertheless equipped with batteries which make it possible for the chip to store elements of a physical type, like temperature, pressure,… This type of tag is thus in general coupled with physical sensors, which are small wireless detectors useful in controlling environmental factors (for example controlling energy consumption). Their cost can range from $10 to 100 a piece;
- *passive* tags, which are the most widespread, are stimulated by electromagnetic induction (in fact by the wave emitted by the ''*forward Channel*'' reader) and in return emit a fixed alphanumerical sequence via well-defined radio frequencies (''*backward Channel*''). Since these tags do not contain batteries, their lifespan is unlimited. Their cost is minimal (from 20 cents to a few dollars); the cost being based on the sophistication of the chip (the memory size or the capacity for encoding).

[34] …through nanotechnologies or RFID tags. As regards health care, we also witness the implanting of radio-tags in humans (the Company 'Applied Digital Solutions' and its Verichip). These solutions can be very useful for certain categories of patients at risk (Alzheimer's, cardiovascular or diabetes sufferers), insofar as one can insert medical data considered urgent into the chip, thus allowing the problems which this emergency data reveals to be read off the chip remotely and, thus, intervention as needed for a patient unable to express himself. The recent report of the European Group on the Ethics and Technology already quoted accordingly describes many applications whose interest is obvious. Thus, an implant in the body of a patient with a chronic disease like diabetes makes it possible to remotely control via the telephone the state of the diabetic patient and even, within the context of an interactive RFID, to send him the impulses necessary for re-establishment of a compromised situation.

[35] The particularity of RFIDs consists in the fact that they introduce a bond between an object and information relative to that object (its temperature, its location, etc.); that object may be the human body. Surely, and this is the point, can one start from there and conclude to information relating to the owner of the object or a chip bearer and initiate certain medical treatments, advertising campaigns, etc., aimed at him? And yet, it is not necessary to know his identity or even seek it. What is essential is that that subject X, an RFID bearer, is at such a place, has made such a purchase, and has a valid ticket. In such cases, can one speak about data of a personal nature, within the meaning of article 2 a) of directive 1995/46/EC? The concept of identity is at the heart of this type of data's definition. No doubt, this definition is broad in that, as we are reminded by the Article 29 Working party in connection with cookies (Working Paper 4/2007 on the concept of personal data, WP no. 136 (June 20, 2007)) or RFIDs ((Working paper 5/2005 on questions of data protection posed by RFID technology, WP no. 105 (January 19, 2005), both texts are available on the Commission site: http://www.ec.europa.eu/justice_home/fsj/privacy)). The Working Party refers to preamble 26, 'identifiability' is conceived in terms of ''all the means liable, reasonably, to be set up, either by the data processor, or by another person, to identify the aforementioned person''. And since, as the group itself recognizes, the very breadth of this approach to the concept of data of a personal nature prevents its covering every case, it remains theoretical, for example, if those using the data provided by cookies or RFIDs don't seek to identify the person concerned but simply to profile a computer owner so as to decide on certain actions in his regard.

[36] About the opacity of the present functioning of our terminal equipments and the absolute need to ensure its transparent functioning by default, see on this criterion, see the reflections of Y. POULLET and J.M. DINANT in ''*Informational Self-determination in the Internet Era*'', Report on the Application of Data Protection Principles to Worldwide Telecommunications Networks, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg 12/13/2004, T-PD (2004) 04 final, available online on the Council of Europe's website.

[37] About these intrusive software, read http://www.clubic.com/actualite-21463-phishing-et-spyware-les-menaces-pesantes-de-2005.html. Let us recall that Art. 5.3 of the European Directive 2002/58/EC on e-privacy forbids these intrusion into the terminal equipment without the consent of its user.

technical norms and controls that guide computers and more broadly the terminal equipment's development.[38]

4.1.3. *Multifunctional user terminals and the convergence of networks*

A second characteristic is the ''multifunctionality'' available in most user terminals (personal computers of course but also 3G cell phones). The traditional division between media based on their function (telephone for voice; television for image and sound, etc.) is disappearing as all content is now digitalised[39] and with user terminals having multiple uses. This in turn allows the providers of service, or anyone involved in the supply, to propose certain sites, to use cross-platform formats of previously separate functions (so that on the same terminal equipment we use voice communications services, we listen to the radio, we send e-mails, we watch television,…).

4.2. *Internet evolution*

4.2.1. *Network convergence and worldwide participation*

The Internet revolution that we are all watching has several interesting aspects. We often insist on the global aspect of the interchange between people, without leaving our chair, enabling us to reach the four corners of the earth. The convergence of all the networks presently is discussed and new models of fourth generation interactive television are in course of implementation, leading to the final convergence of all networks/media/formats and the handling of our diverse communications that until now were carried through separate infrastructures.

4.2.2. *The Semantic Web*

Our reflections do not stop here. In order to offer a higher level of interoperability, a dialogue between different contents not even in the same format, and the possibility to understand messages sent, the web has become semantic.[40] Computers are creating metadata, that is, they are associating information that they store or send with this metadata to allow easier access for people or computers to access or analyse the information from a distance. Automated analysis of e-mail content is a good example of this new possibility. With this new ''intelligence'', information systems are capable of analyzing the content of various databases and do not require that the data has a predefined internal structure. We cannot overemphasize that the creation of these metadata markers, which allow us to find information through filters, keywords and conceptualisation, is inherent to the Semantic Web and has not been set in motion or even consciously used by the person we call the user, but rather is the result of automated operations carried out by the computer.

4.2.3. *Web 2.0*

Web 2.0 refers to a large variety of applications characterised by user participation in the creation and functioning of online sites. We are referring here to social networking sites, or encyclopaedias like 'Wikipedia' and content sharing sites like 'YouTube' or 'Dailymotion'. These kinds of uses raise new questions as regards the protection of personal data.[41] This is so, first, because these sites concern sometimes intimate details that are supplied willingly and actively by the users: emotions, the group of friends, and the events in their lives or the lives of others, their health; and second, because the information is about them and those close to them. Here we can see the web user in two roles that in the past were separate: from one site as data subject – the subject of the personal content posted on the Internet – and from the other site as data processor since web user might also be the generator of personal data posted on the website.

The program allows the service provider, but also third parties, firstly, to analyse the content and information placed on the site by the user, secondly, apart from this data and the multiple uses generated by this latter to profile him or her and thirdly to take advantage of the so-acquired knowledge including use outside of its original context.[42] Therefore, employers might well analyse available social networking material when evaluating a candidate for a particular job. We need to keep in mind that the web ''remembers'' events posted even only temporarily. Finally, it is troubling to see how ''private'' and ''public'' spheres are intermingled on these sites.

4.3. *Methods of identification and authentication*

4.3.1. *Digital identities: why?*

Another remarkable evolution on the Internet has come from the availability and use of identification and authentication methods of users on the net. These methods allow users to identify and to be identified or, with identity management systems, to allow access to informational resources or services. In addition, beyond this, it is possible to identify users with certainty and thereby add or deduce new information about them drawing on sources from all

[38] About the importance of these private standardisation bodies as W3C or IETF, read P. TRUDEL et al., *Droit du cyberspace*, Montréal, Themis, 1997, Book 3 and the critiques addressed to that privatisation, M.A. FROOMKIN, «Habermas@discourse.net: Towards a critical theory of Cyberspace», 116 *Harvard Law Rev.*, 1996, p. 800 and ff.

[39] So the standards JPEG for pictures, EFR for the voice, MPEG for moving images…

[40] On the future Semantic Web, see M. RUNDLE, *Ethical implications of emerging technologies in the Information Society*, UNESCO Publications, 2006. ''The *Semantic Web* is an evolving extension of the World Wide Web in which the semantics of information and services on the web are defined, making it possible for the web to understand and satisfy the requests of people and machines to use the web content. It derives from World Wide Web Consortium director Sir Tim Berners-Lee's vision of the Web as a universal medium for data, information, and knowledge exchange'' (http://en.wikipedia.org).

[41] About these issues, read notably, G. GONZALES FUSTER et S. GUTWIRTH, ''Privacy 2.0?'' *RDTI*, 2008, special issue, Web 2.0, pp. 351–379. See also the report and the recommendations of the International Working Group on data Protection in Telecommunications: *Report and Guidance on Privacy in Social Network Services, 'Rome Memorandum'*, 43rd meeting, Roma, March 2008.

[42] These diverse ''data aggregations'' and the privacy threats they generate are described by the HOGBEN report (HOGBEN (ed.), *Security Issues and Recommendations for Online Social Networks*, ENISA, Position Paper no. 1, Heraklion, Greece, Oct. 2007, p. 3 and ff.).

sites over the web with no concern for borders.[43] These ''digital identities'' are a kind of metadata that allow the cross-referencing of the individual's information available on different databases; in other words as matching identifiers. We need to underline the dangers of using the same digital identity in several areas of our online life. It is clear that the more often the same identification method or the same access key is used in different databases, the more easily our identity can be cross-referenced. We know for example that in certain countries, the national registration number is stored in all the governmental databases. This increases the possibility of cross-referencing the information and thus enhances the power of the state as regards the citizen. 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.[44] Overall, the sharing of this identifying data by those who collect it raises the question of how to handle correctly the data within the given context. We will come back to this point later when envisaging the principles of proportionality of the processing and of its content.[45]

4.3.2. *Digital identities: how?*

Finally, let us examine more closely the evolution of the nature of these digital identities. The primary digital identifiers are directly connected to the person, name, address, mobile phone number, passwords or electronic signatures; the secondary identifiers are indirect but are based on known information concerning the individual. ''Cookies'', IP addresses or RFID tag numbers, while not necessarily known to the individual, are associated with a site or object with which the person is connected, and these ID techniques are mastered and understood by the people or businesses that place them there. With biometric identification technology (iris, fingerprints, voice) identity and identifiability are reduced from a flesh and blood reality to just so much data. Here we note a certain evolution, as biometric information can concern an exterior physical trait or look more deeply at the genetic level of the individual. In the latter case, this genetic information can be used to follow the individual from cradle to grave. Contrary to other identification and identifiability data, this particular data cannot be controlled or erased by the person concerned.[46]

4.4. *Ambient intelligence: when and where the virtual world and the physical world meet*

4.4.1. *Real joining virtual connections: from GPS to RFID*

Before looking any further at possible connections between the virtual and real, we must pinpoint the impact of Global Positioning Systems (GPS). GPS assist the individuals wherever they may be (routing services, but also services to inform about the local environment, connected through a mobile phone). These systems permit to trace the movements of the object to which they are associated. The GSM technologies through more and more sophisticated design and their evolving generations also ensure the geographical follow-up of their users. These technologies connected with RFID readers or tags permit association of an individual to a specific object and therefore to send an appropriate message in the context of online ''behavioural advertising''. For instance, it will be possible to propose to the mobile user a short presentation of the movie presented at the cinema when he stops just in front of an RFID equipped affix presenting the film.[47] A reader located into the mobile will detect the presence of the affix and send a message to a marketing company that will send the appropriate images.

The ambient intelligence network allows many possibilities for connecting the real and virtual worlds. Their objective is to allow direct interaction between the person and their environment. This artificial intelligence, which present-day ICT allows, along with easy access to cyberspace, is now present in things, places, even our own bodies. According to the prophetic vision of the computer engineer Weiser,[48] the visible aspect of the technology disappears and it becomes simply ''normal'' i.e. totally integrated into our daily life. These technologies of ambient intelligence owe their development to the extreme miniaturisation of the user terminals (for example RFID, terminals the size of a grain of rice and various types of nanotechnology still in the early stages of development connected through their receptors and the Internet to various information systems). Possible applications are many and allow us, for example, to follow the movements of a consumer in the supermarket and permit a ''dialogue'' between the consumer's chip and that in the purchases to automatically add up the total cost. These embedded chips also allow us to read passports from

[43] On that point, M. RUNDLE, ''International Personal Data Protection and Digital Identity Management Tools'', Paper presented at the Identity Mashup Conference (Harvard Law School, 20 June 2006), available at the SSRN paper collection: http://papers.ssrn.com/abstract or at the Berkman Center for Internet and Society Research Publication Series website (Research publication no. 2006, June 2006-06) available at: http://cyber.law.harvard.edu/publications. From the same author, M.C. RUNDLE et P. TREVITHICK, ''Interoperability in the new Digital Identity Infrastructure'' (Feb. 13, 2007), paper published at Social Science Research Network, available on the website: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=962701.

[44] On that point, read J.M. DINANT, ''The concepts of Identity and Identifiability: Both a legal and technical deadlock for protecting human beings in the information society?'', in *Reinventing Data Protection*, S. GUTWIRTH, Y. POULLET et al. (eds.), Dordrecht, The Netherlands, Springer Verlag, 2008 (to be published in Feb. 2009).

[45] On that issue, notably C. PARKER & J. BRAITHWAITE. Regulation. In P. CANE & M. TUSHNET (Eds.), *Oxford Handbook of Legal Studies*. New York: Oxford University Press, 2005, p. 119 and ff.

[46] About the very specific peculiarity of biometric data and the risks linked with their uses, read C. PRIENS, ''Biometric technology Law. Making your body identify for us: legal implications of biometric technologies'', [1998] 14 CLSR 159 and ff. A. CAVOUKIAN and A. STOIANOV, Biometric Encryption: A positive-Sum. Technology that achieves strong authentication, Security and Privacy, *Information and Privacy Commissioner/Ontario*, March 2007.

[47] See other examples and reflections in N. KING, ''Direct Marketing, Mobile Phone and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices'', 60 *Fed. Communications Law Journal*, 2008, pp. 231–325.

[48] M. WEISER, ''The Computer for the 21st Century'', *Scientific American*, 1991, Vol. 265, no. 3, pp. 66–75.

a distance, order things ''automatically'' i.e. the beer we no longer have in our ''intelligent fridges'', or have our television sense our arrival and send our favourite series to the screen of the computer in the office. The possibilities are truly endless and encourage us to continue the exploration of ambient intelligence (see below).

4.4.2. *Ubiquitous computing*

We can talk about ''ubiquitous'' computing in as much as the terminals can be placed anywhere and note everything we do in our daily lives, our movements, our hesitations, or what we choose to eat. Next, this is a technology that is largely invisible in two ways ('Calm Technology'); it operates in a largely hidden way (we do not know what information is collected, when or for whom), but also, as a natural extension of an activity or movement (a door opens and the computer comes on) assisting us in our choice of activities. Finally, this technology learns. These systems often adapt their operation based on feedback from their use.[49] For instance, in a big supermarket, the system will record our purchases and improve our profile over time to send us specifically targeted publicity.

Consequently, ambient intelligence technologies[50] tend to associate the virtual and real worlds. In the space created in the network where there is dialogue between objects, and between objects and people, this is in the real world, the territory held by ICT. At the heart of this network, human beings can become themselves a ''thing'', simply an embedded chip reacting to other embedded chips.[51] Finally, we can raise question of the medical uses of RFID technology. Implanted in the body, they can monitor functioning from a distance or even correct the functioning, for example relieving stress or stimulating memory.

4.4.3. *The reasons for the success of ambient intelligence technologies*

50% of the ''regulars'' at BAJA Club,[52] a firm managing dancing and gaming clubs situated in Holland and Spain, agreed to have an RFID chip implanted in their body. When journalist asked them why they did this, they replied that this made it easier for them as they were instantly recognized as good clients and could immediately enter the casino. They also said that they avoided the risk of having their wallet stolen since all their spending was deducted directly from their credit card. With this example, and there are many others, it is clearly illustrated how the logic of security and efficiency (to gain time and money) explain why these systems are so successful.[53] It is this same RFID chip that the American government intends to implant in every American citizen so that in the case of accident or if a person is unconscious, they can be identified and obtain the medical file of the person concerned. Along the same lines, there was a strong emotional reaction in Belgium when it was discovered that RFID chips were implanted in the passports ''for security reasons'', and a very great reluctance, even on the part of the manufacturers, for the same passport project proposed by the American government.[54]

[49] ''Humans will, in an Ambient Intelligent Environment, be surrounded by intelligent interfaces supported by computing and networking technology that is embedded in everyday objects such as furniture, clothes, vehicles, road and smart materials – even particles of decorative substances like paint. AmI implies a seamless environment of computing advanced networking technology and specific interfaces. This environment should be aware of the specific characteristics of human presence and personalities; adapt to the needs of the user; be capable of responding intelligently to spoken or gestured indications of desire; and even result in systems that are capable of engaging in intelligent dialogue. AmI should be relaxing and enjoyable for the citizen, and not involve a steep learning curve.'' (IST Advisory Group's Report, ''*Ambient intelligence: from vision to reality. For participation in Society and Business*'', 2003 ftp://ftp.cordis.europa.eu/pub/ist/docs/istag).

[50] The term was used for the first time in 1999 by the Advisory Group of the IST Program of the European Union (the ISTAG) in its report on the future of technologies. On all of this, cf. J. AHOLA, ''Ambient Intelligence'', *ERCIM News*, 2001, n# 47, available on the site: www.ercim.org/publications/Ercim_News/enw47. Cf. also the expression of ''Ubiquitous Computing'' launched in 1991 by M. WEISER, ''The Computer for the 21st Century'', *Scientific American*, 265 (3), p. 66–75.

[51] Read, A. ROUVROY, Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence, in *Studies in Ethics, Law, and Technology*, 2008, available at SSRN: http://ssrn.com/abstract=101.3984.

[52] On that experience, see: http://www.baja.nl.

[53] Within the framework of employment relationships, the 'implanted' chip or simply one 'carried by the employee' will make it possible for the employer to note his hours of arrival, to control his moving about or even detect any abnormalities. In the insurance sector, the application of RFID technology may induce radical transformations: whereas the amount of insurance premiums is currently fixed at the time of the contract signature, according to the limited information available to the insurer at that time, the application of RFID technology would make it possible to vary the amount of the premiums charged over time depending on the behaviour of the policyholder. Auto insurance premiums, for example, would thus become dependent on criteria such as the number of kilometres travelled, average speed, etc. The informational asymmetry between the insurer and the policyholder would be appreciably reduced and, as the evaluation of the risk became finer, one would witness the increasing individualization of risk evaluation, which, pushed to its ultimate end, would in fact mean the end of insurance. As François Ewald (F. EWALD (1991) *Insurance and Risk* in G. BUTCHELL, C. GORDON, P. MILLER (eds.), *The Foucault Effect: Studies in Governmentality*, Burchell, University of Chicago Press, 1991) explains, the concept of individual risk contradicts the traditional principle whereby, in the insurance field at least, a risk is always collective, even if its materialization is individual.

[54] About these debates, see the conclusions published by the Smart Card Alliance (November, 3 2006), available on the website: http://www.smartcardalliance.org/pages/publications-whti-passport-card) regarding the use of RFID technology in the passports and the possibility of their at distance reading: ''*The vicinity read Rfid Technology proposed for the passport card, in combination with its weak cryptographic protection, will feed citizen distrust due to the undeniable observation by some technologies that the citizen's unique reference number could be obtained and used to track the citizen whenever the card is outside of its protective sleeve. This raises serious privacy concerns that will have to be overcome if the program is to be embraced by Americans*''. In the same line, the Budapest memorandum on the MRTD (Machine Readable Travel Document) available on the FIDIS (European Research Project FP 6) website: http://www.fidis.net/press-events/press-releases/declaration-de-budapest.

Thus, security, that of the public but also that of organizations and citizens, calls for ever more efficient control, surveillance and alarm systems.[55] Economic profitability, in the broadest sense, and efficiency become additional justifications, where the concerns of the public services and companies on the one hand, meet the interests of consumers and citizens on the other, interests carefully presented by those same public services and companies.

5. Two important trends

5.1. *The privatisation of cyberspace*

5.1.1. *The meaning of the idea*

Here we would like to indicate that many of the norms used in cyberspace and the operation of the network (IP addresses, web protocols, etc.) are outside the control of public authorities whether they are national, regional or international. The control of the Internet is private. Primarily, the Internet functioning and rare resources are controlled by private international organizations such as W3C (*World Wide Web Consortium*), IETF (*Internet Engineering Task Force*) and ICANN[56] and, through discussions between private organizations and not negotiations between states.

Privatisation of cyberspace has another significance when we see the access to cyberspace, as much for those using it as for those providing the content, is constrained by certain actors in the field: ISPs, particular websites and search engines. They can orient our search for information, our movements on the net and make us accept 'their' rules; rules such as accepting publicity and disclosing our identity, etc. These companies are often the same people that install filters, limits and procedures to remove content and thus become the self-proclaimed censors of the public spaces on the Internet.[57] In the same sense, we know how people have contested certain types of DRM systems (Digital Rights Management)[58] when the techniques went much further than anything required by the logic of protecting intellectual rights. Cases exist where restraint was so excessive as to be detrimental to the basic freedom of others or inhibited access of everyone to certain essential material.

And finally, we can see that surveillance technologies, applied more and more in public spaces (shopping malls, department stores, discotheques, etc.), are in fact privatizing space that until now has been for all of us anonymous, and in addition to watching our every move, techniques work to exclude certain segments of the population, as has been seen in sociological studies.[59]

5.2. *The global consequences of local actions and decisions*

5.2.1. *The information society and its regulation: parallels to environmental regulation*

Among those active on the net, we need to particularly examine those who offer services based on these technologies. The way these products and services are built can have important repercussions for the whole planet. This is particularly true when the economic power of the companies concerned can decide the conditions of who accesses or publishes what information in huge areas of the world. It must be noted in particular that the Internet offers a tenfold increase as concerns the impact of certain press organizations.

The Internet can also increase by tenfold the influence of an individual, when directly or indirectly, consciously or unconsciously, with a single message posted on the Internet, a single comment in his blog, he destroys the reputation of another person, passes on a virus, sends or uses child pornography and thereby encourages human degradation and slavery. If all these actions might be perpetrated from home, they can have terrible consequences on the other side the world. The Internet can give our acts, even those that are entirely personal, enormous global impact with no particular effort on our part. This then raises questions regarding individual and collective responsibility. It may be useful to look at it as an information ecosystem, in a similar way as problems of environmental degradation encourage us to think of our individual responsibilities in worldwide terms. The principles of sustainable development and especially those concerning shared risks and the principle of precaution could be equally useful to us in regulating the Internet as they are to the field of bioethics, but until now, there has been no comparable consensus.[60]

6. Some ideas and advice to assure data protection in our information society

6.1. *Plan of the third section: three caveats*

The characteristics of these new technologies, the uses we make of them and the way they are applied lead us to re-

[55] Read notably D. LYON, «Surveillance Society, Understanding Visibility, Mobility and the Phonetic Fix», in *Surveillance and Society*, Vol. 1 (1), p. 1 et seq., 2002.

[56] See *supra*, 4.1.3, Footnote 38.

[57] D. NUNZIATE, ''The Death of the Public Forum in Cyberspace'', *Berkeley Technology Law Journal*, 2005, p. 1115 and ff.

[58] These measures reinforced by their legal enactment contribute to limit *a priori* the access to certain works including despite legal exceptions (DRM) or/and acknowledge the presence of the work in any of its fragment without any discussion about the subsistence of the conditions of the legal protection in all these fragments (Tattooing). They permit a reinforcement of the control of any reuse of each element of the work. On the relationships between IPR and Data Protection, read L. BYGRAEVE, ''Digital Rights Management and Privacy: Legal Aspects in the European Union'', in E. Becker et al., *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (Heidelberg: Springer Verlag, 2003, pp. 418–444).

[59] A. WAKEFIELD, «The public surveillance Functions of Private Security», *Surveillance and Society*, 2005, 2 (4).

[60] About the need to apply in the Internet regulation the same principles than those asserted in the environmental regulation, read Y. POULLET et A. ROUVROY, «Le droit à l'autodétermination informationnelle et la valeur du développement personnel – Une réévaluation de l'importance de la vie privée pour la démocratie», in *L'état de droit virtuel*, Proceedings of the Colloquium organized by L.H. Wilson Chair at Montreal, October 2007.

examine the way in which we regard privacy and private life. While it may shock some lawyers, who are too often given exclusive responsibility to protect data, there are three important caveats they must bear in mind.

First, stop acting like a lawyer. When looking at new developments that allow new possibilities, do not react legalistically, rather look at the social impact and the transformation of human relations created by these technologies. Second, understand that the law is not the only solution to the risks created by this new technology: 'If technology created the problem, technology can solve the problem'. The law can allow technology to solve its own problems. Third, keep in mind two keywords from the legislation on data protection 'proportionality' and 'transparency'. Now, these concepts need to be fully understood and applied in the contemporary world.

The three points raised above require further elaboration.

6.2. "Viva data protection rights" an idea with limits

6.2.1. A few examples

Do not limit yourself to the legalistic considerations; look at the wider picture, how information technology modifies our way of living. It is only by looking at the changes and uses of these technologies, often very positive, though occasionally with some negative aspects, that we can eventually find an appropriate legal solution in combination, or not, with other regulatory solutions.

Three examples can illustrate the point. The first concerns uses brought in for electronic government. We know that the use of ICT in government departments increases the level of communications between departments. In one case, it is to verify a certain piece of information about a citizen, in another, to see if the regulations have been followed, or to automatically check who is eligible for benefits. While these internal communication channels are laudable, as much for the efficiency of the bureaucracy as for the rights respected and service rendered to the citizen, a radical transformation of the relationship between the citizen and the state is taking place. The state is no longer a local office, but rather, a whole network. A citizen who asks for a building permit confronts faceless administration collecting information from various necessary sources, automatically weighing the different factors and rendering a verdict. The only identity a citizen has for the state administration is their electronic identity and pin code, their national identification number. In the area of social benefits, the decision in any given case is based entirely on whether or not specific criteria are met. No consideration is given to the person, their difficulties or the situation they may find themselves in. The citizen is no longer a person, simply a number, and a number in 'Big Brother's machine'.

The second example leads us to question the multiplication of cooperative networks within various industries. For instance, the insurance industry has set up a database to fight against the risks of fraudsters, defaulters and those that make frequent claims. The risk of this kind of cooperative venture is the fear that certain people will be 'blacklisted' and thus excluded from services that are essential in our society. In effect, what can someone do if they are on the blacklist, need a car for their work and cannot get car insurance?

The last example comes from a recent event related in the local newspaper. A school worked out a system that instantaneously recognized students enrolled in the school by placing an RFID chip in the school bag of each student. Placing such a chip in this way raises many questions that, while not being judicial, are essential to consider. We can well imagine how a child between 5 and 10 years old might resent the school if he was locked out of school simply because his mother had bought a new school bag the day before. What will the childcare worker think when their 'productivity', that is, the number of children present, is automatically controlled by the system?

6.2.2. A 'Technology Assessment' approach

These three examples show the interest of having a wider 'Technology Assessment' approach to examine the full social consequences of innovation, rather than by narrowly defined technological efficiency. This analysis allows a clearer determination of what is at stake and the risks involved when analyzing data protection procedures. It is only in as much as we have weighed the above considerations that we can properly appreciate the legitimacy of the innovations and their eventual impact on our freedoms.

6.3. While technology offers risk, it can also offer solutions

6.3.1. The RFID case

The recent European debate regarding RFID chips leads to certain conclusions regarding the responsibilities of terminal manufacturers and suppliers of RFID systems. These conclusions concern the infrastructures of the collection and transmission systems, the data generated by the RFID terminals, the databases themselves and the analysis on which the ongoing decisions are based. It was essential that the European debate enlarge the basic protection of data to include the infrastructures and terminals. How can the data be properly protected if the technical solutions do not take into account present-day constraints and transpose them efficiently into regulation? For instance to look at the case of RFID again, do we agree with the Article 29 Working Party[61] that a person carrying a chip should be able to deactivate it easily and that transmissions should be protected cryptographically? This approach called 'Privacy by Design'[62] is based on some early thinking in the area first framed in French law in 1978:

> *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.*

[61] *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.

[62] As asserted by Anne Cavioukan, DPA Commissioner from Ontario (Canada) in its introductory remarks to the Privacy Guidelines for RFID Information Systems available on the website: http://www.ipc.on.ca: "*Privacy and Security must be built in from the Outset – at the design Stage*".

Based on this text, data protection agencies 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. They are responsible for the risk.

6.3.2. *Beyond the law, technology to the rescue*

A second example of how technology can assist[63] in protecting personal liberties is the general demand that 'Identity Management' systems allow control of access and data transmission upstream and downstream in the data flux and thus automatically assure the prescriptions and limits established for the use of the personally identifiable data.

We can look at many such examples: for instance, the use of cookies. These kinds of programs will flag their arrival, block them, and offer the option to refuse or accept them. They can also establish 'no-robot' parameters for a website that prevents search engines from cataloguing the site automatically. There is also a call for 'Privacy Enhancing Technologies',[64] labelling systems and finally, collaboration between public and private organizations to standardize systems.[65]

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[66]:

> *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.*

6.4. *Two keywords to take seriously: proportionality and transparency*[67]

6.4.1. *Proportionality of the analysis and content*

If we can only remember two concepts as regards the legislation on privacy, it needs to be these two. A close examination of their meaning reveals something new every day, nuances regarding new applications or uses, and in general, the characteristics of these new technologies.

First, let us examine proportionality. Proportionality covers both the content and the analysis of the data. As far as the analysis goes, we can think about the following questions.

- Is not there a way that is less intrusive to personal liberty to reach the same objective(s)? For example, to resolve a particular question, it is often simplest to use intelligent cross-referencing of the trail left by users of today's communication technologies. However, these trails show a lot of extraneous information; where the individuals are, their relations with others, sites they have visited, and even the discussions they have had.
- Is it necessary to force the cooperation of those involved? I.e. the ISPs or other service providers; force them to retain and store all the communications data, and establish methods for the use of this data as a legal proof in a court of law?
- Profiling Internet users is easy by cross-referencing data from various sources, but can calculating the credit risk of a potential client or personalizing publicity offers justify the profiling and the reductionist view of the individual?

6.4.2. *Some considerations and criticisms of ''consent'' as the basis to legitimize data analysis*

'Consent' is cited to justify all kinds of data analysis, but we must establish clearly what this means. On the Internet 'consent' is an easy argument to make because the web is so interactive and consent is given for piffling advantages, but beyond this it is very difficult to refuse consent, in fact refusing it is somehow 'abnormal', and thus pushes the user to usually give it.

This approach is supported by the argument that 'the right to data protection' is the right for the individual to decide what data will be circulated. The person concerned by the data is the best placed to decide[68] whether or not the information should

[63] Like the famous EuroPrise labelling system developed jointly by different Data Protection Authorities (www.european-privacy-seal.eu). The privacy certificate aims to facilitate an increase of market transparency for privacy relevant products and an enlargement of the market for Privacy Enhancing Technologies and finally an increase of trust in IT.

[64] On that issue, read KPMG et al. (2004). *Privacy-enhancing technologies: White paper for decision makers*. Ministry of the Interior and Kingdom Relations, The Netherlands. http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf. See also the EC Communication to the E.P and the Council, «*Promote Data Protection through the development of technologies increasing the Privacy Protection*», Com(2007) 208 final, Brussels 2.5.2007.

[65] European Committee for Standardisation (CEN) & Information Society Standardisation System (ISSS) (2002). Initiative on privacy standardisation in Europe. Final report. Brussels: CEN/ISSS. http://www.cen.eu/cenorm/sectors/sectors/isss/activity/ipsefinalreportwebversion.pdf; see also, J.K. WINN, ''Technical Standards as Data Protection Regulation'' in *Reinventing Data Protection*, Proceedings of the Colloquium held at Brussels, Nov. 2007, Springer Verlag, 2009 (forthcoming).

[66] 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.

[67] About the priority of these two key concepts in order to understand Privacy legislations, read DE HERT and 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 al. (ed.), Interscientia, Antwerpen–Oxford, 2006, p. 74.

[68] The context of the Internet creates new possibilities for the 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 seq.; 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.

be circulated. The individual's consent is thus necessary to legitimize any data analysis of information of a personal nature. The argument that data of a personal nature can be a 'thing' and might be alienated from the person concerned, or used as a tradable commodity, is a disputable idea.[69]

For example, we can very well imagine that a medical file belongs as much to the patient who 'generated' the information, as to the treating physician. In the 'Owner approach', personal data is considered as valuable merchandise that can be the subject of negotiations and transactions with other people through a series of licenses.[70] The 'Contractual Approach', which is very similar to the 'Owner Approach', is centred on the agreement between the parties concerned regarding use of the data. This does not really examine the question of whether or not personal information can be considered wholly as property, but does allow the parties concerned to make promises with regard to data of a personal nature and their possible uses. Schoeman[71] adds:

> *[O]ne difficulty with regarding privacy as the 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.*

6.4.3. *Proportionality and mainstream ideas*

Proportionality goes on to examine the content of the analysis, the information technologies themselves and especially, the storage capacities and analysis of data, which make both the collection of more information and their constant transfer more and more common. Is this mass of data necessary, adequate and pertinent? The data protection managers must be attentive not to retain unnecessary data and to assure that only authorized users access data to which they have a legitimate right.

The need to reaffirm this principle of proportionality arises the moment that the level of efficiency, whether in terms of economic efficiency or security, might substantially be improved through advances in ICTs.

Thus, we see that public security but also the privacy of organizations and citizens demands ever better systems of control, surveillance and warning. Economic efficiency in the widest sense and efficiency in general are further justifications. Here we can see the interests of government and organizations on the one hand, and the interests of consumers and citizens in efficiency on the other; arguments put forward as the justification for both states and organizations.

6.4.4. *Transparency of data treatment and beyond information systems*

The second keyword is transparency in the treatment of information. Of course, the data manager has the obligation to inform those concerned of their right to access, correct or signal their opposition to information contained about them, as enshrined in data protection laws. However, how can we not envision reinforcing these rights and obligations to re-establish something like a level playing field and thereby correct a growing information imbalance between those who hold and transform the data and those referred to in that same data. Is it not therefore necessary to require a clear exposition of the pathways that the information follows, a map that shows complex ebb and flow of the data?

6.4.5. *Transparent terminals: technology to make things clear*

Is it not necessary to oblige user terminals to operate in a clear and transparent way? Much of what they do at present is hidden and outside of the control of the users. We can also ask ourselves if the equipment we use is adapted to that requirement for clarity and transparency that permits the user to have full control of the information sent and received. 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 the 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.

Above and beyond the right of the user to be informed of this flux of information arriving, we can ask ourselves what right exists to authorize, or not, as the case may be, a third party to enter our 'virtual home'.[72]

7. Conclusions

7.1. *Technology and privacy: Aesop's tongue*

It is clear that information technologies bring everyone the possibility of liberation: the discovery of new worlds; to

[69] 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 us 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 &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.

[70] 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, p. 1125 and ff.; J. LITMAN, ' Information Privacy/Information Property', 52 *Stanford Law Rev.*, 2000, p. 1250; K. BASHO, 'The Licensing of the personal information. Is that a solution to Internet Privacy? ', 88 *California Law Rev.*, 2000, p. 1507.

[71] F. SCHOEMAN, «Privacy: Philosophical Dimensions of the Literature», in *Philosophical Dimensions of the Privacy*, F.D. SCHOEMAN (ed.), 1984, p. 3.

[72] That comparison between the protection of terminal equipment, considered as a virtual home, and the 'physical' home envisaged by the article 8 of the European Convention can be deduced from the article 5.3 of the European Directive on e-privacy. This provision forbids any intrusion into the terminal equipment through spyware, cookies and other pieces of information or software except with the user's consent or for very specified legitimate reasons.

breakout from everyday existence; to express oneself and to communicate with others. It brings each person undeniable advantages, whether they are economic (buying on the Internet, fewer trips to the shops) or in terms of security (video surveillance systems).

However, these technologies represent a risk to our liberties at least as great as the advantages that they present, and these risks are growing. Not only must we accept to be followed constantly, to be reduced to a number, to accommodate messages arriving constantly in our mailbox, on our screens, even in our bodies; beyond this, we must give way to the perception of personal information as merchandise, exposing ourselves on the net through various sites and social networks. Here especially, the added value brought by the increasing recognition of the right to privacy as really the defence of the human person, the person's development and dignity become absolutes; properly placing priorities of security and economic efficiency in their place of only relative importance.

'Security first' thinking automatically treats each individual as a suspect and economic logic dictates that we will all act based on rational self-interest. These 'modern day' maxims must be contested urgently, as by continually seeing individuals in such a negative way, as is done in particular through the technology of our information society, we risk inducing the very behaviour that in fact justifies the security and economic approaches above,[73] but at the price of losing our most precious capacities of our freedom and our liberty.

If we can accept to question these public perceptions, we can be assured that people reach their full potential, not only in terms of personal liberty, but also their creative and political potential, which is at present latent in our information society. We see that the right to the protection of privacy is not simply one among several other fundamental rights but the fundamental precondition so that other rights and liberties can be exercised.[74]

7.2. *There is the challenge*

At present, those responsible for protecting our freedoms do not seem to be up to the job. It is not a question here of human or financial resources but a lack of allies. The state, which has traditionally been the guarantor of our liberties, is more and more interested by the advantages that technology can bring in terms of efficiency and security. The public themselves seem more fascinated by the technology than fearful of the risks its use creates. The cause of freedom seems very remote and difficult to defend when citizens are more concerned with the imperatives of the short term.

7.3. *How to meet this challenge?*

This can be achieved, no doubt, by lifting the veil of the network that surrounds us: education that allows the understanding of legislation that has incomprehensible language; legislation that makes sense when it embraces all the kinds of data we put out there on the web in sites such as FACEBOOK; when we show consumers how publicity works on the net; or when employees discover how employers can use the traces left by their GPS or their cell phone or their computer to their detriment.

Creating new alliances between these representatives of freedom, consumer groups and unions is a second objective for all those authorities in charge of data protection. These Data Protection Authorities must always remember that they are not by nature independent. This can only be earned by the constant effort to be and remain independent.

Professor Yves Poullet *(yves.poullet@fundp.ac.be) CLSR Editorial Board, Director, Centre for Information and Law (CRID), University of Namur, Belgium http://www.crid.be.*

[73] We totally agree with the European Data Protection Supervisor (E.D.P.S.) when he asserts «*a message such as:* ''No right to privacy until life and security are guaranteed'' is developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford. […] the Home Secretary of the United Kingdom, Dr John Reid, called for human rights law to be rewritten, stating that ''The right to security, to the protection of life and liberty, is and should be the basic right on which all others are based''. […]This position could be potentially dangerous and may produce more problems than it seeks to solve… There should be no doubt that *effective anti-terror measures can be framed within the boundaries of fundamental rights. It is these rights that need to be protected under all circumstances in a democratic society*. In the past examples can be found in different parts of Europe where the failure to protect fundamental rights has served as source of continued unrest rather than ensure safety and stability (CEPD, «Letters to the incoming presidency: fundamental rights are not captives of security», 11 June 2007, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-06-11_Letters_portuguese_presidency_EN.pdf).

[74] As expressed by BURKERT, privacy might 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 (in H. BURKERT, 'Dualities of Privacy – An Introduction to 'Personal Data Protection and Fundamental Rights'', in *Challenges of Privacy and Data Protection Law*, M.V. Perez, A. Palazzi (eds), Cahier du Crid, no. 31, Bruylant, Bruxelles, p. 14).