COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 13/12/2004 T-PD (2004) 04 final

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

REPORT ON THE APPLICATION OF DATA PROTECTION PRINCIPLES TO THE WORLDWIDE TELECOMMUNICATION NETWORKS

Information self-determination in the internet era

Thoughts on Convention No. 108 for the purposes of the future work of the Consultative Committee (T-PD)

By

Yves Poullet
Expert to the Unesco and to the European Commission
Dean of the University of Law in Namur (Belgium)
Director of the Centre for Computer Research and Law

Jean-Marc Dinant, Information Technology Master
Expert to the BelgianCommission for privacy protection and to the Group 29
Senior lecturer of the university of Namur

With the co-operation of
Cécile de Terwangne, Teacher at the University of Law in Namur
Maria Veronica Perez- Asinari, Senior Researcher to the CRID

INDEX AND TABLES

INTRODUCTION

The purpose of this report was to help the Consultative Committee identify new avenues of enquiry and possible areas for future work. This would involve highlighting some of the challenges arising from the technological development of electronic communication networks and services, and drawing on these to put forward proposals for a number of research topics or themes for recommendations that the Consultative Committee could then submit to the Committee of Ministers.

Accordingly, the report will first of all describe the changes that have taken place in the technological landscape since the adoption of Convention No. 108 along, with some of the major issues relating to these changes (Part I), then examine the provisions of the Convention in the light of these changes (Part II) and finally propose a number of new principles for what in the conclusion of the report is termed the third generation of privacy protection regulations (Part III).

This report is based on ideas that have gradually taken shape in the course of our own work and activities in data protection institutions, and on discussions held among researchers in our own centre. We would like to thank Ms Cécile de Terwangne and Ms Maria Veronica Perez Asinari for their help in writing this report and their many comments which led us to improve and amplify what we have written. Our thanks go also to our colleagues in Namur, Ms Karen Rosier and Mr T. Léonard. Moving beyond the Namur circle, a preliminary version of our ideas was aired at various forums: at a conference organised by the Italian *Garante* in June of this year, at the first meeting to present the report to the T-PD the same month, and at the Prague Conference organised by the Council of Europe on 14 and 15 October[1]. There is no doubt that the report would not be what it is without the many contributions received at these different presentations. The comments we received gave us confirmation that although our initial thoughts may have been far from complete, they were nonetheless well-founded.

To assist readers, under the heading “Avenues of enquiry”, we have printed in bold those areas where we believe further research is needed and have included a number of suggestions in this regard. These headings are not systematic. In addition, we did not wish to burden readers with too many footnotes, referring them simply to particular learned articles and other documents. We do not claim to have been exhaustive nor that the questions highlighted are the only important ones for the subject we were analysing. We have merely attempted to set out certain opinions with the hope that these will be shared.

[1] Cf. Y. POULLET, “Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection”, report to be published in the Proceedings of the Conference. Parts of that report are reproduced in this document (in particular, Part III)

PART I: THE NEW VULNERABILITY OF THE INDIVIDUAL IN THE GLOBAL TELECOMMUNICATIONS NETWORKS

1. Introduction

This first part will be assessing the actual[2] and typical[3] risks run by an individual in his or her private or working life through the use of electronic telecommunications networks. This report is therefore not concerned with analysing risks associated with the management of purely manual files or the transmission of information on a physical medium other than a telecommunications terminal.

One of the problems brought about by the development of these networks is the information imbalance created between those responsible for processing and those on whom information is being processed. Current technology, based on ever faster, more powerful, smaller and omnipresent computers, is able to collect and transmit, in practice and systematically, numerous traces without it being apparent that such information has been collected, or indeed how and why.

The reply to this first part could in fact be a question: "How should one protect oneself?" In our opinion, this is very badly worded as it presupposes that it is the individual's responsibility alone to protect himself or herself. So the first question to be asked is "who should do the protecting?" This implies, of course, the question of the funding of and responsibility for such protection.

2. The technological landscape and its evolution

2.1. THE SITUATION IN 1980

It should be remembered that less than a generation ago the internet as it now exists was simply inconceivable.

For the record, the first mass distribution personal computer appeared at the beginning of the 1980s. It was the IBM PC junior and was already equipped at that time with the Microsoft Disk Operating System (MS-DOS). Companies' local networks began to be set up around 1985. The Numéris network (ISDN)[4] was developed about 1987. The first browser appeared in 1990-91 and made it possible to "surf" a very small number of web sites, most of them American. At

---

[2] The aim is not to describe what could happen but what does happen, and with some thoughts as to what might happen in the near future.

[3] The typical profile we have in mind is the lay internet user, a "netizen" (Internet citizen) who is not a technician, who does not have a great deal of financial resources or time to devote to protection. Clearly, readers might object that in a given situation, individuals can obviate certain risks by acting accordingly. Apart from the fact that this presupposes a non-negligible level of education, technological skill, time and perhaps money, and we are assuming the opposite, our response is to consider the cause of the risk: would it not have been possible to design another technology that did not require internet users to have to protect themselves? One of the major dangers in the telecommunications network society is that of the marginalisation, penalisation or even exclusion of those wishing to protect their anonymity (including their non-traceability).

[4] Integrated Services Digital Network

that time, the speed of private lines was of the order of 2400 to 9600 bits a second. Mobile telephones appeared around the mid-1990s.

Before 1990, for most people the telecommunications networks were used for just two purposes: telephoning and sending faxes. Many practices did not involve the use of a network of telephonic communications: reading a newspaper, ordering goods or services, listening to the radio, watching television, placing a small ad, consulting a telephone directory or small ads, making a payment, opening a door, sending or receiving mail, etc.

2.2. THE DIGITISATION OF INFORMATION AND OF ITS TRANSMISSION

The first fundamental change linked to the development of the new information and communication technologies (NICTs) was the digitisation of sound and picture signals and of information itself. At the moment, any audible or visual content can be digitised, ie it can be transmitted as a 0 or a 1 and therefore stored and transmitted by electronic equipment. This digitisation functions at the global level thanks to internationally standardised digitisation algorithms (for example, JPEG for photographs, EFR for speech, MPEG for moving images, etc) that are known to all and account for the universal rules that make it possible to switch from analogue to binary content and vice versa. The feature of the modern telephones (ISDN or GSM) is that they digitise speech in real time, send it over the network in binary form and transform the digital signal on arrival into an audible vocal signal.

It may be wondered what the advantage is in digitising every signal. In fact, there is a twofold benefit. Firstly, it enables ever smaller and ever more powerful computers to deal with this signal, and secondly the first development is followed by another, namely “packaging”.

The old telephone networks worked on the basis of **circuit switching**. This means that each telephone exchange was in fact a switching centre that involved physically connecting certain wires to one another in such a way as to enable an electric current carrying an analogue speech signal to pass through. This is not the best method for several reasons. It is necessary to create a physical end-to-end link between two people, sometimes over long distances, thus making it impossible for others to use the portion of the line used by these two individuals. This aspect proved all the more inconvenient as the transmission capacity of a single channel was increasing. In order to overcome this drawback, a multiplexing system was used.

At the moment, on the internet and other networks a **packet switching** rather than a circuit switching system is used. The information, which has first been digitised, is sent in the form of small packets (typically from tens of bits to a few hundred. Packet switching generally permits the optimum use of the frequency range and, therefore, of the capacity of the telecommunications medium. This method enables a single communication carrier to be shared in an extremely flexible way between hundreds or even thousands of users simultaneously.

Each packet contains the address of the sender and the recipient. On the network, each node (switch) that receives a packet knows where to send it on the basis of its destination address (this is called routing). If it cannot send this packet for some reason or other, it can return it to the node that has forwarded it together with an explanation.

An important consequence as far as we are concerned is that the recipient knows or is able to find out where the packet was sent from and even the sender's address since this is stated on the packet received.

2.3. EXPONENTIAL PERFORMANCE GROWTH FOR THE COMMUNICATIONS MEDIA

Another recurrent aspect of telecommunications networks consists in constantly increasing their efficiency in terms of flow rates. A number of major trends can be identified.

1. **Flow rate increase**[5]. According to the current state of the art, fibre optic cables, which are insensitive to electromagnetic interference, permit flow rates of the order of 10Gbits/second[6]. Present-day cables contain several fibres (from a few dozen to a few hundred). Thanks to DSL technology, it is normal today to achieve flow rates of up to four megabits a second without having to modify the conventional twisted pair telephone wire and with equipment costing less than a hundred euros. This means it will eventually be technically possible for television to be distributed via the internet rather than satellite or a dedicated coaxial cable. Experiments along these lines are incidentally under way in a number of countries. This presents a new challenge. At the moment, satellite and cable distribution technically do not, or hardly, enable the broadcaster to know what programmes the consumer is watching (technically, all the signals arrive at the terminal device of the subscriber[7], who chooses what to watch). In the case of internet television, it will be possible to find out what each individual is watching and even insert advertising targeted at him or her at precisely chosen moments.

2. **Evolution of the processing power. Increase in processing power.** Processing power has increased in correlation to the power and capacity of computer components. In 1987, a typical PC had an 8 MHz processor with 640 KB of random access memory and a hard disk of 20 megabytes. Today in 2004, a computer typically on sale in supermarkets has a 2.4 GHz processor (3,000 times more), 256 MB of RAM (400 times more) and a hard disk with a capacity of 60 GB (3,000 times more). Moreover, at equivalent speed, modern processors are significantly more powerful than their predecessors and there is an increasing tendency for there to be a greater number of processors inside a computer, some of which play a more specialised role (ASIC[8]) controlling a specific task (for example, display or the transmission and reception of signals on the network). Certain processes, which used to be impossible, are now becoming perfectly feasible. The sampling and digitisation of a voice or an image can now be done in real time, with the result being of a quality very close to the original.

3. **The versatility of telecommunications networks**. This versatility is made possible by the digitisation of all types of content (text, image, video, speech, etc), which enables them to be universally represented in the form of bits. In addition, substantial flow increases enable rich and complex content, such as multimedia, to be transmitted in real time.

4. **Permanent connectivity**. This is another remarkable feature of the development of telecommunications in the last few years. It is made possible by the flow increases and the distribution of information in the form of packets. Moreover, the spread of wireless networks permits the mobility of telecommunications terminals and their connectivity whilst en route.

---

[5] Not in terms of speed. Speed is a separate concept from flow. Basically, the information flowing through a copper wire or a fibre optic cable always passes through at the speed of light. An increase in the flow depends on the ability to alternate the “zeros” and the “ones” more quickly.

[6] This refers to the equipment currently installed. Prototypes enable much faster speeds to be achieved.

[7] This is why it is possible to record a television programme while watching another at the same time.

[8] Application Specific Integrated Circuit: a processor specially designed for a specific task (eg the digitisation of an analogue signal, encryption or decryption). Typically, an ASIC chip will run approximately one hundred times faster than a non-application-specific processor to carry out a particular task.

5. **Flat-rate pricing.** In the case of many networks, pricing is based on a line rental representing the connection to the network and perhaps a small additional charge for certain uses of the network. The effect of this pricing structure is twofold. Firstly, charging a flat rate means the network operator no longer has any reason to collect and preserve traffic data since it no longer charges for each of the connections made. Secondly, the price is no longer based on the costs, or at any rate no longer on an individual basis. Item-by-item pricing will always pose a bigger problem for respect for privacy than a flat-arte system.

6. **Pseudo-free software.** It is normal today for individuals wishing to use a service provided by the information society (for example, send an e-mail, surf the web, etc) to be offered, if not the terminal then at least the software enabling the service to be accessed. In fact, this "client" software is in practice much more numerous and is more complicated to produce and maintain than corresponding client software. To put it another way, when Microsoft sells its HTTP Internet Information Server ASP, it also sells, somewhere or other, the service that consists in offering tens of millions of users the free browser (MSIE) that makes it possible to connect up to it. The policy of providing it free of charge is thus not cost based – far from it – but leads to distortions of competition for firms that only want to produce "client" software (such as Opera or Mozilla). Without going into details[9], these market newcomers provide functionalities that provide much better protection for personal privacy.

In functional terms, most of the network equipment can be defined today as computers. It is worth recalling Moore's law here, which states that computer performance doubles every eighteen months, or is multiplied by a thousand every fifteen years, and that the price for the same performance goes down by half. This means that, everything else being equal, the power of computers will be multiplied by a thousand in 2019. However, many experts predict that this law will cease to apply when the size of circuits reaches tens of nanometres. Nevertheless, it is possible at the same time that optronics[10] will eventually replace electronics and thus permit a fantastic increase in performance to be achieved.

In the light of these facts, it should be emphasised that human sensory capacities have not significantly changed in this period. The bit rate necessary for a sound is still around 10kbits a second (speech) and 20kbits a second (high fidelity) and a film with sound requires between 256kbits a second (videoconference) and 2 gigabits for high quality.

In conclusion, it has become, and will become, more and more possible and less and less expensive to record the lives of all the individuals on the planet (our own and those of other people …).

By way of illustration, we can examine the feasibility of recording *all* the telephone calls from Europe to the entire world. This is no mean task, since it is necessary to store the equivalent of fifty billion minutes of voice calls[11] on an annual basis[12]. Considering that about ten thousand

---

[9] We would point out that Mozilla/Firefox enables invisible hyperlinks outside the domain being visited to be blocked and that Opera makes it possible to prevent the disclosure of the reference page through which the details of the user's clickstream pass on their way to cybermarketing firms. MSIE version 6.0 does not possess these functionalities.

[10] The idea is to transport information using light rather than electric wires. The big advantage of this solution lies in being able to avoid the increasingly large amounts of heat generated by the current microprocessors.

[11] Calculation based on an extrapolation of the figures for 1999 provided by the International Telecommunications Union (seen at http://www.itu.int/ITU-D/ict/statistics/at_glance/Eurostat_2001.pdf in May 2004)

bits per second are required to digitise speech and that the data can be compressed by a factor of two (which is normal) it can be seen that at least an average of about five terabytes will be necessary to store 24 hours of traffic, which is entirely possible today with array disk systems that enable each disk to store some 400 gigabytes[13]. Moreover, the average bit rate of this continuous flow of hundreds of thousands of simultaneous calls is about 0.5 gigabits per second, which can easily be handled by a single fibre optic cable of the thickness of a hair[14]. In other terms, it would be technically possible to send ALL this telephone traffic down a glass tube just a few microns thick and record it at a reasonable price using conventional equipment that anyone can buy over the Internet.

If we wished to record all the words uttered by a human being from his/her birth to the time of his/her death, a single high capacity hard disk would be more than big enough today[15].

In commerce, there are currently walkman-type systems capable of recording the content of the equivalent of several hundreds of conventional CD-ROMs in the MP3 format. Digital cameras make it possible to store hundreds or even thousands of photographs, while the conventional chemical film enables a maximum of 36 pictures to be taken. At one megabyte per high-resolution photograph, a high-capacity hard disk today could stock somewhere in the region of 40,000 high-resolution photographs.

The Belgian National Register, which contains the demographic details of all Belgians from their birth to their death as well as their occupations, marriages and death and successive addresses[16], not counting the data on foreign residents in Belgium, would today easily fit onto a DAT cassette the size of a large box of matches or on a few DVDs. It could be transmitted in its entirety by fibre optic cable in less than a minute.

It might be argued that storage is not everything and that it would be very difficult to process this mass of information in order to find particular data. This is not at all the case, for two reasons. First, Moore's Law also and especially applies to the speed with which processors operate. Second, huge advances have been made in recent decades with automatic indexing and pattern recognition algorithms. The time required to carry out a binary search (typically finding the name of a given person in an alphabetical list) depends on the base-two (binary) logarithm of the number of people. In other words, all other things being equal, if it takes a computer one second to find one person among an alphabetical list of 1,000 people, it will need just 3 seconds to find the same person among a list of 1,000,000,000 people.

2.4. SIGNIFICANT CHANGE IN THE NATURE AND CAPACITY OF TELECOMMUNICATIONS TERMINALS

Another major (r)evolution has taken place with respect to telecommunications terminals and goes hand in hand with the lightning development of microcomputers. At the beginning of

---

[12] In 1980, this would have required millions of recording machines with the same number of magnetic tapes. At that time, a recording machine was necessary to record a conversation.

[13] See, for example, the 400GB Deskstar 7K400 at www.hitachi.com.

[14] Currently, rates of 2.5 to 10 gigabits a second are normal on this type of carrier.

[15] On the assumption that a human being lives 100 years, sleeps for 8 hours out of 24 and speaks on average just one tenth of the time, the capacity needed to record everything he or she has said would be 263 Gigabytes

[16] About 2 billion bytes.

the 1980s, telecommunications terminal devices were monofunctional[17]. Since the early 1990s and especially with the integration of multimedia into personal computers, there has been a very strong convergence between telecommunications terminals and personal computers. Currently, all telecommunications terminals are microcomputers. The problem is that, unlike the terminals (telephones and fax machines) and the protocols (especially the ISDN standard) of the past, which were governed by a regulatory framework of the state involving an approval system, today's computers are only subject to technical standards drawn up by engineers recruited by the information and communication technologies (ICT) industry. While certain limitations are factored in by this industry, this is not so much to protect the private lives of the citizens (companies that purchase these technologies have many reasons for wanting to know *their* customers or *their* potential customers) but to avoid the spread of mistrust on the part of the consumers, which would be harmful to business.

2.4.1 Terminals: a change in the social paradigms of communication

The main feature of the telecommunications terminals lies in their natural ability (this is in the very *nature* of information technology) to make copies and keep a record of the communications carried out. The very nature of the terminal equipment, which has progressed from electro-mechanical devices to programmable electronics, leads to an entirely intangible but certain **change in the social paradigm**. The telecommunications device still possesses a determinism no longer dictated by its designer.

In other words, pressing a key no longer brings about an almost mechanical change in the state of the device, a change that, moreover, can generally be perceived (for example, taking the receiver off the hook and hearing the dialling tone or receiving a call and setting off the ringing tone) but constitutes a command to a computer programme that has the ability to do what the user wants if the programmer has so determined and in the manner determined. Moreover, this action is in general ***totally or partly invisible to the naked eye***. The terminal shows the truth but not the whole truth. The core elements are invisible and are not what appears on the screen but what is inputted into, comes out of and is stored in the telecommunications terminal. This is why cookies have caused so much indignation. By default, cookies are invisible and surreptitiously enter and leave the telecommunications terminal. They are generally stored without the internaut being aware of this[18]. A similar mechanism had been thought of for the Teletel terminals (the precursor to the Minitel terminal in France) during the 1980s[19]. The idea was to equip the terminal with a memory which could have been used by the server. Following an outcry from consumers associations and a recommendation issued by the CNIL to the operator, the idea was abandoned. Historically, cookies made their appearance with Version 2 of Netscape Navigator, Netscape having published the first specification[20] in 1996. Version 3 of Internet Explorer implemented these same specifications. Since then, cookies have been standardised by the W3C[21] and the Internet Engineering Task Force[22].

---

17 Linguistically, the same term was employed for the name of the device and for using it: *I telephone, you fax.*

18 I think it is optimistic to believe that 95% of "ordinary" web surfers know what a cookie is and how to protect themselves against it.

19 It was the action taken at the time by the French data protection authority itself, the CNIL, that put an end to such a system (see Marie Georges, Technology for Privacy Protection, page 4, 23rd International Conference of Data Protection Commissioners, Paris, 2001, available on http://www.paris-conference-2001.org/eng/contribution/georges_contrib.pdf).

20 http://wp.netscape.com/newsref/std/cookie_spec.html

21 "HTTP State Management Mechanism" on http://www.w3.org/Protocols/rfc2109/rfc2109 .

The very idea of the "good old" telephone[23] stands in contrast to this model. It possesses features that, although they are self-evident, should be mentioned, perhaps simply because they are so obvious. As a general rule, everything else being equal,

1. it is the user who has to take positive, concrete action (to pick up the receiver, dial the number) in order to make a telephone call. The telephone cannot make a call without a positive human action;

2. the fact that a call is being made is perfectly clear since the receiver has been taken off the hook;

3. the network user can terminate a call by means of a simple, positive and concrete action (replacing the receiver);

4. the user in theory knows who he is calling (rerouting was not possible);

5. a phone call takes place between two individuals and nobody else can know what is being said unless a listening device is installed;

6. each speaker hears everything said on the phone (there is no inaudible service channel carrying service information, such as with the ISDN system).

It is genuinely possible to speak here of a paradigm of transparency and perfect control over telecommunication, which is a universally accepted means of communication. It should be emphasised that the digitisation of the telephone (ISDN) has begun to make fundamental changes to this paradigm.

With electronic telephones and ISDN in particular, it became possible to telephone hands-free and without lifting the receiver. This was where the problems began: this functionality was introduced at the level of the telephone exchanges themselves to permit eavesdropping not only on the call itself but also on the room where the telephone was installed, without the receiver being lifted. [24][25]

---

[22] "HTTP State Management Mechanism" available on http://www.ietf.org/rfc/rfc2965.txt. One sentence is particularly significant: "…"

[23] In jargon called POTS (Plain Old Telephone System)

[24] This was established by the Scientific and Technological Options Assessment of the European Parliament in 1998: "*2.5 ISDN. It is technically possible to tap an ISDN telephone with the help of software that remotely activates the monitoring function via the D channel, obviously without physically lifting the receiver. It is therefore easy to eavesdrop on certain conversations in a given room.*", in Development of Surveillance Technology and Abuse of Economic Information, Vol 3/5, Encryption and cryptosystems a survey of the technology assessment issues. Working document, Luxembourg, November 1999. Read at http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-3_en.pdf in May 2004

[25] The public prosecutor Eva Joly, who was investigating a corruption case, was to become a victim of this possibility: "*a quarter of an hour earlier, the President* of the Court of A*ccusation tried to contact me. My telephone did not ring but she was surprised to hear me questioning the Chairman and Chief Executive of Elf-Gabon. My telephone had become a secret microphone that could be switched on by simply dialling my internal number. I drew up an incident report to be sent to my superiors. Immediately, a rumour went around that I had become paranoid or a mythomaniac.. (...) This is what it is like nowadays: we spend our time proving we are not mad while serious breaches of the law – such as recording the substance of an interview or eavesdropping on a law officer – only stirs us into action and does not bother anyone in the judicial hierarchy (...)".* See Eva Joly, "Est-ce dans ce monde que nous voulons vivre?", Edition Les Arênes, Paris, 2001.

Another social paradigm is the **initiative with regard to making or receiving a call**. In the telephone system of the 1980s, it was the user, and the user alone, who decided this. This could not be otherwise, for three reasons:

1. The electro-mechanical operation of this telephone was characterised by a contact in the handset. It was necessary to lift the receiver to hear a dialling tone and to have a dialling tone to dial a number.

2. The telephone service was paid for by the consumer. It would not have been acceptable for a third party to telephone at his or her expense.

3. Most of the time, telephone receivers remained on the hook. If everyone had used the line at the same time, the local exchange would quickly have been overloaded.

Terminals today (GSM, GPS, RFID, internet, etc) are always active. The charges are based on the duration of the subscription and not (or less and less) on the individual connection, and as the networks use packaging there is no longer a preliminary phase in which a communication circuit is established between two people. It is even possible to communicate with several interlocutors at the same time.

Here, too, the cookie is a symbolic focal point for this paradigm change. In the social imagination, surfing the internet depends on a "client/server" model that involves one party requesting information and the other supplying it. In this context, we have an actual inversion of the client/server paradigm, where the telecommunications terminal becomes a server of cookies addressed to other computers linked to the internet network. …/…

2.4.2. The complexity and opacity of the way terminals function

The **programming of telecommunications terminals** is becoming more and more complex. This complexity is made possible by miniaturisation. Each terminal has become an immense labyrinth whose layout is even incomprehensible to its own owner. In addition, the current trend is for telecommunications terminals to update themselves automatically, which means that this complexity is not stable over time. Moreover, for the closed code systems, it is virtually impossible to know the functionalities of a particular system or to know everything that is happening inside a computer.

This complexity has a price that is paid by the user. Securing the successive versions is not carried out in accordance with standard rules by implementing a rigorous test plan in advance of the market launch but by the users at the market launch.

While ensuring respect for privacy is considered part of software engineering, its integration into the telecommunications product puts the ICT industry at a threefold disadvantage:

1. First of all, it is necessary to develop quality monitoring methods relating to this criterion, which slows down the launch of new software onto the market. In the current situation, this would presuppose the complete re-engineering of the telecommunication protocols, which were designed somewhat naively without anticipating the current dangers and leaving data protection a possible option at the industry's discretion.

2. Secondly, by making the telecommunications terminals less “talkative” some companies are deprived of valuable information and of advertising income in proportion to their “visitorship”.

3. Thirdly, any security measure (and respect for privacy is one of them) generally represents a loss of speed and functionality to achieve a benefit that users rarely comprehend.

In practice, **telecommunications terminals have become remote-controllable and extremely talkative.** Many of the ways in which terminals behave would be totally unacceptable today if their users knew about them. To illustrate our argument and demonstrate its validity, we decided to conduct a thorough, precise and in-depth analysis of the flows of information between an average surfer who consults an online newspaper and clicks on two particular articles and the network.

In order to conduct this examination, we carried out a minor paradigm change. We used a network “sniffer”, which is a type of programme widely used by the administrators of big computer systems to examine the network traffic and perhaps detect attacks or anomalies. In our approach, we have adapted this tool to make it work on a surfer’s computer in order to visualise the traffic entering and leaving the terminal.

The aim here is not to put a specific online newspaper in the dock but to illustrate in a representative way the manner in which many sites operate and, above all, to show how technology **surreptitiously** permits this type of behaviour. In the following, we shall show that simply surfing the internet with the help of a standard navigation programme does not correspond to any of the functional characteristics of the telephone of the past.

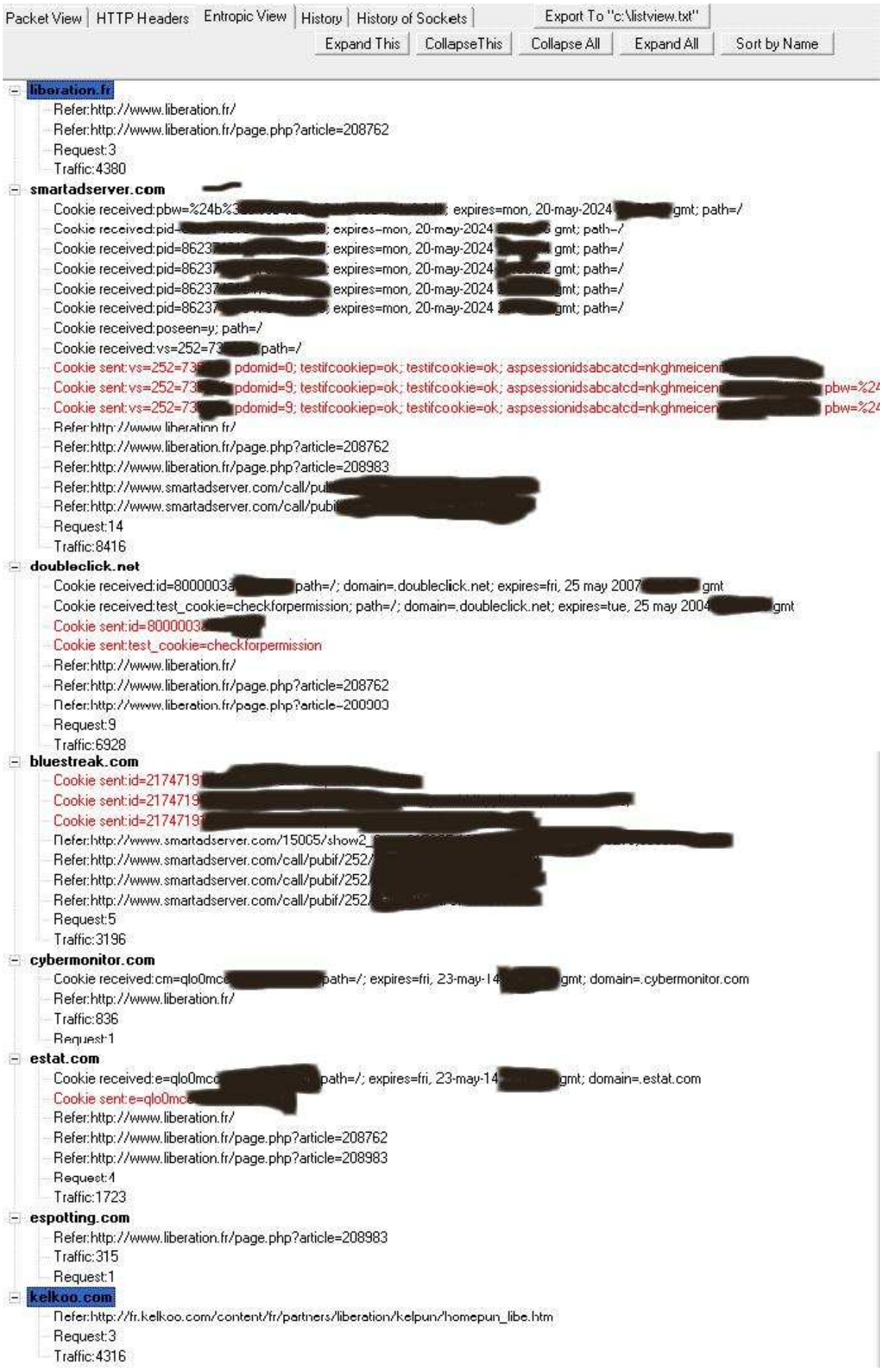
Basing our study on the use of the HTTP protocol by the online newspapers, our intention is to show that this control no longer exists. For this purpose, we describe the actual data flows when an online newspaper is read. What we detail is the normal “daily” experience of the readers of an online newspaper, but it could be transposed to a visit to a portal or a search engine.

1. The navigation software (Microsoft Internet Explorer 6) connects the user on request to the web site concerned but also, at the request of the site visited, to certain other sites in respect of which the newspaper has inserted links into its pages. The user has no means of preventing these connections; they are not visible and he or she is not aware of them.

2. By connecting up to these third parties’ sites, the navigation software will, invisibly, indicate the reference page in its HTTP header, ie it will communicate to this site the precise reference (URL) of the article currently being read.

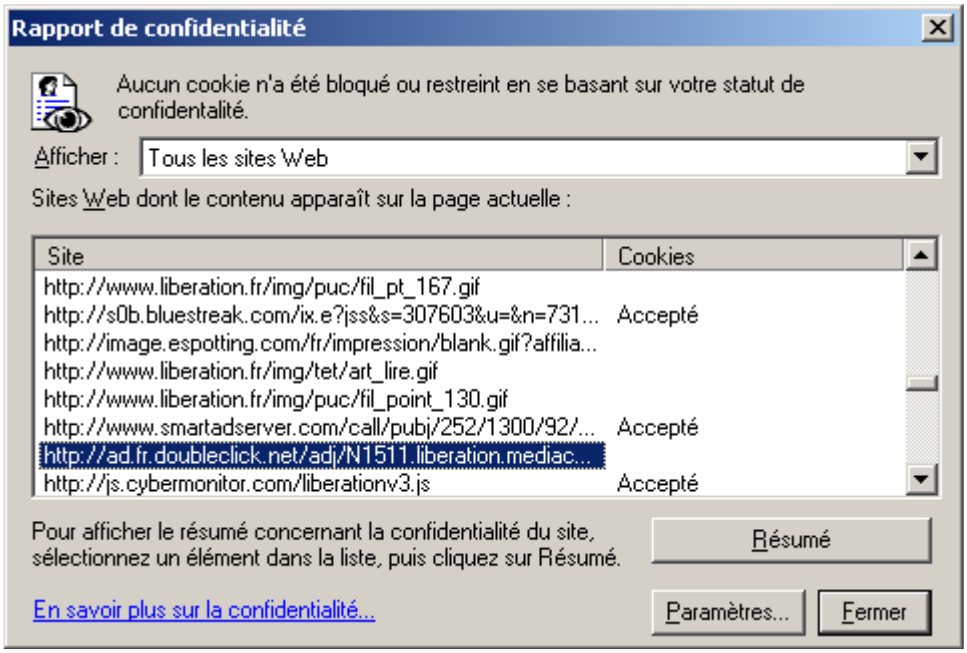
3. When it responds to these invisible HTTP requests sent by the user, the third-party web site employs the cookie technique to write on the user’s hard disk a unique serial number that the navigation software will systematically recall with every reconnection to this site. This unique serial number has a life of between three and twenty years.

4. The user has done three positive things (typed in the address of the newspaper and hit the enter key, clicked on an article, and then another), the navigation programme has performed the three requests (taking up 4380 bytes) but the navigation software has also, unseen, performed 37 requests (accounting for 25730 bytes). And while doing this, ten new identifying cookies will have been received, all in less than 5 seconds.


Packet View
HTTP Headers
Entropic View
History
History of Sockets
Export To "c:\listview.txt"
Expand This
CollapseThis
Collapse All
Expand All
Sort by Name
liberation.fr
Refer:http://www.liberation.fr/
Refer:http://www.liberation.fr/page.php?article=208762
Request:3
Traffic:4380
smartadserver.com
Cookie received:poseen=y; path=/
Request:14
Traffic:8416
doubleclick.net
Request:9
Traffic:6928
bluestreak.com
Request:5
Traffic:3196
cybermonitor.com
Refer:http://www.liberation.fr/
Traffic:836
estat.com
Refer:http://www.liberation.fr/
Refer:http://www.liberation.fr/page.php?article=208762
Refer:http://www.liberation.fr/page.php?article=208983
Traffic:1723
espotting.com
Refer:http://www.liberation.fr/page.php?article=208983
Traffic:315
Request:1
kelkoo.com
Request:3
Traffic:4316

Actual and invisible traffic when a visit is made to the home page of an online newspaper and the visitor clicks on one of the articles. (May 2004)[26]

It should, however, be pointed out that MSIE version 6 enables a "confidentiality report" in the following form to be displayed[27]



(Translation) Confidentiality report

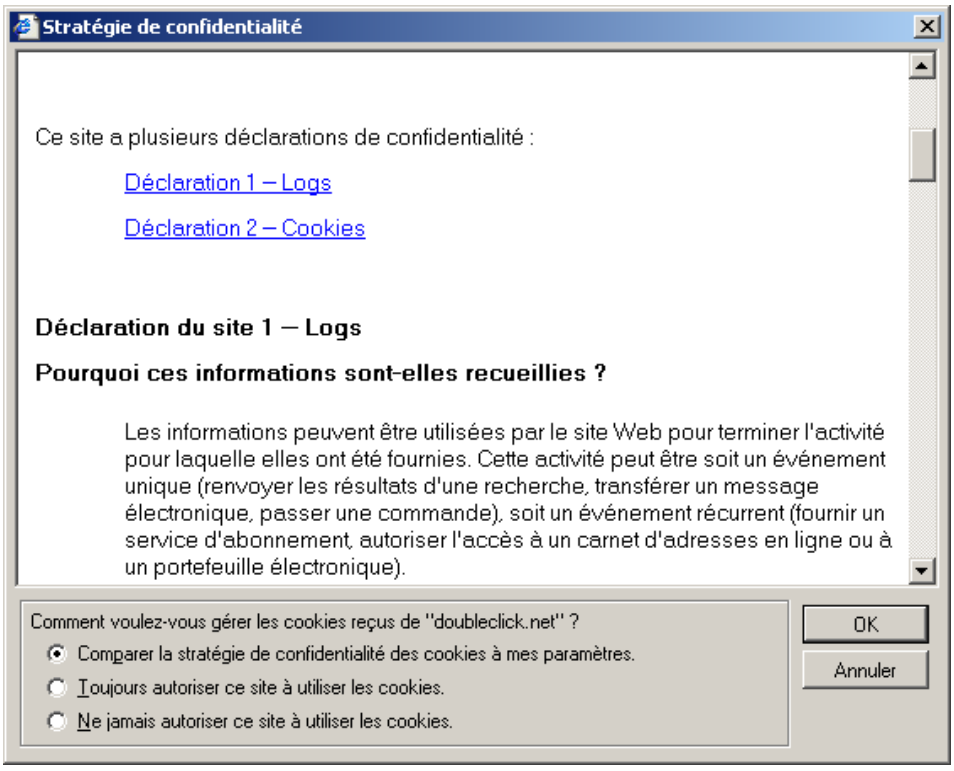
No cookie has been blocked or restricted on the basis of your confidentiality status.
Display: All web sites
Web sites whose content appears on the current page
…. Accepted
To display the summary relating to the confidentiality … Summary
of the site, select one element in the list and click on Summary.
Click here to find out more about confidentiality Parameters Close

In order to find out about a third party's privacy policy, it is therefore necessary to display this window *afterwards* and click on the Summary button. The privacy policy then appears in a narrow window that cannot be enlarged or printed (copy/paste is not possible). The following window is displayed[28]:

[26] Software used: Internet Explorer version 6 FR with the latest updates (patches). Level of confidentiality and security switched to Medium (by default) with prior emptying of the cache and deletion of the history and the cookies.

[27] We believe the "ordinary" web user has neither the time to consult this report *afterwards* nor the technical skill necessary to interpret it.

[28] For technical reasons, the complete privacy policy is annexed to this report.



(Translation) Confidentiality strategy

This site contains several confidentiality declarations
Declaration 1 - Logs
Declaration 2 – Cookies
Declaration 1 – Logs

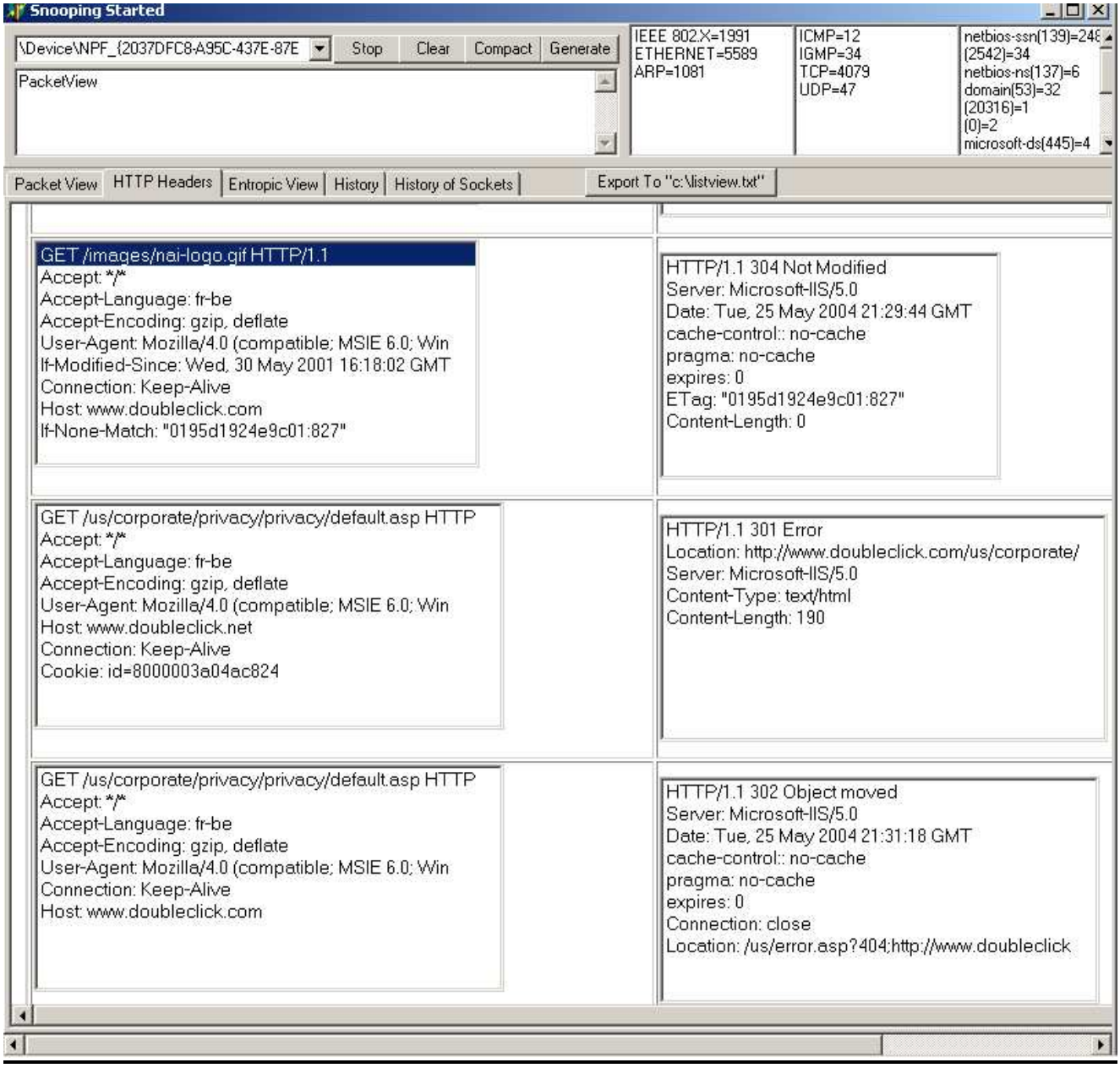
Why is this information collected?

Information may be used by the web site to complete the activity for which it was provided, whether the activity is a one-time event, such as returning the results from a web search, forwarding an e-mail message or placing an order; or a recurring event, such as providing a subscription service or allowing access to an online address book or electronic wallet.

How do you want to deal with the cookies received from doubleclick.net? OK
Compare the cookie confidentiality strategy to my parameters Cancel
Always authorise this site to use the cookies
Never authorise this site to use the cookies

It should be pointed out that the mere reading of this privacy policy triggers the downloading via HTTP of an image on the web site of the third party concerned (in this case DoubleClick), which can thus establish the number of times certain visitors have read this privacy policy and certain data relating to them.

If users wish to have more information on the privacy policy, they can click on a hyperlink that, before directing them to the privacy policy at a site without a cookie, will take them via a specific URL belonging to the third party where their browser will communicate their unique identifying cookie.



This shows that the interest of these firms is not only limited to establishing the content accessed by an individual online, the keywords entered into the search engines or access to portals (via precisely the same technology). Their ultimate aim is also to establish the importance that people attach to respect for their privacy and their level of technical competence. It should be pointed out that people who do not want to receive this identifying cookie from DoubleClick can effect an opt-out, which technically involves authorising DoubleClick to store on the terminal a persistent cookie stating that no cookies other than this one will be accepted. Is it only possible to protect one's privacy by having one's details recorded by a marketing company?

2.5. THE PARTICULAR CASE OF RFID CHIPS

Strangely enough, RFID chips, *like chip cards*, originated from the application of Moore's law: if the power of microprocessors goes up and their price comes down, the result will be a phenomenal drop in the price of processors at constant computer power. For example, some chip cards are equipped with the processor with which the famous Apple II computers were fitted at the beginning of the 1980s. These computers, which is what RFID chips amount to, possess the following characteristics:

- a processor
- a read only memory
- an antenna that makes it possible both to communicate with a terminal and receive the energy required to make the computer work
- absence of input/output devices accessible to a human being
- a very high degree of miniaturisation (of the order of a few millimetres, including the antenna)

The RFID market is assuming worldwide proportions in its efforts to identify and track most goods. Cases cited include Benetton shirts or Gillette razors[29].[30]. The arguments generally put forward are the drive to eliminate shoplifting and a more intelligent ambient environment that would enable even the most unimportant objects to communicate with their user. The serial number could also be used by embedding it into the chip sealed into the item.

By control, we mean an effective and practical threefold ability[31] to

1. see and understand what is transmitted (sent and received) online by a terminal;
2. reject the transmission (sending and receiving) of content online by a terminal;
3. if possible, repair an erroneous transmission.

Like cookies, RFID chips present a problem for the advocates of data protection because the opacity of such chips has reached maximum level. RFID chips are an extreme example of the absence of user control over the communications terminal: the user cannot know whether or not such a terminal exists, where it is located, what it contains or what it is transmitting. He or she cannot even switch it on or off. There is nothing visible to show that the RFID chip has been activated.

In conclusion, it has become and will become more and more possible to record the details of all the individuals on our planet and this will be less and less visible.

---

[29] The underlying aim is ultimately to be able to identify in a uniform way at the global level all the items produced by industry, and there is clearly an incidental temptation to try to identify human beings continuously and establish a relationship between the two enormous databases. As the impressive report by the Commission Nationale de l'Informatique et de Libertés (CNIL) on this subject states, "*At the global level, the goal is to code 50 to 100,000 billion objects, considering that a human being is surrounded by an average of about 2000 objects"*.

[30] The RFID codification system reveals its intention. The EAN (European Article Number) code is made up of 96 bits of which the last 36 are reserved for the article's serial number. The aim is therefore to permit the individual identification of 16 billion identical items (of the same type and products of the same firm). While it is impossible to imagine what company could produce 16 billion identical items or what value there could be in distinguishing between these billions of identical items if need be, it may be noted that this figure is the likely size of the global population in the coming decades.

[31] Aware that, in theory, practice follows the same course as theory but in practice this is never the case.

3. The actors

3.1. Absence of a government policy for overseeing the NICTs

The telephone network has a long tradition of protecting privacy. When the digital telephone (ISDN) was deployed, particular attention was paid to the efficiency of certain services (especially the possibility of suppressing the number of the outgoing line[32]). The implementation of these additional services was incorporated into the technical standard itself and compliance with these technical standards was a condition for the approval of the telecommunications terminals, and therefore their distribution.

Telecommunications via the Internet have been made possible by the development of micro-computer technology and the digitisation of global telecommunications networks. Unlike the telephone, and despite their functional convergence and the fact that they can be used in similar ways, a personal computer with its hardware, operating system and telecommunications software is subject to no operational or functional regulations with regard to the need for confidentiality or user control. This does not mean that some sort of control by an informed user is impossible but rather that such control is complex and is restricted to certain operations.

It is only sparingly and often in response to pressure relayed by the media that the industry grants partial control of terminals and the hidden ways in which they operate. Navigation programmes remain, in the view of one data protection expert, very unequal. While they all incorporate today sophisticated cookie management systems (distinguishing between cookies from third party sites and others), the sending of the reference page to third party sites is still overlooked by the most commonly used navigation programme, which, by default, still enables third party sites to store a unique global identifier on the Internet user's terminal.

3.2. Absence of rules governing the new telecommunications operators

In the 1980s, telephone traffic, like the postal services, was mostly handled by national operators (at least in Europe), most of which had a decades-long tradition and enjoyed a monopoly.

The development of the internet and the liberalisation of the telecommunications sector led to the appearance of new companies set up by as many new players. The latter are responsible for conveying telecommunications but are subjected to less formal controls than their predecessors.

At the moment, any company can become an internet access provider and thus be in a technical position to observe or record telecommunications. There can only be compliance with binding data protection standards if the telecommunications intermediary sector is professionalised at the same time, which presupposes training, access to the market and controls.

---

[32] CLIR ofr Calling Line Identification Restriction

4. Conclusion of part I.

The last two decades have seen an incredibly fast succession of an impressive number of innovations and technological trends that have led to the forming of a global telecommunications network. This technological development has taken place on an international level without any government or civic movement playing a decisive role and without the problems of a reduction in privacy brought about by these networks being tackled or resolved from the technical point of view.

- **Convergent, multifunctional and omnipresent networks in day-to-day life**

The network is multifunctional and tends to link together all existing telecommunication networks. It has invaded our environment and with each passing day it will make further inroads into numerous fields and the objects surrounding us. Many activities which in the past were carried out without any telecommunications network will require such networks to be used in the future. It is not at all unreasonable to think that, in a few years time, most refrigerators will be equipped with intelligent components which will know exactly what food is stored in the refrigerator and when it will be past its sell-by date (thanks to RFID chips). These "intelligent" refrigerators would even be able to take the initiative of displaying on the family TV set targeted advertisements or indeed of contacting supermarkets to obtain offers or order goods. In general, there is a clear tendency to make the objects surrounding us more intelligent by equipping them with a telecommunications terminal.

- **Intelligent terminals, operating in an opaque and complex way, making optional data protection possible.**

Today, computers make up the vast majority of telecommunications terminals. Being based on computers , these terminals generate, in a manner completely invisible to their users, many tracks of the telecommunications that pass through them. These tracks are either stored within the terminal or sent over the network, usually without informing the user. The technical means placed at the users' disposal are incomplete, too complex and configured by default in a way detrimental to the protection of the web surfers' privacy. Respect for privacy has become an option accessible to people with the time and the knowledge at their disposal. The individual's relationship with the protection of his or her data has itself become an item of personal information that many players want to possess.

Telecommunications terminals incorporate various technical identifiers that make it possible to "track" the behaviour of the individual on the network. Most industry players do not consider this tracking process a violation of the privacy of the individual if the latter cannot be identified by a contact point. Cookie technology enables a third-party web site, by default, surreptitiously to insert its own identifier into the terminal on a permanent basis so as to be able to track an individual's behaviour on the internet.

Telecommunications protocols do not include data protection as a key requirement but as an option generally left to the discretion of manufacturers of the hardware and of the software that incorporates these standards.

- **New telecommunications operators**

The telecommunications operators are market newcomers and lack professionalism and training with regard to the protection of privacy. There are no binding rules that make a knowledge of

data protection a key requirement for being allowed to access the occupation of a telecommunications operator.

Avenue of inquiry for the first part

Only by devising a workable data protection model and imposing operational rules for terminals, protocols and telecommunications operators will the protection of privacy on the "network of networks" take a decisive step in the user's direction so that it ceases to be a privilege partially granted on demand to an informed, demanding – and identified – minority.

II. THE NEW TECHNOLOGICAL ENVIRONMENT PROMPTS SOME THINKING ON HOW CERTAIN CONCEPTS AND PROVISIONS IN THE CONVENTION SHOULD BE CONSTRUED.

We are concerned here with answering a key question: do we need specific legislation on data protection in the information society that differs from Convention No. 108 and its additional protocol adopted on 8 November 2001 or is it sufficient to develop the principles of this Convention in order properly to cover the data protection issues associated with the development of the information and communication technologies?

Our reply is based on the text of the Convention and follows the same layout. In our critical appraisal, we also wanted to take account of recent texts more specific to the new technological environment created in particular by the development of the internet. Recommendation R(99) 5 of the Committee of Ministers to the member states on the protection of privacy on the internet, which was adopted on 23 February 1999, and the EE Directive 2002/58 have naturally been taken into account since they represent a first step in considering this new situation. As we shall see, some aspects considered by these new texts lead to the establishment of new principles, and this will be the subject of this third part.

1. Article 1 - Object and purpose of the Convention

1.1 THE AIM: DATA PROTECTION: BEYOND PRIVACY?

"Privacy has a protean capacity to be all things to all lawyers." [33]

1.1.1. From a debate on privacy to a debate on freedoms

Should the definition of the aim of the Convention 108 – "respect for (each individual's) rights and fundamental freedoms, and in particular his right to privacy" – not demonstrate more clearly the broadening of concerns inherent in the concept of the right to data protection? Here, legal writers[34] note the transition from a negative and narrow approach where privacy is considered a defensive and reductive concept (sensitive data), which makes it possible to protect the citizens from action by the state and from breaches of data confidentiality governed by Article 8 of the European Convention on Human Rights (ECHR) to a more positive and much broader approach (defined as a "right to informational self-determination") by assigning to the individual new subjective rights (right of access, etc) and determining limits to the right to process data on the part of public and private players (legitimate purpose, proportionality, security, etc). It is this new approach that is reflected in Convention No. 108.

Convention no.108 clearly reflects this more positive approach by strengthening the means available for citizens to monitor the processing of their data by granting information and access rights and setting out the limits to the file controller's right to information. Is this approach sufficient or is it necessary to suggest a third one, without departing from the Convention?

---

[33] T. Gerety, quoted by D.J. Solove, Conceptualizing Privacy, 90 California Law Review, 2002, p. 1085 f.

[34] D.J. SOLOVE, "Conceptualizing Privacy", 90 *California Law Review*, 2002, 1085 et s.; P.BLOK, *Het recht op privacy*, Boom Juridische uitgevers, 2003.

As we have pointed out, the technologies, more as a result of their implementation than out of necessity, produce and preserve a "trail" of the use of services and make it possible to gain a knowledge of individuals and their individual or collective, personal or anonymous behaviour because processing capacities are incomparably larger than those that existed just ten years ago. In other words, their use increases the imbalance between those who possess the information and the citizens, whether or not they are data subjects. On the basis of information gathered, collective decisions (for example, fixing the reimbursement rate for the costs of treating a disease) or decisions on specific individuals (such as the refusal to grant a loan or provide a banking service) will be taken.

The European Human Rights Charter (Treaty of Nice, 2000) calls, within and beyond this context, for a better distinction to be drawn between the concepts of privacy (Article 7) and data protection (Article 8)[35]. The first concept, which is more defensive in nature, constitutes the negative approach already described, limiting as it does the file controller's right to process sensitive data and preserving the privacy of the persons concerned *(the right to be left alone)*. The second concept calls for a consideration, on the one hand, of the imbalance of power between the data subject and the file controller brought about by the data processing capacities at the latter's disposal and, on the other hand, the impact that the processing may have on the citizen's freedoms, such as freedom of movement, freedom to insure oneself, freedom to house oneself, freedom to inform oneself, freedom openly to express one's opinions, etc.

Accordingly, the creation within inter-company or inter-authority database networks that permit the a-priori profiling of service users can lead to the latter being discriminated against when they are looking for accommodation, seeking information, applying for insurance or acquiring a book[36].

Avenue of inquiry

Does this fact not call for a more preventive and comprehensive approach to the problems observed that is centred on the impact of technologies on human freedom[37] ? This approach would be based on the precautionary principle, which was developed in the environmental field and also focuses on collective risks. It is clear that this role of "technology assessment" is already being played by the bodies responsible for dealing with data protection, especially the Consultative Committee. We are simply calling for greater emphasis on the preventive character of the intervention desired and on an analysis of the impact on citizens' individual or collective freedoms of innovations that have been put or are likely to be put on the market.

1.1.2. The preservation of human dignity over and above the protection of personal data?

---

[35] Article 7: "Everyone has the right to respect for his or her private and family life, home and communications"
Article 8(1)"Everyone has the right to the protection of personal data concerning him or her."
(2) "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."
(3) "Compliance with these rules shall be subject to control by an independent authority."

[36] On this last point, Amazon's "discriminative pricing" practices have been condemned by American consumer associations and have now been abandoned.

[37] To take just one example: the gradual replacement of traditional methods of payment by credit cards, the issuers of which form an oligopoly, calls both for a consideration of the possible impact on citizens' freedom of movement and an analysis of the uses of the card in terms of the general surveillance of the individual's activities.

The Convention guarantees not only the protection of privacy and freedoms but also the **protection of human dignity.** In the German constitutional tradition, the question of the protection of personal data is bound up with the individual's right to human dignity. The reference to human dignity serves as a reminder that the human being is a subject[38] and cannot be reduced to a simple object of surveillance and control. This reminder to respect dignity as a fundamental value of privacy[39] is no doubt necessary in the light of certain uses of technology. Information systems are to an increasing extent carrying out the comprehensive surveillance of populations and individuals, thus creating a system in which the transparency of personal behaviour may prove to be a violation of human dignity[40].

This addition proves necessary since information systems are increasingly permitting the comprehensive surveillance of populations and individuals, thus creating a system in breach of human dignity in which people's behaviour is transparent.

Avenue of inquiry

We are duty-bound to stress that these violations of human dignity may occur even if there is no "processing of personal data" (for example, the camera filming the way in which an unidentifiable person tries a tube of lipstick). The fact that dignity is affected by the gathering of data on individuals even if there is no risk of their being identified (apart from their behaviour which identifies them biographically (see below), must lead to a consideration of whether the principles of the Convention should be applied to this type of violation. Should attention not be drawn in this context to the principles of the legitimacy and proportionality of processing operations and to the right of those whose data have been collected to be given the relevant information?

1.1.3. Privacy as a basis for, or challenge to, other freedoms

It goes without saying that privacy or, on a wider scale, the protection of data, is a guarantee of our freedoms. To take freedom of expression or freedom of association, for example, how can one imagine these freedoms being able to survive if people know that their communications are being monitored and cannot express themselves anonymously at certain moments if the technology keeps systematic track of their messages? My freedom to inform myself presupposes that the information about me is not filtered, that I am not guided with the help of profiling and without - or in spite of - my knowledge to information that others want me to consume. Even worse, the same profiling technique can result in my being denied certain services or information that it is considered not worth allowing me to access. Many more examples could be mentioned with regard to the various freedoms enshrined in the European Convention on Human Rights. **The protection of data is undeniably the basis of several other freedoms that guarantee it.**

---

[38] Cf. the famous passage from Kant's Doctrine of Virtue in the context of human dignity: "A human being is not to be valued merely as a means to the ends of others or even to his own ends but as an end in himself; that is, he possesses a dignity (an absolute inner worth) by which he exacts respect for himself from all other rational beings. He can measure himself with every being of this kind and value himself on a footing of equality with them".

[39] On this relationship, see J.H. Reimann, "The Right to Privacy ", in *Philosophical Dimensions of Privacy* 272, published by F.D. Schoeman, New York, 1984, 300 ff.

[40] The case is cited of the Londoner filmed 300 times a day by videosurveillance cameras or the case of the employee wearing a tag that enables him to be located at any time during working hours and conclusions to be drawn from this with regard to his working or other relationships with other employees who have also been tagged.

However, the concern to protect data clashes with the development of other freedoms. In particular, **a balance must be struck between the requirements of the protection of freedom of expression and freedom of opinion.** The preamble to the Convention implicitly states this: *"Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples"*, but no provision of Convention No. 108 establishes the necessity for this balance[41]

Up to now, account has been taken of this concern not to violate freedom of expression and opinion through data protection by enacting a number of protective provisions governing the work of journalists, including the electronic sphere. It is becoming more and more apparent that the problem is more serious since the internet offers all its users the opportunity (web logs, personal web site, etc) to assert their opinion and inform others about their activities, including their relationships with third parties.

Avenue of inquiry

The application of data protection laws, with the many obligations this protection establishes vis-à-vis these third parties (such as the obligation to inform them) creates a tricky problem with regard to freedom of opinion and expression, which could be restricted. The Linqvist case recently decided by the European Court of Justice illustrates[42] this point. Can a person mention his or her personal, community or professional relations on the internet without having to meet the requirements of the law on the protection of personal data? The Court drew attention to the duty, in the light of the circumstances, to assess the proportionality of a restriction on the exercise of the right to freedom of expression, which entails the application of rules aimed at protecting the rights of others. The wording is vague and involves an assessment of proportionality. This judgment can scarcely equate freedom of journalistic expression, whether it be in a traditional format or on the internet, for which rules have gradually been developed[43], with everyone's free expression, the existence of which is necessarily connected with the freedom of others. Some work will no doubt have to be done on this point.

1.2. SCOPE: ENLARGEMENT RATIONE PERSONAE?

1.2.1. Extension to include legal entities

It is known that member states (Norway, Austria, Luxembourg, Italy to a lesser extent) have extended the scope of their data protection laws or some of their provisions to include legal entities. This extension corresponds to the latitude allowed by Article 3b of the Convention, which provides for the possibility of member states extending the protection "*to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality*".

---

[41] In contrast to the express reference to the processing of data "solely for journalistic purposes or the purpose of artistic or literary expression" in Article 9 of European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[42] ECJ judgment, 6 November 2000, published in RDTI, 2004, pp. 67 ff., with observations by C. de Terwangne, who deals fully with this question.

[43] It should be noted that national regulations vary in the way this balance must be achieved (cf. in this connection the paper by C. de Terwangne)

In the context of the development of new regulations, the question of extending the scope arises again. Thus, Directive 2002/58/EC seeks to enable legal entities to benefit from certain protective provisions – in the name of their so-called "legitimate interests"[44]. This extension concerns in particular the provisions relating to unsolicited communications, the confidentiality of communications and limits imposed on the processing of data and location traffic, but not unsolicited mailings or the receipt of cookies or other spyware[45]).

There appear to be a number of different reasons for this extension. Mention is made of the desirability of guaranteeing legal entities certain rights granted by data protection legislation to the persons concerned (right of access, right to information, right to correct errors) when there is too great an imbalance of information powers between legal entities and file controllers (for example, the case of SMEs vis-à-vis banks, insurance companies, administrative authorities, etc). The desire to protect legal entities, their members and, in particular, their freedom to associate is without doubt a primary reason. It has already been mentioned in connection with the first domestic legal provisions, which sometimes stress the difficulty of separating the existence of the legal entity from that of all or some of its members.

As far as the solution proposed by the directive is concerned, other reasons can be considered: the processing of traffic and location data provides those who handle the information with a considerable knowledge of the activities of legal entities and the people responsible for processing the data. In short, it is the risk run by legal entitles of being subjected in the same way as individuals to the power of those who will have this information at their disposal that justifies extending the scope of the provisions relating to subscribers to cover legal entities. The fact that unsolicited communications involve considerable costs both for natural persons and legal entities would justify the same extension.

Avenue of inquiry

The merits of this extension to include legal entities among the beneficiaries of data protection legislation or some of its provisions should be reassessed in the context of the new uses of the networks. In conclusion, it would be worthwhile for the Consultative Committee to compare the risks that are mentioned as justification for the extension being debated and to inform the Council of Europe of whether such an extension is appropriate.

1.2.2. Extension to include profiles

The second point is more difficult: should provisions to protect profiles be envisaged that go beyond the protection of individuals[46]? Profiling consists of two stages: firstly, the determination of a series of characteristics relating to an individual or group of individuals in connection with one or more demonstrated or expected behaviours and, secondly, the subsequent processing of the data of these individuals or group on the basis of the recognition of these characteristics. Each of these stages is important.

---

[44] On this protection of legal entities and associations, see in particular L. Bygrave, *Data Protection Law*, Kluwer Law International , Information Law Series, Den Haag, 2002, pp. 173 ff.

[45] Cf. in this connection the arguments put forward by J. Dhont and K. Rosier in "Directive Vie privée et communications électroniques: premiers commentaries", *Revue Ubiquité-Droit des technologies de l'information*, 2003, no. 15, p. 7 f.

[46] It should be noted that these regulations exist in Switzerland and to some extent in Norway. On these points, see L. Bygrave, op.cit., p.185 f.

The possibility of gathering data relating to present or past behaviour or personal or anonymous data in ever larger quantities and ever better quality and processing it in more and more detail generates ever greater risks of creating profiles and taking a-priori decisions in the light of these profiles[47]. Accordingly, the way in which a surfer navigates a company's website can be characterised by a number of criteria that will enable him or her to be classified in a particular category[48] after a few visits have been made, to display a page in preference to another when a contact is made[49], and even to deny him or her a service.

This problem of the sharing of power associated with the sharing of information can also be observed in connection with online profiling. Today, the ambition of commercial companies is no longer to make a simple sale but, rather, to succeed on the occasion of a first sale in gathering a maximum amount of information in such as way as to prepare subsequent sales. Information relating to customers makes it possible to calculate the elasticity of demand and accordingly vary prices **individually**. Amazon, for example, has been suspected of practising so-called "adaptive pricing" by using cookies that identify a potential buyer's profile in order to revise its prices upwards according to that person's supposed profile. In economic terms, a single price is unlikely to maximise a company's profits because most buyers have different price elasticity curves. Profit maximisation is achieved when each product is sold at the maximum price that an individual is prepared to pay. In the opposite case, the consumer usually enjoys what economists call the "consumer rent", which is the advantage gained by paying a fixed price for an article when he or she was actually prepared to pay a higher price. In terms of economic power, profiling is a technique that can enable the seller to appropriate the consumer rent in order to maximise its profit.

---

47 R. A. CLARKE, "Profiling : A hidden Challenge to the Regulation of Data Surveillance", 4 *J. of Law and Information Science*, (1993), pp. 403 ff.

48 In many cases, especially marketing, the aim of statistics is to be able to derive the probability of certain not directly observable characteristics from observable and pre-aggregated data. When they grant loans, banks normally carry out a credit rating based on a set of innocuous questions that will enable them to determine whether *statistically* the prospective borrower fits the profile of a creditworthy customer. Let us take a random example. A man in a time-limited post on average pay is given a permanent job with better pay with a good employer. He moves home in order to be closer to his work and does not yet have a telephone. With a view to granting him a loan, the bank asks him three questions:

- Has he or she been with the same employer for a long time? Response: no
- Has he or she been living in the same place for a long time? Response: no
- Does he or she have a telephone ? Response: no

The obvious conclusion to be drawn from this is that the bank is confronted by an individual who keeps changing jobs and moving home and does not even have a telephone. This is the classic profile of the person who does not repay a loan. In other words, the bank has an interest in turning down this type of customer because in general it is these people who pose the biggest problem. The fact that a specific case happens to contradict this theory does not detract from its overall validity if the reasoning is generally correct and if studying borderline cases involves a certain cost. In other words, hasty and sweeping conclusions (eg, he has a Rolls-Royce so he is rich) the effect of which is to exclude access to certain goods or services for people with objective characteristics are justified from the economic point of view of profit maximisation, even if they result now and again in unfounded exclusions. It is sufficient for the exclusion to be by and large profitable. It is clear that excessive profiling makes, and will make, this type of automatic exclusion possible, without any opportunity for the atypical individual to mount a serious challenge.In many cases, statistics are personal data when they are "reapplied" to an individual on the basis of some of his or her observable characteristics in order to infer from them others that are not.

49 Even if it is only the homepage in the surfer's language so as to save him or her from having to repeat this choice, but also to select the news or advertising according to the individual's preferences or even to offer prices for goods or services based on the features of his or her profile. It should be noted that surfers are sometimes asked to help the service provider to target them better so that they can respond more appropriately to all their needs, including sexual. This ever more sophisticated a-priori profiling is the basis of the entire development of one-to-one marketing.

This interpretation of the Convention in terms of the balance of the power generated by information relating to individuals shows very well that the Convention's objective of restoring the balance can only be achieved if "anonymous"[50] profiling is removed from its scope.

In the public sphere, centres of expertise and statistical institutions are similarly tasked with gathering information of a diverse nature from various sources in order to establish profiles and thus help the authorities take their decisions or monitor compliance with them[51]. It will thus be possible to establish the profile of the fraudster and then identify in multiple and, as the case may be, interlinked databases the people to be watched regarding matters to do with social security or tax legislation.

Avenue of inquiry

It is therefore important that, irrespective of the personal nature of the data processed, certain rules are laid down with regard to the establishment of profiles (first stage) independently of their subsequent application in a second stage to individuals[52]. In this connection, these rules can be developed from the principles of modern data protection legislation. For example, consideration might be given to obliging those who establish profiles to inform the group concerned of the rationale behind the processing even before any application. The principles of the legitimacy and compatibility of purposes with regard to the use of the profiles that it is planned to produce and the principle of the proportionality of the data gathered to characterise these profiles could also prove relevant, as could limits to the use of data referred to in terms regarded as sensitive according to the Convention. Finally, consideration could be given to transposing to private players rules developed in connection with public statistics, where committees made up of statistics users, representatives of the supervisory authorities etc meet to analyse statistical programmes and their rationale (principle of user participation).

2. Article 2 – Definitions:

2.1. THE CONCEPT OF PERSONAL DATA (ARTICLE 2A))

This concept is based on the identification or "identifiability" of the individuals concerned by these data. In principle, data protection regulations are only applicable if the data processed can be related to a specific person[53]. However, the concept of identity is unclear in relation to certain new situations. For example, is the RFID that tracks an item of clothing[54] an item of personal data when it at least relates to an object (like the IP number, which ultimately

---

[50] On this concept, see our remarks on the notion of identity below in respect of Article 2a) of the Convention.

[51] On these applications, see the prophetic article by J.Bing, "Three Generations of computerized systems for Public Administrations and some implications for Legal Decision Making", 3 *Ratio Juris* 1990, pp. 219 ff.

[52] Article 15(1) of European Directive 95/46 on the protection of individuals with regard to the processing of personal data does govern profiles but only at the moment when they are applied to a particular person. Article 15(1) demands that a person in respect of whom a decision is taken on the basis of an automated decision is informed of the rationale of the system applied to him or her and is able to challenge the application of the automated reasoning in his or her particular case.

[53] With respect to "profiles", we have shown that certain data processing operations can be dangerous even though initially no link with specific persons is established that would enable the processing to be subsequently (in a second phase) automatically applied to specific people and permit decisions on them to be taken.

[54] One of the first applications of RFIDs was the insertion of microchips into Benetton clothing.

relates to a computer and not a specific user)? We shall compare three aspects in respect of this question before suggesting some avenues of inquiry.

2.1.1. Identity: an ambiguous concept

The concept of identity is ambiguous because it can mean at least three different things:

1. a characteristic of a person that is a feature of his or her ***biography***[55] (for example, his or her age, transactions, family, hobbies, employer, professional qualification, removals, purchases, etc);

2. ***an anchor point***, ie an **identifier** that will enable several biographical characteristics of the same person to be linked together (for example, a session cookie, a customer number or a number identifying the terminal)[56]. The anchor point is not biographical as such but a pointer to a location where all the biographical data that comprise it can be stored. These pointers enable purely biographical data to be interlinked by bringing together in a single profile behavioural analyses of the same person at different locations and different moments.

3. a ***contact point*** that will enable a third party to take the initiative to contact an individual. (by e-mail, post, fax, telephone, etc).

The passage of time influences the quality of these data. For example, a dynamic IP address is an anchor point that lasts quite a short time. The word “address” is itself ambiguous as it signifies both an identifier of a specific person at a specific moment and a means of contacting him or her.

These three features of information remain conceptually separate even though they may in practice coexist or even be combined in the same piece of binary information.

In the physical world, postal addresses are vulnerable because they (and, to a lesser extent, electronic addresses) combine the three features mentioned above. A postal address consisting of the first name and surname, the street number and the locality is at the same time:

- a biographical element: by disclosing to a third party not only the place where the person lives but also, by implication, his or her standard of living (the neighbourhood where he or she lives) and ethnic origin (his or her name);
- an anchor point: by disclosing the same address to several third parties, it is technically possible for the latter to pool their information. If several people live at the same address and have the same surname, it can be surmised that they belong to the same family.
- a contact point: the postal address enables anyone to send mail to a specific person.

2.1.2. Identity given a narrow interpretation by industry

---

[55] In the etymological sense: it is a matter of recording a slice of life, and the thickness of this slice or, in more scientific terms, the graininess of the data will clearly be very important with regard to the subject we are dealing with.

[56] Typically the MAC address, the unique serial number identifying each network card or the IMEI number identifying every mobile telephone and transmitted over the network, etc. Historically, it may be noted that Microsoft programmed Powerpoint, Word and Excel in 1998 to store this unique number secretly in every document created by the user.

A significant case in point is that of Abacus. It was arguably popular pressure that prevented the merger between the databases of Abacus[57] and DoubleClick. It is indeed surprising that the merger between DoubleClick's "anonymous"[58] profiles and Abacus' nominal database should have been technically possible at all. This quite simply means that DoubleClick, which claimed it was not collecting any information relating to an identifiable person, nevertheless possessed an anchor point that enabled the link to be made. This link is very likely to be the famous identifying cookie that DoubleClick has installed on millions of personal computers[59]. It is enough for an invisible hyperlink to be present on a personal form online for DoubleClick to be able to make this link.

A current industry trend consists[60] in considering anchor points and simple biographical data linked to them to be unidentifiable or unidentified data relating to an individual[61]. Contact points that are stable over time are generally accepted as being personal data. In other words, the surveillance and traceability of an individual or goods that he or she uses or possesses are not seen by most people as a breach of privacy if the person concerned is not identifiable and remains anonymous (ie, if his or her identity is not known and people do not know how to contact him or her)[62].

As if our behaviour were not a constituent element of our identity.

2.1.3. Identity given a narrow interpretation by industry

Although it refers to privacy, European Directive 95/46 never defines the concept of ***personal data.*** These data are "*information relating to an identified or identifiable natural person*". It therefore remains to be established what "identify" means. The directive goes on to

---

[57] "A cooperative membership database, contains records from more than 1,100 merchandise catalogs, with more than 2 **billion** consumer transactions from virtually all U.S. consumer catalog buying households". Read at http://www.abacus-direct.com in May 2004.

[58] http://www.doubleclick.net/company_info/about_doubleclick/privacy : " *DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address.*

[59] DoubleClick serves more than a billion advertising banners a day.

[60] The Microsoft Update declaration of confidentiality is along the same lines. After stating that the site collects the following information:

1. Windows version number
2. Internet Explorer version number
3. Version numbers of other software for which Windows Update provides updates
4. Plug and Play ID numbers of hardware devices
5. Region and Language setting

The Windows Update Privacy Policy available on http://v4.windowsupdate.microsoft.com/fr/default.asp (last visit, 15 may 2004) states that the Windows operating system "*evaluates a Globally Unique Identifier (GUID) that is stored on your computer to uniquely identify it. The GUID does not contain any personally identifiable information and cannot be used to identify you*".

[61] See (J. DHONT, V.PEREZ, Y. POULLET in colaboration with J.REIDENBERG and L. BYGRAVE, *Safe Harbour Agreement Implementation Study*, study available on*:* http://europa.eu.int/com/internal_market/privacy/index_en.htm. ….)

[62] See DoubleClick's privacy policy: Do users have access to their personal information collected by the web site? **Answer: «** No personal information is collected, so none is accessible."

say that "*an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". Mention may incidentally be made of the pleonasm (a person is identifiable if he or she can be identified, directly or indirectly, in particular by reference to an identification number). "Recital" 26 states that "*to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*".

This concept of identity remains ambiguous and this ambiguity also remains tangible with regard to the way it was interpreted by various European countries when they transposed European Directive 95/46 into their respective national legislation. I shall take as examples the transpositions carried out by Belgium, the United Kingdom and Sweden.

Belgian law[63] defines as personal data "*any information relating to an identified or identifiable natural person ('data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". This is a carbon copy of the text of the directive.

The scope of the British legislation[64] is narrow because it states that "*personal data means data which relate to a living individual who can be identified - (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.*" (Section 1(1) of the UK Data Protection Act 1998). The Freudian slip may be noted. It could be said that data relating to an individual are not personal if the data controller cannot identify the person concerned. However, in this precise case there are no personal data, there is no processing of data and, consequently, there could be no "data controller"[65].

In Sweden, the Personal Data Act 1998 defines personal data as "*(a)ll kinds of information that directly or indirectly may be referable to a natural person who is alive*"[66]. Surprisingly, no mention is made here of the notion of identity. Implicitly, it could be thought that the Swedish law (which was intended to transpose European Directive 95/46) considers that information cannot be attributed to a natural living person without him or her being identified. On the internet, it is possible to imagine a customer who cannot be identified at all (for example, using an IP relay chain without weblogs) and is assigned a number of non-identifying cookies attesting to his or her homosexuality and interest in AIDS treatments. In the strict framework of Directive 95/46, the law would not apply to these two cookies because they do not relate to an

---

[63] Law of 8 December 1992, as modified by the Law of 11 December 1998. A consolidated version of this law is available at the web site of the Belgian Commission for the Protection of Privacy (HTTP://www.privacy.fgov.be).

[64] The UK Data Protection Act 1998 art 5 states that personal data means data which relate to a living individual who can be identified- (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller..."

[65] Here, the drafters have disregarded the precision introduced by Recital 26 of Directive 95/46. This leads to collateral damage: imagine the manager of a supermarket simply noting the registration numbers and types of the vehicles in the car park as well as their arrival and departure dates and times. Generally, it is not very likely that a supermarket manager will be able to go so far as to identify the person concerned simply from the registration number in his possession. This type of recording system would therefore not be covered by the British Act. There are no personal data, so there is no data processing let alone a "data controller". This system can be extended, refined and consolidated at the national level and this would provide a system that enables vehicles to be tracked via the car parks throughout the country. It is thus easy to imagine such a system on the internet in a data paradise, with anyone whatsoever being able to piece together the itinerary or even timetable of his or her neighbour, boss, lover or spouse.

[66] "All kinds of information that directly or indirectly may be referable to a natural person who is alive".

identifiable person. However, the web site (for example, one offering life assurance quotations online) that receives this visitor and his or her cookies could conclude, rightly or wrongly, that he or she has a relationship with a homosexual who probably has AIDS. The Swedish law, on the other hand, could become applicable if the feature "homosexual, probably with AIDS" is *attributable*, at the moment of the connection, to a living natural person, even if he or she remains unidentifiable.

Avenues of inquiry

In conclusion, it is clear that the Consultative Committee will have to deal with the concept of personal data, a concept that is the key element of data protection legislation, and draw up a recommendation on how to interpret it by taking account of internet service providers' identification practices. At this stage, here are a few initial remarks:

1. A definition of personal data based on the undefined and indefinable notion of identity and the pendant concept of anonymity is ambiguous and not directly workable. From the practical point of view, it would be better to refer to biographical data, identifiers linked to individuals or to terminals (indeed, objects), and points of contact.

2. Within the scope of our study, it should be noted that considering an item of data (such as a cookie, the IP or a GUI) as "personal data" will lead to the application of the provisions of the Convention and, accordingly, the obligation to process this data (if only to enable rights of access, etc), even though it would not normally have been processed. In addition, the application of the provisions, such as the obligation to inform the person concerned, could prove impossible without identifying him or her.

3. On the other hand, not treating the IP and the GUI as items of personal data would pose a problem in the light of the risks that the subsequent use of these data represent in terms of the profiling of the individual and, indeed, the possibility of contacting him or her. In this connection, there is evidence that, with the combination of web traffic surveillance tools, it is easy to identify the behaviour of a machine and, behind the machine, that of its user. In this way the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the "identity" of the individual – ie, his or her name and address – it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her identity. The definition of personal data should reflect this fact.

2.1.4. The particular case of traffic and location data: a specific regime?

Should traffic and location data be defined as data requiring specific controls?

These data are defined as follows by European Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector[67]:

- "traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing";

[67] Recommendation N° R(99)5 of the Committee of Ministers of the Council of Europe on for the protection of individuals with regard to the collection and processing of personal data on information highways gives wether any definitions nor particuler rules on this data type.

- "location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

With regard to location and traffic data, their special status in the directive can be put down to their purpose, which is limited from the outset: the conveyance of messages to or from the users of electronic communications services and the dangerous nature of the systematic processing of such data, which reveal these people's movements, consumption habits and lifestyle. Finally, it is stressed that the users of such a service, except in the case of value-added services, are in a position of relative weakness since the use of the network implicitly calls for the generation, storage and transmission of a large amount of technical data whose meaning and potential use they are unaware of and which they cannot easily track (see above and our thoughtson the operational opacity of the networks in Part I, 2.4.2.).

The Directive accordingly limits the processing of such data from the outset to just one exception: the data subject's duly informed and at any time revocable consent. At the same time, is not the main explanation for making the use of these data to provide value-added services contingent on the data subject's consent the fact that, since the consent can be easily given and withdrawn via the actual use of the technologies, it can be considered that this consent becomes the only basis for the legitimacy of processing operations relating to these additional services?

Avenue of inquiry

It would probably be worthwhile dealing with the particular issue of traffic and location data in a specific recommendation aimed at the designers of terminal devices that generate this information and for the companies that store it, namely the providers of networks and communication services offered to the public.

These are services that essentially or principally consist in the transmission or broadcasting of signals on the electronic networks.

The addition of this definition enables the regulation of these "providers", whose intervention between the sender of the message and its recipient is necessary, to be introduced (analogous to the former regulation of voice telephony operators and conveyors of mail, such as the post office). This regulation should specify the means of ensuring the confidentiality of correspondence and the limits to the right to process traffic and location data, compel providers to separate processings carried out in the context of services involving the simple conveyance of communications and added-value services (analogous to the ONP rules concerning the regulation of telecommunications), determine the rules for co-operation between public authorities and these providers in the case of procedures to investigate violations and, finally, impose on them an obligation to warn their customers of the privacy risks involved in using their services.

2.2. THE CONCEPTS OF DATA FILE (ARTICLE 2B) AND AUTOMATIC PROCESSING (ARTICLE 2C)

According to the Convention, the definition of processing does not extend to the data gathering operation. Is this a gap that needs to be filled? Article 5 does state that the data must be obtained fairly and that the processing may only comprise the storing of the data, but when information is gathered on the web or via one of the internet protocols it is always at least stored in the computer's random access memory (RAM).

Avenue of inquiry

In addition to this initial observation, two issues should be dealt with.

Firstly, is pure surfing not data processing or does it not constitute the implementation of the ultimate aim of those who have put the pages on the internet or, more particularly, of the transmission operation, which is the last phase of the processing? It is clearly impossible to apply data protection legislation to someone who simply surfs the internet (obligation to inform the persons concerned, obligation to report, etc) and it is also obvious that the data have nevertheless been briefly stored and processed, as we shall show in response to the second question.

Second question: many pages of sites accessible on the internet contain personal information (pictures, texts, sound tracks). Does the mere presence of all this information render the Convention applicable or is it necessary for the data to be to some extent organised and structured according to the persons concerned or for logical or arithmetical operations at least to be applied to all this personal information in such a way that the data relating to an identified or identifiable person can be more easily gathered? In our opinion, mere sequential visualisation (eg, a football match transmitted over the internet) does not constitute processing if it is not possible to conduct operations relating to personal data contained in the pictures concerned (for example, image scanning that permits the automatic recognition of individuals). In order for there to be processing, it is not enough for information relating to individuals to be present but, rather, it is necessary for operations to be applied to this data (value-added principle). It will no doubt be objected more and more application software is available for our computers and permits the structuring of previously unstructured information or that such services are offered at the same time as access to a database. For example, word- or name-based searchware enables a search of huge amounts of freely available texts to be made to identify the appropriate passages relating to a specific person. Its availability, indeed its potential application, then results in the recognition of the existence of processing operations. Given the constant development of technology that makes possible today what could be imagined yesterday and will enable us to imagine tomorrow what was inconceivable yesterday, it is becoming increasingly rash to believe that that this or that processing operation will be technologically unfeasible.

2.3. THE "CONTROLLER OF THE FILE" (ARTICLE 2D)

The definition of the term "controller of the file" involves an analysis in the present case of the person responsible for defining the purpose(s) of the processing, the categories of data processed and the operations to be applied. In the context of co-operative networks, it is quite common for the participants in these networks to entrust tasks of common interest to a body charged with offering value-added services to all the participants. For example, hospital doctors and general practitioners can store their medical files at a central location, have their mail sent via this body, which will also provide archiving and time-stamp services, have resources made available to them by this body for processing medical imagery, etc.[68]. The status of these bodies is difficult to perceive with regard to the concept of the "controller of the file". Given the variety

[68] On this situation and the significance of the concept of "processing" in this area, see J. Herveg and J. M. van Gysegheim "La sous traitance des données du patient dans la directive 95/46", in Lex electronica, 2004, n°9, available at: http://www.lex.electronica.org.

of services they provide, should we consider them as controllers or mere processors, which is a notion not envisaged by the Convention but is contained in Directive 95/46[69]?

Avenue of inquiry

A definition of this and the establishment of a number of principles concerning the responsibility of subcontractors and links between them and the controller are necessary as soon as situations that can be described as involving subcontracting proliferate in the network and among the services offered by it.

It would be worthwhile considering the status of the person who is the subject of personal data as the controller of the file, or at any rate the co-controller of the file, in certain cases where the person whose data are processed specifies the purpose of the processing and the means employed. For example, is not the person who entrusts certain data to an infomediary in order to have them processed in such a way as to prevent some commercial solicitation or other and to filter certain messages within the meaning of the Convention a controller of the file who turns to a subcontractor in the person of the infomediary? Similarly, how can someone be described who asks for a medical record to be produced in order to have these details more easily available to show the doctors of his or her choice? The consequences and advantages of such a description should be carefully examined.

2.4. A NEW CONCEPT TO BE ADDED: MANUFACTURER OF TERMINAL EQUIPMENT

Avenue of inquiry

The idea is to add to the present Convention No. 108 a special system that imposes on manufacturers of terminal equipment (including software elements incorporated into the terminal) certain obligations aimed at the transparency of its operation and preventing the unfair or illicit use of personal data associated with the connecting to and communicating with the network. It should be noted that these manufacturers are not covered as such by the present directive since they are not controllers of a file. However, as the design of the equipment they supply authorises many processing operations, certain security responsibilities should be imposed on them so as to prevent those operations that could be carried out by third parties in an unfair or illicit manner, and they should be required to ensure transparency since the user of the equipment must be able to exercise a certain amount of control over the data flows generated by its use (see remarks above concerning the user's right to transparency).

3. Article 4 – Duties of the Parties:

Paragraph 1 refers to the "necessary measures to give effect to the basic principles". It is worth noting that, in 1981, the explanatory report both stressed the importance of measures to implement the principles that risked remaining a dead letter without them and called for measures of self-regulation as a guarantee of operationality.

This concern to find auxiliary resources either in the development of technical standards[70] and Privacy Enhancing (PETs)[71] or in the emergence of new occupations or methods that

[69] Cf. Article 1e): "'processor'" shall mean a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data."

guarantee respect for the principles of data protection (labels, infomediaries, etc) can be explained[72] for various reasons, particularly significant in the Internet world:

- the greater **effectiveness** of such measures that either use the resources of technology to impose solutions in conformity with data protection requirements (technological solutions)[73] or are based on an agreement among the players concerned to find solutions that protect data from uses of these technologies that are imposed, improper or unfair;
- the **transnational** character of the solutions that can be developed in this context;
- the difficulty for the data protection authorities to ensure this respect on their own
- the necessity to create a climate of user confidence vis-à-vis a network considered "opaque".

The combination of three methods of regulation and their proper co-ordination are no doubt the right way to increase the protection of the data subjects and raise their awareness[74]. The example of "privacy policies" confirms this. When looked at more closely, the statutory obligation to publish a web page mentioning the company's data protection practices, accessible to the user and conforming to legal requirements involves the use of a number of instruments, which are in this case not necessarily regulatory in nature. An assessment of the situation and the question of whether practice meets statutory requirements may be left to certifiers and auditors[75], the possible intervention of whom should be announced by means of a label. The various sectors can propose privacy policy models. In order to avoid the use of different formats, forms of expression and vocabulary, it might be preferable to establish a minimum basis and a vocabulary that these various labels would have to adhere to - a kind of meta label as it were. It is perhaps necessary to envisage a legislative measure[76] that could settle these various points.

The privacy policy should be made accessible via software applications that ensure that the visit to the page concerned is obligatory and, if necessary, will authorise an expert system to compare the data subject's "privacy preferences" to the choices made by the data controller and enumerated by the privacy policy. It should be pointed out that this act of taking cognisance of a privacy policy must from the outset take place as anonymously as possible.

---

70 In this context, the security and privacy standards currently under discussion at the ISO.

71 Privacy Enhancing Technologies

72 See our report for the Prague Conference organised by the Council of Europe on 14-15 October 2004 *"How to make data subjects aware of their rights and obligations and make them responsible for their own protection*." See also C.J. BENNETT et C.D. RAAB, *The Governance of Privacy*, Ashgate, 2003.

73 J. Reidenberg, "Privacy Protection and the Interdependence of Law, Technology and Self-Regulation ", in *Variations sur le droit de la société de l'information, Cahier du Crid, n° 20,* Bruylant, Brussels, 2002, pp. 126 ff.

74 On this point, see J.R. Reidenberg, "Lex informatica: The Formulation of Information Policy Rules through Technology", 76 *Texas Law Review* (1998), pp. 553 ff.

75 It is possible to conceive of certifiers and auditors being subject to accreditation themselves according to a set of conditions laid down by a public authority or at any rate with its approval. Cf. the parallel with the Trustmark UK system. See on this system R. De Bruin, XXX

76 For example, eight American federal institutions have launched the Advanced Notice of Proposed Rulemaking procedure (ANPR). which calls for public comments concerning improvements to the privacy notices that the financial institutions must provide to consumers under the Gramm-Leach Act.

Another example is no doubt the regulation of website privacy certification labels[77]. The proliferation of labels is confusing for the surfer . What value should be put on a label liable to be copied, issued a long way away by an unknown body whose independence is unclear, whose monitoring of the quality of websites is uncertain and which is poorly equipped to impose penalties for failure to comply with the label's standards. The certification of labels, that is to say the exercise of oversight by a public authority or a body whose composition proves that it is independent and represents the various interested parties may be a solution the authorities could put in place or initiate[78].

Avenue of inquiry

In short, the appropriate solutions, it may be assumed, are to be found in a subtle mix, in a system of co-regulation[79] in which the law is not only followed up but also rendered effective in technical and self-regulatory systems, to which it should aspire and promote. These various co-regulation of self-regulation measures are, however, only acceptable if they meet the triple requirements of legitimacy, conformity and effectiveness[80].

Such measures are no substitute for the obligation to establish the basic principles of a control framework by means of official regulation. It is against the background of these principles that the technical measures[81] and the market's responses to the problems posed by the development of electronic communications services are assessed. The establishment

---

[77] On this labelling of websites, cf. the discussions at the "E-confidence Forum" set up by the European Commission and the suggestions it has made (http://www.econfidence.jrc.it)

[78] For such a mechanism designed to ensure the conformity of websites with consumer protection and consumer security legislation, cf. the Trustmark UK system. See R. De Bruin, XXX

[79] On co-regulation, see Y. Poullet, "Technologies de l'information et corégulation", in *Liber Amicorum M.Coipel*, Y. Poullet - P.Wery - P.Wynants, Kluwer, 2004, à paraître .

[80] About co-regulation, see Y. POULLET, "op.cit.: « *The **"legitimacy"** is "source oriented and underlines the question of the authors of a norm. To what extent, might the legal system accept a norm elaborated outside of the actors designated by the Constitution or under constitutional rules? This quality of the norm means that the authorities in charge of the norm promulgation must be habilitated for doing that by the community or communities of the persons which will have to respect the rule they have enacted. This legitimacy is obvious as regards the traditional State authorities acting in conformity with the competence devoted to them by the Constitution. It is less obvious when the regulation is the expression of private actors themselves as it is the case with self-regulation, particularly when it is the fact of certain obscure associations or even of private companies able to impose their technical standards.*

*The **"conformity"** is "content oriented" and designates the compliance of normative content vis a vis fundamental society values, those embedded undoubtedly in the legal texts but also beyond that those considered as ethical values to be taken into account by the legal system. Again this criterion is quite easy to satisfy and to verify in case of traditional texts issued by governmental authorities insofar these texts must be taken in consideration of already existing rules with superior values. It seems more intricate to satisfy to this criterion when the compliance with existing legislative text is not systematically checked insofar these text are not existing or not clearly identified. Indeed self-regulation is often a way to avoid the traditional and constitutionally foreseen regulatory methods of rule-making.*

*Finally, the **"effectiveness"** is "respect oriented". To what extent, a norm will be effectively respected by those to whom the norm is addressed ? So, the question about the information about the existence of the norms, about the sanctions and the way by which they might be obtained are central for determining the effectiveness of a norm. By this criterion, one means in particular the fact for the addressees of the norm to be aware of the content of the norm but also for norms to foresee a cost for its non respect by addresses who are so stimulated to follow the rule."*

[81] As Mr Dix wrote: "« Technology is however no panacea for privacy risks in cyberespace ; it cannot replace a regulatory framework or legislation, contracts or code of conduct. Rather it may only operate within such a framework. Privacy by negotiation is therefore no alternative to regulation but a necessary additional tool"(A. DIX, "Infomediaries and Negociated Privacy Techniques", papier présenté à la *Conférence « Computers, Freedom and Privacy » (CPF 2000), 19 avril, Toronto, disponible à : http://portal.acm.org/citation)*

of the inadequacy of such measures or responses may force the public authorities to issue new regulations (subsidiarity principle [82]).

As already stated: the law is necessary. It guides self-regulatory initiatives and acts as a yardstick by which these can be assessed and judged. In addition, nothing is worse than users being left to their own devices, not knowing which regulation to trust, the market only being able to be a good guide if it is transparent and the "consumer" able to separate the "data protection" factor from other criteria. The user empowerment that certain negotiation technologies would bring about will remain an illusion if it is not subjected to the supervision of the law.

Avenue of inquiry

The call for co-regulation presupposes the promotion of new players who help to raise awareness and offer users genuine ways of controlling their environment, such as website certifiers and infomediaries. Co-regulation leads to the promotion of the development of new "secure" technologies and their being made available in respect of both data subjects and intermediaries, such as internet access providers. Software and anonymisation services provide a good example in this connection.

4. Article 5 – Quality of data:

4.1. CONSENT AS A BASIS FOR THE LEGITIMACY OF PROCESSING

The requirement that there be a legitimate purpose involves a consideration of the question of **consent as the basis for the legitimacy of certain processing operations carried out in connection with the use of internet services by the data subject.** As we know, even if Article 5 limits itself to mentioning the general principle of legitimacy, the issue of consent is mentioned by the data protection authorities, the European Directive (Article 5.1) and by legal writers as the primary basis for the legitimacy of a processing operation. Since modern networks are interactive, consent can more easily be claimed to be the basis for the legitimacy of data processing and be preferred to other more traditional bases such as a balance of interests. The ease with which the file controller can obtain the data subject's explains why some countries do not hesitate now to demand in their laws that consent be given in order to legitimise certain processing operations, like Directive 2002/58/EC on the processing of traffic and location data[83]. This consideration now leads some to believe that consent may be enough to legitimise processing. It should be remembered in this connection that the development by the World Wide Web Consortium (W3C) of the Platform for Privacy Preferences (P3P)[84] was also based on the possibility for web surfers to negotiate with service providers who have failed to respond to their privacy preferences and then reach an agreement that serves as a legitimate basis for the planned processing operation. Even if no broad use has ever been made of this possibility of holding

[82] Which can be expressed as follows: "Any matter you can resolve by self-regulation or co-regulation must be dealt with in this way".

[83] Mention should also be made of the opt-in system chosen to resolve the question of sending unsolicited mail. Other arguments in favour of the ability to opt in are the intrusive character of the mail that directly penetrates the data subject's home, the ease with which such messages can be sent and the absence of any costs for the sender.

[84] Apart from the opinion issued by the Article 29 Group (Opinion 11/98 of the European Data Protection Working Party, the so-called Article 29 Group) concerning the Platform for Privacy Preferences (P3P) and Open Profiling Standards (OPS), which is available at http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdoes/wp11.fr.pdf), see on this protocol, J. Catlett, "Technical Standards and Privacy: An open Letter to P3P Developers", available at *http://www.junkblusters.com/standards.html*.

negotiations, especially through electronic agents, P3P remains an indication of the industry's willingness to provide itself with the means of negotiating with the data subject the use that might be made of his or her data. The protection of privacy could thus to some extent be negotiated[85].

Avenue of inquiry

Nevertheless consent does not appear to us to be a sufficient basis for legitimacy. We think that, in certain cases, the legitimacy of processing that is even backed by a person's specific, informed and freely given consent may be called into question. There are Three reasons that support this view:

- **consent that has even been obtained by fair means cannot legitimise certain processings that are contrary to human dignity or to other key values that an individual cannot relinquish.**

- **consumers must be protected against practices that involve their consent being solicited in exchange for economic advantages.**

- **finally, the question of the protection of privacy is not just a private matter but brings social considerations into play and calls for the possibility of intervention and marginal supervision by the authorities.**[86]

4.2. THE PARTICULAR CASE OF CONSENT IN THE CASE OF MINORS

The consent of minors to the processing of personal data concerning them poses some tricky problems. The consent must come from a person legally capable of giving it. The consent given by a minor is on no account sufficient without parental authorisation, but this does not prevent minors having to be consulted, provided that they understand, or even requiring not only parental authorisation but also the minor's own autonomously expressed consent .

Recently, the development of interactive internet services has given these principles a particular topicality. Children are a preferred target for all kinds of internet "vendors" and several methods of gathering information are used to induce them to provide personal information, such as competitions, membership forms, etc.

It thus appears necessary to check parental consent to the provision of such information. The American Children's Online Privacy Protection Act (COPPA), of 1998[87], requires that the provider of services that gather information from minors be subject to the principle of "verifiable parental consent", which is defined as "any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and

---

[85] On the technology-based contractualisation of the processing of data, 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 f.; M. Rotenberg, "What Larry Doesn't Get the Truth", *Stan. Techn. L. Rev*., 2001,1, available at the website http://www.Stanford.edu/STLR/Articles/01_STLR_1

[86] Cf. in this connection the thoughts put forward by Schwartz in the article mentioned in the previous footnote.

[87] Sect. 1302(9). The text of the American law is available at the Federal Trade Commission 's website http://www.ftc.gov/ogc/coppa1.htm. The law provides for some exceptions to this requirement.

disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child".

Recently, the Belgian Privacy Protection Commission[88] issued a more guarded opinion on the same subject, stressing the child's autonomy and underlining the limits to it: "The *Commission is of the opinion that parental consent does not have to be systematically required when data relating to a minor are processed on the internet. It thus emphasises that parental consent should not be a mechanism permitting a parent to override the child's decision unless there is a serious risk that the child will not correctly appreciate the consequences of its decision or that its natural naivety will be exploited. The Commission therefore stresses in this document the necessity to obtain parental consent in specific circumstances, especially when the child has not reached the age of discernment, when sensitive data are gathered, when the aim pursued is not in the minor's direct interests (marketing, transmission of the data to third parties) or when the data are to be made public (dissemination of information at a discussion forum or at a school's website).*

4.3. INCOMPATIBLE PROCESSING

The principle of the "**compatibility**" of purposes requires that in the case of derived processing these operations must not clash with the reasonable expectations of the person concerned. The acceleration of technological progress, the infinite number of new processing opportunities offered by the software and the data available on the network warrant giving some attention to the question of subsequent processing and its compatibility with the initial aims of data recording.

For example, RFID chips, which were originally designed by consumer goods manufacturers as a means of preventing theft in the big department stores, have become a powerful tool for analysing the behaviour of consumers, their profiling, etc. If a scientific author makes his curriculum vitae and publications available for the purpose of making his work known, this may serve to classify him politically or in terms of his thinking. The publication of court judgments in huge databases has an academic objective and helps to make the law known. However, the possibility of running a search of the names of the parties or the type of case may enable blacklists to be drawn up (for example, a list of employees who have brought an action against or been dismissed by their employers).

Avenue of inquiry

The regulation that might be proposed must take account of the benefits that could be provided by subsequent processing operations[89]. As far as possible, consent or the coding, indeed anonymisation, of the data (minimisation principle) must no doubt be required. Failing that, it should be possible to consider compelling the file controller who wants to carry out a processing operation at a later date to provide detailed reasons, in the interests of ensuring a balance of interests, for believing it is legitimate to do so and at least to inform the data subjects collectively.

---

[88] Opinon (Avis) no. 38/2002 on the protection of the privacy of minors on the internet. Available at the Commission's website: http://www.privacy.fgov.be.

[89] For example, a health-care database may, after being used for an initial purpose connected with a patient's treatment, be used for the purposes of scientific research; a bank may offer its customers a new service at a given moment based on the more detailed exploitation of customer data.

As far as technical solutions are concerned[90], consideration could, for example, be given in the context of search engines to providing network users with the means of stating themselves what they understand by "compatible" purposes. For example, the "no robot" systems inserted into web pages prohibit these pages being considered by search engines. Here is another example of technical solutions: in connection with the marketing uses of data gathered on the net, infomediaries offer their services to select the possible employment of web surfers' data for marketing purposes, etc.

4.4. THE USE OF COMMUNICATION SERVICES WITHIN GROUPS AND THE LEGITIMACY OF THEIR INTERNAL DATA PROCESSING

Information systems are often used by a group of people, for example within a family (use of the same PC or the same terminal) or an organisation (sharing of common resources by means of an intranet). In addition, terminals may be made available to users by a person who is at that particular moment the sole subscriber to the services used by these various individuals (for example, a father or the director of a company who takes out the subscriptions to the mobile phones placed at the children's or employees' disposal). This sharing of resources or provision of terminals enables these individuals to monitor their use by people dependent on them. This supervision may be legitimate if it is linked to matters relating to the security of the network or to limiting expenditure but it can also lead to an unwarranted increase in the surveillance powers of one group over the other.

Avenue of inquiry

There have been several regulatory or self-regulatory initiatives to lay down rules concerning, and limits to, the surveillance of employees with regard to their use of the information-based resources at their disposal. It would no doubt be good if the Consultative Committee were to examine these often unco-ordinated rules and, after listening to the parties concerned, establish a number of common principles that will enable behaviours to be harmonised. In addition, it would be advisable to consider the distinction between "subscribers" and "users" advocated by Directive 2002/58/EC, which leads to a consideration of the limits to the processing by the subscriber of traffic and location data generated by users (for example, bills or invoices) and grants specific rights to users vis-à-vis subscribers (for example, the right to restrict the identification of the calling line and to object to the processing of traffic data).

5. Article 6 – Sensitive data:

Avenue of inquiry

Two special categories of data should be added to the list of sensitive data in the light of the new dangers brought about by technological developments:

- **the "identification numbers" (with or without a link to the person's identity in the narrow sense) that enable many databases or data to be connected together and are becoming widespread in both the private and public sector;**

[90] This is a nice anticipation of the principle we shall develop in Part III under the title "Principle of the promotion of technological solutions that comply with data protection requirements or improve the situation of persons protected by law.

- **the "profiles" defined by Swiss law as "a combination of data that enable an assessment of the key aspects of the personality of an individual to be made". The Swiss approach could be extended along the lines of Norwegian law to cover "anonymous profiling" when this is used to take subsequent decisions concerning persons covered by this profile**[91]

In addition, the extremely broad definition of sensitive data (eg, a surname reveals racial origin; the purchase of a work on the Koran at a site web may reveal a person's religious convictions, etc) makes it absolutely necessary to abandon the approach based on a definition of the actual nature of data in favour of a purpose-based approach – is the purpose of the processing to reveal a person's racial origin, etc? This approach would make it possible to consider the actual processing of data as sensitive rather that the data itself, even if no sensitive data were involved. For example, a search of trips to Rome conducted by a web surfer using Google or his or her purchases of religious books, reading of a papal encyclical, etc, may be treated as revealing a religious opinion.

6. Article 7 – Data security:

This article considers security in a very limited sense: principally, the destruction of data and breaches of confidentiality. It would be advisable for security to relate to the three aspects of security in the broad sense – integrity, reliability and confidentiality – and for the nine guiding principles for the security of information systems drawn up by the OECD in 92 (responsibility, awareness, ethics, multidisciplinarity, proportionality, integration, timeliness, reassessment and democracy) to be adopted.

In addition, the lack of network security and the proliferation of opportunities for illicit actions make it necessary for the providers of electronic communications services to be obliged to issue warnings concerning their use.

Finally, emphasis should be placed on the importance of self-regulation in this connection: the development of standards; auditing methods; regimes for the approval of information systems, etc. The organisation and technical security of information systems but become an integral part of data protection policy.

Avenue of inquiry

In the last few years, standardisation organisations have made many attempts to bring about the technical and organisational standardisation of data security and protection[92]**. These various efforts must be monitored and supported by the Consultative Committee.**

With regard to security, mention should be made of the requirements concerning the confidentiality of communications in the broad sense. The requirements regarding the confidentiality of communications can be attributable to the fact that interactive network technology now enables its user to communicate with other people connected to it and to do so for personal purposes. This explains why the principle of the confidentiality of correspondence and the ban on eavesdropping must henceforth be extended to all electronic communications,

---

91 See Lee Bygrave, Data Protection Law, Information Law Series, Kluwer Law Inst., p. 330 f.

92 For example. the work of the ISO/IEC/ITU/UN ECE MoU Management Group and Privacy Technology Standards and recent decisions (taken in Berlin 25-29 October 2004) of ISO/IEC JTC 1/SC 27 (Information Technology- Security Techniques) to support the development of privacy technology standards (Resolution 15) and launch an evaluation and a PETS test project (PETTEP project) (Resolution 18).

both with respect to their content and their existences. There also arises the question of the status of the companies that convey the messages or intervene in this process: should the example of the regulations concerning the postal services and the traditional operators of telephone networks be followed by imposing on these companies regulations that would guarantee such confidentiality?

7. Article 8 – Additional safeguards for the data subject:

Several suggestions and recommendations could no doubt be proposed on this issue by the Consultative Committee. The goal is to propose an improvement in the situation to ensure that data subjects are able to exercise "information self-determination" at the moment when, as we have shown in Part I, their control tends to diminish in view of the opacity of the operation of terminals and the network. In Part III, we call for the recognition of new rights, which is a very important consequence of the loss of control over the information environment by the users of information systems. Thus, we want the following rights established at the very least:

1. a right of the person concerned to **mutual benefits**;
2. the right of the person using a terminal to have **equipment at his or her disposal that functions transparently** and reduces illicit actions as far as possible.

The following will doubtless be added:

3. the recognition of the right of the person concerned to understand the thinking behind the decisions applied to him or her on the basis of automated reasoning.
4. the duty of the providers of electronic communications services to engage in "legislative education" vis-à-vis their customers. This involves drawing the attention to the principles of the Convention of those who want to use the connection to provide database access services or create processing arrangements on the basis of the services offered and, at any event, warning every user about the risks associated with the use of the internet.

8. Article 9 – Exceptions and restrictions

A general exception should be added, according to several writers, with regard to the processing of personal "family or domestic" data. There is a sound argument for this: the privacy of those who process data on their own account cannot be violated in the name of protecting other people's data. However, as the above-mentioned Linqvist case shows, the scope of this exception must take account of the fact that private thoughts posted on a website undeniably have their origin in the private or domestic sphere of the persons concerned and are made accessible to an indeterminate and unlimited number of people.

Paragraph 2 should provide for exceptions associated with the need to guarantee freedom of expression or opinion (principle of a fair balance between data protection and freedom of opinion and/or expression).

Paragraph 3 on statistics or research only considers the risks associated with the protection of individual data used for research or statistical purposes.

As we have stressed, statistical work and scientific research call for certain precautions even when they relate to anonymous or anonymised data since they enable the profiles thus created to be applied to individuals[93]

9. Article 12 – Transborder flows of personal data and Article 2 of the Additional Protocol (signed on 8 November 2001)

Article 2 of the Additional Protocol adopts the concept of an "adequate level of protection" as the criterion for the acceptance of a transborder flow. It is assumed that this reference to the European Directive's criterion implies agreement with the many documents interpreting this concept that have been produced by the competent European authorities since the publication of the directive (so-called Article 29 Group and decisions of the Commission on the question of adequacy[94]). It is no doubt worth pointing out that the determination of adequacy presupposes a dynamic interpretation since is not established once and for all but in the light of new interpretations and regulations given to the Convention by the case law of the Court of Strasbourg (recommendations, additionnal protocols).

The same goes for the two derogations, in particular the second one relating to guarantees considered sufficient. Reference is no doubt made to the exceptions proposed by Directive 95/46 and their interpretation since then (decisions regarding contract clauses).

Avenue of inquiry

The issue of transborder flows raises a number of questions that have not yet been addressed by the Convention:

1. **Should criteria not be adopted for the location of processing on the web?**
2. **What is a transborder flow? Should a distinction not be drawn between flows involving an active transfer of data and those involving a passive transfer, ie entirely under the control of the controller of the file located abroad (eg, automatic extraction of certain data contained in a database of a branch of a multinational company)? Should one not speak of potential transborder flows in the case of services accessible via the internet?**
3. **There are various exceptions to the principle of the ban on transborder flows of data: the "adequate protection" provided to the controller of the file by external rules in force in the state concerned, the contract between the controllers importing and exporting a file. the internal rules that the file controller(s) impose on themselves within a group of companies and, finally, a number of social cases associated with the nature of the flow concerned. The question raised by several controllers concerns the ability easily to identify what type of exception applies in their specific case. In other words, a system needs to be established that makes it easier to identify the types of**

93 see remarks on Article 1 above (supra 5.1.)

94 Cf. the numerous opinions issued by the so-called Article 29 Group in this connection, especially the working document WP 12 on transfer of personal data to third countries: application of Articles 25 and 26 of Directive 95/47 relating to data protection (available at http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp1998/wpdocs98_fr.htm) and the study by B. Havelange and Y. Poullet, "Elaboration of a methodology in order to evaluate the adequacy of the level of the protection of the individual vis à vis the processing of personal data in third countries", European Commission, Official Publications Office, ISBN 92- 828-43O4, 1998", appended to the annual report of the Article 29 Group set up pursuant to Article 29 of Directive 95/46/EC.

flow to which each category of exceptions applies, and it is necessary to provide an interpretation of the scope of each exception on the basis of this system.

4. **Should a number of elements of law and applicable jurisdiction not be outlined in the case of transborder flows?**

5. **How is it possible to regulate access from abroad to data located in Europe (cf. the case of the American authorities' practice with regard to data on airline passengers (passenger name records) or flows from and to member countries intercepted in transit by international or foreign networks (cf. the ECHELON case)?**

6. **Finally, there is the question of the operationality of the decisions taken in the name of the sovereignty of the Council of Europe member states for the purpose of defending human rights. How can this be guaranteed? One idea would be to create an obligation for the providers of electronic communications services to be located in the territory of a member state.**

10. Conclusion of part II

The principles set out in Convention No. 108 provide, thanks to their flexible scope generally satisfactory solutions for guaranteeing adequate protection for data subjects who use networks and information systems – provided, of course, that some of the Convention's concepts and rules are made the subject of a study concerning their meaning in a context, especially of a technological nature, that is no longer the same as the one in which these principles were drawn up. A progressive interpretation of the concept of identity and of the file controller has been suggested. Similarly, the provisions relating to the legitimacy of processing operations in the context of interactive, international or co-operative networks demand consideration of the scope of, and limits to, consent, the compatibility of processing operations and their security and, finally, the ubiquitous question of transborder data flows.

However, the consideration of two important texts published since the Convention and which we wished to taken into account from the outset in the analysis of the development of the principles of the Convention makes it possible to pinpoint a number of additional regulatory provisions that are necessary to meet the challenges to data protection posed by internet-related technological developments in respect of issues that are not dealt with by the Convention but appear to be a particularly relevant response to the new risks emphasised in the first part of our study.

Thus, la Committee of Ministers Recommendation No. R (99) 5 for the protection of privacy on the internet mentions the importance of the data subjects' anonymity: "*Anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy*"[95]. This claim to a "right of anonymity" appears to have been followed up by other European texts. In addition, the recommendation draws attention in Part III to the duties of "*internet service providers*", a concept that Part IV extends to an entire range of players: "*access providers, content providers, network providers, navigation software designers, bulletin board operators … (and) "all types of information highways"*. This desire to impose responsibilities on these new players who owe their existence to the development of our interactive networks is to be found in the remarks on traffic and location data considered below, but these responsibilities do not stop there.

In particular, Directive 2002/58/EC on privacy and electronic communications pinpoints the particular role of two players:

- network operators (including internet access providers), that is to say those who provide *"transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals*[96] constitute essential interfaces between the network user as a data subject and a multiplicity of internet players who could process the multiple data generally consciously or not by the network user. They have certain duties, such as the obligation to prevent risks associated with the use of the network, to guarantee the security of their services, to permit restrictions on the identification of the calling line, etc;

- suppliers of terminal equipment, especially - but not exclusively – navigation software, whose technical features must be in compliance with the provisions of the directive. In

---

95 Paragraph II.3 of the Recommendation. See also paragraphs II.2, II.4 and III.4.

96 Directive 2002/21/EC, Article 2d).

particular, the directive provides for the possibility of imposing certain *"measures (that) may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data"*.

In other words, the above-mentioned texts call for measures that go beyond the provisions of the Convention: firstly, the "right to anonymity", secondly regulations governing "terminal equipment"[97], and, thirdly, the establishment of specific regulations and obligations in respect of the communication service providers that necessarily involved in the routing of messages. These additional measures are justified, as we have said, because of new risks due to changes in the technological landscape, including the loss of control over two interfaces that has been established in the case of the data subject, these interfaces being the terminals, the functioning of which is opaque, and the technical intermediaries who interpose themselves between the network user and the recipient of the communication.

In order to underpin these three demands, Part III identifies and explains, on the basis of recent national or international instruments, some new aspects of data protection inherent in the desire to give data subjects back some of their control over their environment and over the circulation of their data-based image.

[97] To be understood in the sense of Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (http://europa.eu.int/comm/enterprise/rtte/dir99-5.htm), that is to say as a product permitting *communication or a relevant component of a product designed to be connected directly pr indirectly by any means to interfaces of public telecommunications networks (ie, telecommunications networks whose purpose is entirely or partly to provide publicly accessible telecommunications services).*

III. SOME NEW PRINCIPLES TO PROMOTE INFORMATIONAL SELF-DETERMINATION IN THE NEW TECHNOLOGICAL ENVIRONMENT

Those features that are most characteristic of the electronic communications service environment – growing presence and multifunctionality of electronic communications networks and terminals, their interactivity, the international character of networks, services and equipment producers and the absence of transparency in terminal and network functioning – all increase the risk of infringing individual liberties and human dignity.

To counter these risks, certain new principles must be established if data subjects are to be better protected and have more control over their environment. Such control is essential if those concerned are to exercise effective responsibility for their own protection and be better equipped to exercise proper informational self-determination.

This is a first attempt to outline such principles. It is based on a range of material and we have tried to structure it around five main principles, since at this stage we prefer not to speak of new "rights" for data subjects. Their content and extension should be discussed by the Consultative Committee, and could then, if appropriate, form the basis for recommendations and other *ad hoc* measures to give them greater force.

1. First principle: The principle of encryption and reversible anonymity

The encryption of message offers protection against access to the content of communications. The quality varies, as do encryption and de-encryption techniques. Encryption software for installation on internauts' computers (S/MIME or Open PGP protocols) is now available at a reasonable price. Meanwhile, given its ambiguity, the notion of anonymity should perhaps be clarified, and possible replaced by other terms such as "pseudonymity" or "non-identifiability". What is sought is often not absolute anonymity but rather **the functional non-identifiability of the author of a message vis-à-vis certain persons**[98]. There are many non-binding documents[99] advocating citizens' "right" to anonymity when using new technological services. Recommendation No R (99) 5[100] of the Council of Europe's Committee of Ministers states that "*anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy*", hence the importance of privacy enhancing techniques already available on the market.

---

[98] See J. Grijpink and C. Priens, Digital Anonymity on the Internet, New Rules for Anonymous Electronic Transactions?, 17 CL&SR § (2001), p. 378 ff.

[99] See in particular S. Rodota, Beyond the E.U. Directive: Directions for the Future, in *Privacy: New Risks and Opportunities*, Y. Poullet, C. de Terwangne and P. Turner (ed.), Cahier du CRID, Kluwer, Antwerpen, n° 13, p. 211 ff.

[100] Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways, available on the Council of Europe site. See also Recommendation 3/97 of the so-called Article 29 Group: Anonymity on the Internet, and the opinion of the Belgian privacy commission on electronic commerce (No. 34/2000 of 22 November 2000, available on the commission's site: http://www.privacy.fgov.be), which points out that there are ways of authenticating the senders of messages without necessarily requiring them to identify themselves.

Avenues of inquiry

Those using modern communication techniques must be able to remain unidentifiable by service providers and other third parties intervening during the transmission of the message and by the recipient or recipients of the message, and should have free or reasonably priced access to the means of exercising this option[101]. The availability of readily affordable encryption and anonymisation tools and services is a necessary condition for computer internauts' exercising personal responsibility.

The anonymity or "fonctional non-identifiability" required is not absolute however. Citizens' right to anonymity has to be set against the higher interests of the state, which may impose restrictions if these are necessary *"to safeguard national security, defence, public security, [and for] the prevention, investigation, detection and prosecution of criminal offences"*. Striking a balance between the legitimate monitoring of offences and data protection may be possible through the use of "pseudo identities", which are allocated to individuals by specialist service providers who may be required to reveal a user's real identity, but only in circumstances and following procedures clearly laid down in law.

Avenues of inquiry

Other approaches might include the enforced regulation of terminal equipment, to prevent browser chattering, permit the creation of ephemeral addresses and differentiation of address data according to which third parties will have access to the traffic or localisation data, and the disappearance of global unique identifiers by the introduction of uniform address protocols.

Finally, the status of "anonymisers", on which those who use them place great reliance, should be regulated to offer those concerned certain safeguards regarding the standard of service they provide while ensuring that the state retains the technical means of accessing telecommunications in legally defined circumstances[102].

2. Second principle: The principle of reciprocal benefits

This principle would make it a statutory obligation, wherever possible, for those who use new technologies to develop their professional activities to accept certain additional requirements to re-establish the traditional balance between the parties concerned. The justification is simple – if technology increases the capacity to accumulate, process and communicate information on others and facilitates transactions and administrative operations it is essential that it should also be configured and used to ensure that data subjects, whether as citizens or consumers, enjoy a proportionate benefit from these advances.

Several recent provisions have drawn on the proportionality requirement to oblige those who use technologies to make them available for users to enforce their interests and rights.

---

[101] See the recommendation of the French national data processing commission that access to commercial sites should always be possible without prior identification (M Georges, Relevons les défis de la protection des données à caractère personnel: l' Internet et la CNIL, in *Commerce électronique- Marketing et vie privée*, Paris, 2000, p.71 and 72.

[102] Requirements could be laid down for the services provided and concerning confidentiality, as is proposed for electronic signatures. Official approval of an anonymiser would indicate that the requirements were being observed. Such official approval might be voluntary rather than obligatory, as in the case of quality labels.

One example is European Directive 2001/31/EC (the "E-Commerce Directive"), which includes electronic anti-spamming provisions. Similarly, Article 5.3 of Directive 2002/58/EC on privacy and electronic communications even includes the requirement that *"... the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information ... and is offered the right to refuse such processing ...."*. Subscribers' right, under Article 8.1, "via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis ... and on a per-line basis" is another potentially valuable approach if the notion of "calling line" is extended to various Internet applications, such as web services and email[103]. This implies a related obligation for the service provider to offer users the options of refusing to accept unidentified calls or preventing their identification (Articles 8.2 and 8.3).

Legislation of the Freedom of Information variety introduces a similar right to transparency vis-à-vis government by adding further information that the latter is obliged to supply. A welcome development in the United Kingdom is the recent introduction of a public service guarantee for data handling[104]. A Swedish commission[105] has recently recommended legislation that would entitle citizens to monitor their cases electronically from start to finish, including their archiving, and oblige the authorities to adopt a good public access structure, to make it easier for individuals to identify and locate specific documents. There is even draft legislation that would make it possible, one way or another, to link any official documents on which decisions were based to other documents on the case. In other words, a public service that has become more efficient thanks to new technology must also be more transparent and accessible to citizens. Citizens' right of access extends beyond the documents directly concerning them to include the regulations on which a decision was based.

Avenues of inquiry

It is even possible to imagine that certain of the rights associated with data protection, such as the right to information, the rights of access and rectification and the right of appeal, might soon be enforceable electronically. Many applications could be proposed:

1 it should be possible to apply data subjects' right to information at any time through a simple click (or more generally a simple electronic and immediate action) offering access to a privacy policy, which should be as detailed and complete as the greatly reduced cost of electronic dissemination allows. Such a step must be anonymous as far as the page server is concerned, to avoid any risk of creating files on "privacy concerned" users. In addition, in the case of sites that have been awarded quality labels, it should be obligatory to provide a hyperlink from the label symbol to the site of the body that awarded the label. The same would apply to the declaration of the file controller to the supervisory authority. A hyperlink would be installed

---

[103] Note the link between these provisions and the anonymity principle.

[104] A Public Service Guarantee For Data Handling: now available for implementation in public bodies. This sets out people's rights about how their personal data is handled by public authorities and the standards they can expect public organisations to adhere to http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2

[105] P. Seipel, Information System Quality as a Legal Concern, in *Information Quality Regulation: Foundations, Perspectives and Applications*, U.Gasser (ed.), Nomos Verlagsgesellschaft, 2004, p. 248. See also the Swedish commission report by P. Seipel, Law and Information Technology: Swedish Views, Swedish Government Official Reports, SOU 2002, 112.

between an unavoidable page of any site processing personal data and that of the relevant supervisory authority. Finally, consideration might be given to the automatic signalling of any site located in a country offering inadequate protection;

2 in the future, data subjects must be able to exercise their right of access using an electronic signature. It would be obligatory to structure files so that the right of access was easy to apply. Additional information, such as the origin of documents and a list of third parties to whom certain data had been supplied, should be systematically available. As noted earlier[106], increasingly, the personal data accumulated by the vast public and private networks are no longer collected for one or more clearly defined purposes but are stored in the network for future uses that only emerge as new processing opportunities or previously unidentified needs arise. In such circumstances, data subjects must have access to documentation describing the data flows within the network, the data concerned and the various users – a sort of data registry[107];

3 it should be possible to exercise the rights of rectification and/or challenge on line to an authority with a clearly defined status responsible for considering or maintaining a list of complaints;

4 the right of appeal should also benefit from the possibility of on-line referral, exchange of parties' submissions and other documentation, decisions and mediation proposals;

5 finally, when individuals concerned wish to challenge decisions taken automatically or notified via a network (such as a refusal to grant a building permit following a so-called e-government procedure), they should be entitled to information, via the same channel, on the logic underlying the decision. For example, in the public sector[108] citizens should have the right to test anonymously any decision-making packages or expert systems that might be used. This might apply to software for the automatic calculation of taxes or of entitlement to grants for the rehabilitation of dwellings.

3. Third principle: The principle of encouraging technological approaches compatible with or improving the situation of legally protected persons

Recommendation 1/99 of the so-called Article 29 Group (the EU Data Protection Working Party)[109], which is concerned with the threat to privacy posed by Internet communications software and hardware, establishes the principle that software and hardware industry products should provide the necessary tools to comply with European data protection rules. In accordance with this third principle, regulators should be granted various powers.

---

106 See paragraph 3.

107 This idea is the subject of two recent Belgian laws that require the establishment of sectoral committees for the networks linked to the National Register (Act of 8 August 1983 establishing a national register of persons, as amended by the Act of 25 March 2003, MB. 28 March 2003, art.12§1) and to the commercial registration authority (Banque Carrefour des entreprises) (Act of 16 January 2003 establishing the authority, MB. 5 February. 2003, article 19§4).

108 The same principle applies to private decision makers, subject to the legitimate interests of the file controller (particular relating to business confidentiality, which could limit the duty to clarify the underlying logic).

109 Recommendation on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.

For example, they should be able to intervene in response to technological developments presenting major risks. The so-called **precautionary principle**, which is well established in environmental law[110], could also apply to data protection. The precautionary principle may require telecommunications terminal equipment (including software) to adopt the most protective parameters as the default option to ensure that those concerned are not, by default, exposed to various risks of which they are unaware and which they cannot assess.

Similarly, in accordance with the principle of reciprocal benefits, it is appropriate and not unreasonable to equip telecommunications terminal equipment with weblogs, as is the case with server-type software used by on-line undertakings and government departments. This would enable users to monitor persons who have accessed their equipment and, where appropriate, identify the main characteristics of the information transferred.

This can be illustrated by one of the provisions of the EU Directive on privacy and electronic communications. Article 14 states that where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary, way of protecting personal data from the risks of unlawful processing – risks that have been created by all these new technological options. Going further, it is necessary to prohibit so-called privacy killing strategies[111], in accordance with the security principle enshrined in Article 7 of Council of Europe Convention 108. The obligation to introduce appropriate technical and organisational measures to counter threats to data privacy will require site managers to make sure that messages exchanged remain confidential, indicate clearly what data is being transmitted, whether automatically or by hyperlink, as is the case with cybermarketing companies, and make it easy to block such transmission.

This security obligation will also require those who process personal data to opt for the most appropriate technology for minimising or reducing the threat to privacy. This requirement clearly has an influence on the design of smart cards, particularly multifunctional cards[112], such as identity cards.

Another example of the application of this principle concerns the structuring of medical files at various levels, as recommended by the Council of Europe.

Avenues of inquiry

It might be possible to go further by recommending the development of privacy enhancing technologies, that is tools or systems that take more account of data subjects' rights. Clearly, the development of these technologies will depend on the free play of the market but the state must play an active part in encouraging privacy compliant and privacy enhancing products by subsidising their research and development, establishing equivalent voluntary certification and accreditation systems and publicising their quality

---

[110] It would probably be useful to develop a comparison between the regulatory modes of these two issues : privacy on one hand and environment on the other hand, taking into account the similarities of their contexts : transnational nature of the issues at stake, important technological aspects and similarity of the approaches taken : self or co-regulation, right to information of the data subjects, principle of security.

[111] Expression used in, **Law and Technology Convergence in the Data Protection Field?**, in *E-commerce Law and Practice in Europe*, I. Walden and J. Horne, Woodhead Publishers Ld, Cambridge, 2002, Chapter 8.2

[112] On the privacy compliant design of multi-application cards, see E. Keuleers and J.M. Dinant, « Data protection: multi-application smart cards. The use of global unique identifiers for cross-profiling purposes". Part 2 :"Towards a privacy enhancing smart card engineering", in *Computer **Law and Security Report***, Vol. 20, n°1, 2004, pp. 22-28, Elsevier, Oxford, 2004.

labels, and ensuring that products considered necessary for data protection are available at affordable prices.

4. Fourth principle: The principle of full user control of terminal equipment

The justification for this principle is obvious. Since these terminals can enable others to monitor our actions and behaviour, or simply locate us, they must function transparently and under our control. Article 5.3 of Directive 2002/58/EC, cited above, offers a first illustration of this point. Those concerned must be informed of any remote access to their terminals, via cookies, spyware or whatever, and be able to take easy and effective countermeasures, free of charge. Directive 2002/58/EC also establishes the rule that users of calling and connected lines can prevent the presentation of the calling line identification.

Going beyond these examples, we would also argue that **all terminal equipment should be configured to ensure that owners and users are fully informed of any data flows entering and leaving, so that they can then take any appropriate action.**

Similarly, as is already the case under some legislation, possession of a smart card should be accompanied by the possibility of read access to the data stored on the card.

User control also means that individuals can decide to deactivate their terminals once for all, and at any time. This is important as far as Radio Frequency Identifiers (RFIDs) are concerned. Data subjects must be able to rely on third parties[113] that vouch that such technical means of remote identification have been fully deactivated.

Users may well apply this principle to firms that are not necessarily covered by traditional data protection rules because they are not responsible for data processing. Examples include suppliers of terminal equipment and many forms of browser software that can be incorporated into terminals to facilitate the reception, processing and transmission of electronic communications. This point will be considered further in Section III.

The principle also applies to public and private standard setting bodies concerned with the configuration of such material and equipment.

The key point is that the products supplied to users should not be configured in such a way that they can be used, whether by third parties or the producers themselves, for illicit purposes. This can be illustrated by a number of examples:

- a comparison of browsers available on the market shows that chattering between them goes well beyond what is strictly necessary to establish communication[114];

- browsers differ greatly in how they receive, eliminate and prevent the sending of cookies, which means that the opportunities for inappropriate processing will also vary from one browser to another. However, blocking pop-up windows or the systematic communication of references to articles read on-line or of keywords entered on search

[113] Clearly this refers to accreditation arrangements such as those already described in paragraph 15 (joint regulation) or to approval issued by the authorities to certain undertakings (public regulation).

[114] See Jean-Marc DINANT, « **Le visiteur visité** », in Lex Electronica, vol. 6, n°2, winter 2001

engines is apparently impossible, at least in a simple way, on the default browsers installed on the majority of the hundreds of millions of personal computers.

- attention should also be drawn to the use of unique identifiers and spyware by suppliers of browser tools and communication software.

Avenues of inquiry

More generally, terminal equipment should function transparently so that users can have full control of data sent and received. For example, they should be able to establish, without fuss, the precise extent of chattering on their computers, what files have been received, their purpose and who sent or received them. From that standpoint, weblogs appear to be an appropriate tool that is relatively easy to introduce.

In addition to users' right to be informed of data flows entering, there is the question of whether persons are entitled to require third parties to secure authorisation to penetrate their "virtual home". Of relevance here is the Council of Europe Convention on Cybercrime, particularly articles 2 (illegal access)[115] and 3 (illegal interception)[116]. In this case, the identification or identifiability of persons taking part in telecommunications is not a precondition for the Convention's application. Similarly, unauthorised access to a computer system is not confined to hacking into major systems operated by banks or government departments but also concerns non-authorised access to telecommunications terminals, represented in the current state of the art by computers[117].

In other words, we maintain that placing an identifying number in a telecommunications terminal or simply accessing this number or some other terminal identifier generally constitutes unauthorised access. In such a legal context, there can be no question of assessing the proportionality of such actions. Authorisation remains a positive act that is quite distinct from any acceptance that might be inferred from silence or a failure to object.

It cannot therefore be assumed, as DoubleClick did[118], that simply by failing to activate a cookie suppressor users have authorised all and sundry to install this type of information on their terminals.

---

[115] Article 2 - Illegal access: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

[116] Article 3 - Illegal interception: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

[117] See, in this context, the excellent article by Thierry Leonard, "E-commerce et protection des données à caractère personnel : Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet" on http://www.droit.fundp.ac.be/Textes/Leonard1.pdf

[118] Following a class action brought against it several years ago in the United States, DoubleClick's practice is now to send all non-identified terminals an initial non-residual and non-identifying cookie named "accept cookies". If the cookie is returned, DoubleClick assumes that the terminal accepts cookies and sends an identifying cookie that remains in place for about ten years (previously thirty). If the cookie is not returned, DoubleClick will indefinitely send the cookie requesting authorisation. An opt-out is available that enables informed users to store a cookie that signifiies that they do not accept them.

5. The principle that users of certain information systems should benefit from consumer protection legislation

The routine use of information and communication technologies, formerly confined to major undertakings, and the rapid development of electronic commerce that has multiplied the number of on-line services have led to a more consumerist approach to privacy. Web surfers increasingly view infringements of their privacy –spamming, profiling, differential charging policies, refusal of access to certain services and so on – from the standpoint of consumers of these new services.

Thus, in the United States the first hesitant steps towards legislation on data protection in the private sector focussed on on-line consumer protection. Reference has already been made to Californian legislation[119] but we should also bear in mind the 1995 Consumer Privacy Act and, more recently, the 2000 declaration of the Federal Trade Commission[120], which emphasised the need for privacy legislation to protect on-line consumers. In Europe as in America measures to combat spamming are concerned with both consumers' economic interests and data subjects' privacy.

Avenues of inquiry

- **This convergence between consumers' economic interests and citizens' freedoms opens up interesting prospects. It suggests that the right to resort to certain forms of collective action, which is already recognised in the consumer protection field, should be extended to privacy matters. Such an entitlement to "class actions" is particularly relevant in an area where it is often difficult to assess the detriment suffered by data subjects and where the low level of damages awarded is a disincentive to individual actions.**

- **In addition, many other aspects of consumer law could usefully be applied to data protection. Examples are the obligations to provide information and advice, which could be imposed on operators offering services that essentially involve the management or supply of personal data, such as Internet access providers and personal database servers (case-law databases, search engines and so on), the law governing general contractual conditions (applicable to privacy policy) and measures to combat unfair commercial practices and competition.**

- **Finally, providing personal data as a condition of access to a site or an on-line service could be viewed not merely from the standpoint of data protection legislation – does the user's consent meet the necessary requirements and is it sufficient to legitimise the processing in question? – but also that of consumer law, if only in terms of unfair practices in obtaining consent or the major detriment arising from the imbalance between the value of the data secured and that of the services supplied.**

- Another avenue to be explored is whether consumer product liability for terminals and software can be extended beyond any physical and financial harm caused to include infringements of data protection requirements. How far is the supplier of browser software whose use leads to breaches of privacy objectively liable for data infringements by third parties?

---

[119] See California Online Privacy Protection Act (OPPA), and Californian « Business and professions Code »

[120] See the report to Congress "Privacy Online: Fair Information Practices" May 2000, available on the FTC site: http://www.ftc.gov/os/2000/05/index.htm. In the United States, the FTC, which is very active in the consumer protection field, has played a key role in protecting citizens' privacy.

CONCLUSIONS

The advent of the Internet has created a need for a third generation of data protection regulations. It is not a question of turning one's back on the first two generations but of providing an addition level of protection, while leaving unaltered the measures already introduced. The first generation was mainly based on the nature of the data, namely whether it was sensitive and concerned individuals' private domain. Informational self-determination was then equated with banning the processing of such data, and was encapsulated in Article 8 of the European Convention on Human Rights. The second generation was concerned, not just with protecting personal data, but also with the way in which its processing could modify the balance of power between information processors and the subjects of that processing. Informational self-determination was thus extended to adjusting this balance by ensuring that such processing remained transparent and restricting the right to process data about others. This was the origin of Convention No. 108. It has many emulators and has amply justified its existence.

The emerging third generation, which we hope will be rapidly adopted, is characterised by its recognition of the technology itself. The use of new technologies multiplies the amount of data and the individuals capable of accessing it, increases the power of those who collect and process it, and bridges frontiers. A further factor to be taken into account is the complexity and opacity of this technology. A third party – be it the terminal or the network – now intervenes between individual and data controller. Informational self-determination calls for a measure of control over this third party.

Avenues of inquiry

How should this control be exercised? The following suggestions do not exhaust the subject:

- **"The answer to the machine is in the machine" according to Clarke[121], in connection with the problems the information society poses for copyright. It may also suggest ways of tackling the threats that same society poses for privacy. As has already been seen, the principle of reciprocal benefits and the promotion of "privacy minded" technological approaches can help those concerned to exercise closer control over the circulation and use of their personal information.**

- **This optimism has its limits. Although these technologies may contribute to what some call user empowerment, there is a risk that the individuals concerned will be left to face data controllers unaided. In reality, the technology is not neutral: although it is widely on offer to citizens, it is still indirectly financed by the businesses and official agencies and departments that pay the computer servers. Inevitably, the latter are likely to be more attentive to data controllers' interests than to those of data subjects. So-called privacy protection technology transforms or could transform the relationship between individuals and their own personal data into a property relationship that, thanks to the new technologies, becomes negotiable. It therefore needs to be stressed that informational self-determination is a personal freedom that is absolutely not open to negotiation and that society has a duty to fix certain limits to the right to use these data.**

[121] C. Clarke, "The answer to the machine is in the machine", in *The Future of Copyright in a Digital Environment*, B. Hugenholtz (ed.), Kluwer, 1996, p. 139 ff.

- **This focus on the technological tools must also extend to new players outside the ambit of second generation legislation, namely communication services and terminal equipment suppliers. Their role is critical to any attempts to enable the users of new information society services to monitor data entering and leaving the system, as well as the data tracks they offer to networks and their possible use. Consideration must be given to establishing strict liability for the supply of privacy compliant equipment and services.**

Firstly, therefore, Internet access providers, and mobile and other telephone operators are responsible for informing the public of the risks attached to the use of their networks, reporting privacy-threatening technologies and offering access to appropriate privacy-friendly applications. These access providers have a key role as they act as gatekeepers between users and the network. They are therefore asked[122] to "inform users about technical means which they may lawfully use to reduce security risks to data and communications", to "use appropriate procedures and available technologies, preferably those which have been certified, to protect the privacy of the people concerned ....., especially by ensuring data integrity and confidentiality as well as physical and logical security of the network" and to inform Internet users of ways of "using its services and paying for them in an anonymous way". Subscribers should be offered a hotline enabling them to report privacy violations and providers should subscribe to a code of conduct requiring them to block access to sites that fail to meet data protection requirements, no matter where the site is located.

The second target is made up of equipment and software manufacturers and developers, and those responsible for drawing up technical standards and protocols used in the transmission of network information. They should ensure that their products or standards[123]:

- **comply with the law, for example by ensuring that Internet browsers transmit the minimum information necessary for connection and adopting appropriate security measures;**

- **facilitate the application of the principles outlined in Part II, for example to allow users direct access to their personal data and a right of automatic objection, particularly through the use of weblogs;**

- **raise the level of protection of personal data.**

- **New technology makes it increasingly possible to process data relating to individuals not, as was traditionally the case, through data relating to their legal identity, such as name or address, but via an anchor point or even an object (so-called ambient intelligence) associated with it. This means that the danger often no longer resides in the collection of personal data as such but in the subsequent application of abstract profiles to individuals.**

- **Terminals, in the broad sense, must be become totally transparent technological tools for those who have and use them. Moreover, in many cases they actually**

---

122 Recommendation R (99) 5, III, 1, 2 and 4.

123 See the Belgian Commission opinion no. 34/2000 on e-commerce and data protection.

belong to the individuals concerned and may be seen as part of their home. Any intrusions into their privacy must be treated like any other intrusion.

- **The opacity and complexity of sophisticated information systems to which persons submit data call for surplus information that is no longer focused solely on the processing itself or individual characteristics, but rather on the overall functioning of the information system and its ability to generate a vast quantity of information, present and future. Hence the need to document data (origin, users, logical justification), describe the various information flows and lay down rules governing how decisions are taken, who has access and how it is monitored.**

- **Hitherto, the data protection authorities have made little use of technological tools. They rarely employ computer specialists or penetrate the inner sanctums of those who decide what technological developments will take place and how products will be configured. Just as European states have demanded the establishment of a Governmental Advisory Committee (GCA) to the ICANN, a private body responsible for managing Internet domain names and addresses, it might equally be necessary to propose or even insists on a Data Protection Advisory Committee to ICANN, W3C (World Wide Web Consortium) and the IETF (Internet Engineering Task Force). It is necessary to make the electronic communications sector fully aware of the importance of data protection.**

To summarise, the main topics of the proposed avenues of inquiry for Consultative Committee consideration are:

- the need to supply individuals with all they need to understand and control their computer environment, particularly where it penetrates their homes. They must be given control of any tools whose use reveals them to others;

- the need to give society the tools to control technological developments that could otherwise threaten the survival of our individual and collective liberties.

Highway legislation imposes certain rules on users not just to reduce accidents but also to strike a satisfactory balance between the rights and obligations of different road users, with the courts being inclined to offer particular protection to the most vulnerable among them. This necessitates not just a highway code but also specific legislation on the road network itself and the vehicles permitted to use it, which are subject to certain mandatory standards.

On the information highways, there is no legislation laying down operating rules for telecommunications to protect users' privacy or requirements to ensure that telecommunications terminals that allow users to travel on these highways operate fairly and transparently.

Only by applying traditional data protection principles to these new technologies, which are implicit but unavoidable components of all telecommunications, can computerisation lead to a democratic information society, bringing general progress for all.

Yves Poullet
yves.poullet@fundp.ac.be

Jean-MarcDinant
jean-marc.dinant@fundp.ac.be

http://www.crid.be