COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-PD-BUR(2010)09 EN

THE BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD-BUR)

Report on the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) resulting from technological developments

(Part I)

CENTRE DE RECHERCHES INFORMATIQUE ET DROIT

By:

Jean-Marc Dinant, Doctor in Information Technology
Research Director at. the Computer and law research centre (CRID), Legal Expert

Cécile de Terwangne, Professor at the Law Faculty at Namur University
CRID Research Director

Jean-Philippe Moiny, aspiring to F.R.S-FNRS,
CRID Researcher

In collaboration with:

Yves Poullet, Dean of Namur University (FUNDP), Professor at the Law Faculty
CRID Research Director

Jean-Marc Van Gyseghem, CRID Senior researcher

TABLE OF CONTENTS

PART I

PART II

PART I

Author:

Jean-Marc Dinant, Doctor in Information Technology
Research Director at. the Computer and law research centre (CRID), Legal Expert

---

1. New micro-telecommunication networks

The first decade of the 21st century has seen new telecommunication networks spread at an ever-increasing speed, while the development of the Internet, as much in terms of speed as mobility and ubiquity, continued apace, at least in developed countries.

Various wireless short-range networks (between a few centimeters and some tens of meters that we will hereafter call "micro-networks"), mainly networks like WiFi, RFID and Bluetooth, have recently developed without much case for the respect of data protection and privacy of their users.
WiFi interfaces today are widespread in laptops and progressively in mobile phones. In practice there is a convergence between laptops and mobile phones. The former increasingly enable telephony through VoIP applications such as Skype. The latter not only enable their users to telephone, but also increasingly to surf, receive and send emails or even access social networks via the Internet. These networks represent today a major threat that is insufficiently taken into account in relation to the traceability of users, or more broadly in relation to human carriers of these terminals connected to these new telecommunication networks. These risks can be summarized as follows:

- **Loss of control**: the absence of a physical wired connection for these new networks makes their disconnection problematic and their functioning invisible even to an informed user. This problem is particularly troublesome for RFID chips that operate without batteries, and whose minuscule size of a few millimeters does not help the user detect their presence. As these chips are used notably in the fight against shoplifters, there is obviously no interest in making these chips visible, since a potential thief could ripout or damage them.

- **Lack of privacy**: the three networks mentioned above are not systematically encrypted. Particularly concerning the WiFi network, it is relatively easy for a third party to pick up and read the traffic between a wireless terminal and a wireless base station.

- **Traceability possibility**: Even when communications are encrypted, the unique electronic serial number that equips a WiFi base station, a RFID chip or a Bluetooth mobile phone remains

generally easily readable. These devices are server in nature, meaning that, technically, they automatically respond to a connection attempt, even if it is abusive and not acted upon, by communicating their globally unique electronic serial number (GUID = Global Unique Identifier). In general, it is therefore technically possible to read a Bluetooth serial number, the MAC address of a WiFi card or the serial number of a RFID chip, even without initiating a real communication.

In conclusion, these widely distributed new networks whose growth will be exponential in the years to come, allow in a technical and invisible manner the individual tracking of each terminal equipped with a WiFi, Bluetooth or RFID interface, unknown to its owner even when the terminal equipment is not voluntarily activated.

2. The boom of geolocation

Harnessing the serial number of a wireless terminal can be done using a computer equipped with geolocation, typically GPS[1]. Since these new micro networks are increasingly connected to terminals that are themselves connected to the Internet, the dynamic IPv4 address that is renewed randomly and regularly no longer provides effective protection against the traceability of telecommunication network users. Indeed, it is often possible to identify a serial number or a unique tag specific to the micro network used. The fusion of these micro-networks with the global Internet network silently and unavoidably leads to individuals being increasingly and systematicaly tracked.

We must comprehensively analyse the risks of this geolocation. It is more than just knowing where an individual is at a particular time:

- This system applied to a large proportion of the population allows to know **with whom** a specific person is and thus be able to map out family, professional or friendly relationships of each person.

- Many places are marked with special significance. Knowledge goes beyond mere information. Number 25 in the main street of a big city is *a priori* not very meaningful, unless we know it is a mosque, a psychiatric hospital, a union's headquarters, a police station or a court.

- The paths of an individual represent a certain type of behaviour. It is thus possible to know if a person stops in front of a window or if she is jogging. Inside a department store the paths of individuals are representative of purchasing behaviour.

This geolocation can also be coupled with systematic monitoring of users' online behaviour previously described[2]. The coupling of both systems (online profiling and geolocation) is

1

2

technically facilitated by the interconnection of geolocation micro-networks with the terminal used to connect to the Internet.

3. The invasion of cookies or the disappearance of untraceability

Cookies were designed to trace Web users, notwithstanding the change of IP address or sharing the same address for multiple users. This traceability may be necessary for online electronic transactions but technically only the direct session cookies are justified for this purpose. Yet, what poses a problem today are residual cookies or from third parties and consequently residual cookies from third parties that transclusively monitor traffic. On this note, the world champion is unquestionably Google which, thanks to its Google Analytics system continuously collects traffic (the URL and therefore the content) on most websites.

However, until recently, a configuration of browser settings allowed the informed user to block third party cookies. It is noteworthy that no conventional browser allows to block transclusivity (ie the automatic incorporation of contents by third-party sites unknown to the user (contactability) and the communication of traffic data to these third-party sites (observability). The blocking of residual third-party cookies acts solely on traceability. Two important elements have challenged this marginal control of traceability.

The first reappraisal of the possibility for the advanced user to block cookies in the HTTP web protocol was triggered by the emergence of flash cookies. Macromedia distributes flash technology on a global scale as a plug-in that is installed on most common browsers. This plug-in has its own mechanism and an independent data management system that can be used in the same way as a cookie system. In this case, the blockage carried out by the browser turns out wholly irrelevant. It is possible for an expert user to find a way around to this plug-in's strange behaviour that has this ability to read and write data on the mass memory of the terminal. However, as flash cookies are little known and that to block them requires in-depth technical knowledge, this type of blocking is seldom used.

A second phenomenon casts doubt on the blocking of third-party cookies by the informed user. For mobile phones in general and for the Apple iPhone in particular, there is a tendency for major websites to develop their own applications. While their website could be used via a standard web browser like Firefox, many companies (Amazon, Facebook, Google, some newspapers) develop and distribute their own application. This application uses the HTTP protocol but the user no longer has the ability to block cookies and, even less the transclusivity.

Along the same lines, the systematic incorporation of the MAC5 address in the IP version 6 address (IPv6) increases (will increase) significantly and on the sly tracking capabilities of surfers on websites. Despite a change of IP address and contrary to the current IP version 4 (IPv4) protocol, each IPv6 address will contain the unique serial number of the computer's controller. This risk, far greater than residual third-party cookies, currently remains insufficiently taken into

consideration by data protection authorities. An alternative IPv6 protocol generating a random address exists and has been approved by the W3C.

In general, it can therefore be observed that the weak barriers that enabled the informed user to fight against traceability on the Internet are slowly but surely being eroded.

4. Social networks

If at the end of the twentieth century, email and chat were the most popular means of interpersonal communication on the Internet, we have seen social networks develop, which are a natural technical evolution of the blogs of yesteryear. The innovation here is social: where blogs focused on an issue or particular theme, social networks focus on individuals. These social networks have rapidly become a way to interact and make oneself known on the Internet. The designers of these social networks have rapidly perfected specific applications that allow others to browse these networks and intervene on the profiles that are stored there, according to what users and the network designer allow. These social networks are generally falsly free, i.e. their users pay the social network through its advertisement exposure. Policies to protect the privacy of these networks are generally dictated by the site designer who can enable those concerned to set up, to a certain extent that they determine, the visibility of stored information vis-à-vis third parties.

Historically, laws regarding the protection of personal data focused on the twin concepts of personal data and "file master" or "processing manager". These two concepts seem to have now become at the same time too vague and too narrow to lead to effective regulation of the right to respect for privacy within the ever-changing technologies and uses of information and communication society.

5. A functional approach to the concept of personal data

Any data related to an individual usually identifies one of their characteristics. This data may be biographical and/or tracer.

In the first case, the data pertaining to an individual says something about this person: e.g. a fact, a gesture, a route or a purchase; it is the person’s property that may be shared between several people. For example, being Catalan or Corsican is personal data of each and every Catalan or Corsican. It is "biographical" data in the etymological sense, i.e. information which describes life, or more exactly a slice of life, a characteristic of an individual. What is at stake here is therefore the **knowledge** of one or more characteristics of an individual **in a particular context**.

In the second case, the data relates to an individual and constitutes a unique characteristic or a single value of certain variables that clearly distinguishes it from other people within a given

population. So, an IP address uniquely identifies a person at a given time. It is a Unique Identifier. This identifier is hardly problematic when it comes to identifying an individual in a particular context (account number in a bank, patient number in a hospital, student number in a university, citizen number in a public service, affiliate number in a trade union, etc.). However, in practice, these identifiers are rarely local but instead rapidly become global, i.e. multicontextual. We then talk of a Global Unique Identifier. This kind of identifier enables to trace the same person in several different contexts. The issue here is therefore **multicontextual knowledge** of the same person.

Contactual data is a third type of data. An email address, a postal address, the URL of a "wall" on a social site lets a third-party communicate content to an individual identified by a contact data. Thus, for example, knowing an email address could identify several web pages related to the same individual. **Contactability**, or what's at state for this kind of data or the possibility technically offered to a third party to inject informational content (in particular advertising) in a letterbox or on a screen. In this context, marketing is naturally concerned and, more specifically the individual's control over his **advertising exposure**.

This functional division of data actually distinguishes three types of personal data which are substantially different. They are, more precisely, properties of personal data. Thus, an email address such as "john.smith@coe.int" combines the three properties described above. We know that John Smith works at the Council of Europe. By typing his email address in a search engine, we can find related information and finally the email address allows us to contact John Smith, possibly for promotional purposes.

Very (too?) long debates have taken place for a long time on the nature of personal data of the IP address or cookies. It is worth-noting that the apparent importance of this debate is linked to a confusion among businesses, particularly multinationals. Article 8 of the ECHR does not protect the private life of an identified or identifiable person. Any person even non identified or identifiable is entitled to such protection. The right to protection of personal data does not exhaust the right to protection of private life. Thus, for example, the ubiquitous surveillance of people in public or private places by means of video surveillance is indeed an intrusion into the lives of the people filmed, even if they remained non identifiable thanks to clever blurring of faces.

In other words, in our view, there are no data concerning an individual which don't identify him, either in a traceable or biographical way, or that does not allow to contact them.

It should be noted that some of these problems are already taken into consideration by certain European directives which do not seem to have an equivalent in the Council of Europe. Thus, for example, Directive 95/46/EC provides for the right to object to direct marketing without any justification. Directive 2002/58/EC regulates the use that may be made of email and subjects its use for commercial purposes to the consent or to the possibility to exercise a right of opposition by the person concerned. Directive 2006/24/EC exhaustively sets out traffic data to be retained by telecommunications operators, by deragation from Directive 2002/58. Etc.

It should be noted that these provisions of European Community law demonstrate greater pragmatism and claim to protect private life and personal data. Moreover, it can be noted that the protection of email will benefit to legal entities as well as to natural persons.

In conclusion, it has become less and less relevant to wonder whether this or that data is personal data but rather to identify the risks posed by the use of data from information technologies and communication in a particular context by a given user and to bring about a principle response.

In our opinion, the most sensitive data today are the Global Unique Identifier hardware (electronic serial number) or software (cookie) insofar as, being firmly attached to a telecommunication terminal, they allow the same user to be traced in different contexts. The use of these unique numbers should be restricted to the terminal. They should not have to transit to telecommunication networks, in the absence of appropriate safeguards.

Traffic data should also enjoy special status. In European law, the principle of immediate destruction or anonymisation of traffic data is contained in Article 6 of Directive 2002/54. By exemption of this general principle, operators, based on Directive 2006/24, are forced to keep a limited amount of data for a limited period of time and solely for the prosecution and the search of criminal offenses. It is cutting to note that Google today collects in real-time all web traffic data on an individual basis and for commercial purposes (direct marketing brought in more than six billion U.S. dollars to Google in 2009) while such collection is explicitly prohibited to telecommunication operators for detection and prosecution purposes by the police for criminal offenses. In other words, a powerful Internet player daily and de facto collects far more personal data for commercial purposes than the police services can, through operators, for the fight against public safety violations.

6. The file master

Directive 95/46/EC as much as Convention 108 distinguish two people responsible for data processing: the processing manager (file master) and the subcontractor.

This categorisation no longer seems appropriate. The ICT world has become specialised and new professions have been created. Others will emerge tomorrow.

To achieve successful completion of this regulation, the legal regime should be adapted based on the role of the company that does the collecting, storing or transmitting of data regarding individuals.

We are also fully aware that this regulation is currently facing a problem of private international law. Like consumer law, shouldn't data protection (which is becoming an increasingly important aspect of consumer law) be that of the person concerned and not that of the company

establishment that collects, stores or transmits that data? This will be discussed in detail in the second part.
Under public pressure, some major players (Facebook, Google) have sometimes changed their privacy policies, but such a trial and error method of regulation does not seem satisfactory. Increasingly subtle attacks against personal data protection and privacy of Internet users are motivated by economic considerations of major Internet players and generate, as a side effect, problems whose social costs are paid by society as a whole.

On this specific point, we observe that the financing of many Information and Communication Society tools (search engines, social networks, email,...) is based on advertising. The key argument of publicists, namely free Internet, reveales some flaws when analysed. If advertising finances the Internet, it must be asked who finances the advertising. Far from receiving free Internet, the consumer actually pays twice. He first pays in kind by being profiled, analyzed and manipulated both consciously and subconsciously. The consumer pays a second time by buying the product or service promoted, whose cost is inevitably included in the end price.

Many authors have reflected on the commercial exploitation of privacy and personal data. It is now commonly accepted that the protection of private life is a fundamental freedom. And it is because it is a fundamental freedom that private life can, to some extent and under certain conditions, be profited from. Following the example of the right of image capitalised by stars of show business, each individual should be able not only to refuse or accept advertising exposure but also to profit from it in hard cash. It would therefore be desirable that access to information and communication society services no longer depends on a de facto obligation to comply with behavioural analysis and injection of advertising content, but can be paid by the consumer through a financial contribution. These services without advertisements could be made accessible to citizens by Internet service providers, with a modest fixed financial contribution included in the cost of the Internet subscription. Indeed, if one divides the benefit of Google roughly by the number of Internet users concerned, we realise that access to Google's services could be given for the price of around one euro per user per month, without significantly affecting Google’s profits.

7. A success story?

In our view, the modern mobile phone network remains an example to follow in the protection of private life integrated at the heart of technology. On the one hand, mobile phone terminals must (at the risk of not being approved and therefore impossible to sell) include the Calling Line Identification Restriction. This feature allows any user, even beginners, to hide their phone number from the person they call. Technically, it should be known that this number is always transfered, allowing for example emergency services, as provided by or in accordance with law, to be able to identify the number calling their services.

Mobile telephone devices also have an electronic serial number called IMEI (International Mobile Equipment Identity). This serial number is transmitted to the telephone network operator and to nobody else. The network operator does not technically transmit this serial

number to the mobile device of the telecommunication recipient. However, under Directive 2006/24, operators must keep this identification data. These technical features give the user real control over the mobile phone. They can hide their phone number and manage its traceability and contactability. Their communication is encrypted and is not easily observable by a third party.

We can see some consensus about the principles of privacy and personal data protection (privacy ontology: control observability, traceability and contactability; respect of the principle of finality (data contextualisation), much research on "privacy by design" is underway.

We believe that faced with the current and future challenges the law should apply in a different way to all players of information and communication society, according to the role they play and the type of data they process. On the information highway, the highway code is no longer enough; vehicles must be produced, as well as the technology that implements these principles of driver protection. "If the technology is the problem, the technology may be the answer ..."

PART II

Author:

Cécile de Terwangne, Professor at the Law Faculty at Namur University
CRID Research Director

Jean-Philippe Moiny, aspiring to F.R.S-FNRS,
CRID Researcher

In collaboration with:

Yves Poullet, Dean of Namur University (FUNDP), Professor at the Law Faculty
CRID Research Director

Jean-Marc Van Gyseghem, CRID Senior researcher

INTRODUCTION

This report aims to identify areas where specific problems have arisen in connection with the principles of protection of personal data when making use of new technological developments.

All in all, the reflection looks to what extent the provisions of Convention 108 for the Protection of Individuals with regard to the automatic processing of personal data and its Additional Protocol of 8 November 2001 concerning the supervisory authorities and transborder data flows always respond adequately to the expectations and current concerns related to recent technological developments. Do these provisions still adequately ensure data protection when turned to the Internet, multiple applications that have emerged on the Web 2.0, geolocation technology, data exchange, RFID chips, biometric identifiers, surveillance techniques, etc…?

To this end, the report is in two distinct parts. The first part, in an attachment, contains a description of changes in “landscape technology” since the date of adoption of Convention 108 while addressing the important issues related to these changes. It discusses the "new vulnerability of individuals faced with changing technology." The second part of the report is the object of the following pages. It is devoted to an analysis of Convention 108 provisions in view of what is at stake from these new facts so as to identify possible gaps in the existing text faced by new dangers and expectations in terms of data protection.

This report may in some way be considered an update of the report "informational self-determination in the Internet era", on the application of data protection principles of Convention 108 to global telecommunications networks, written in 2004 by the Computer and Law Research Centre (CRID), Namur

University (Belgium) at the request of the Council of Europe. To this extent, some parts that are still relevant are taken from the original text with the necessary adjustments in form. These passages are highlighted in yellow.

COMPARISON OF CONVENTION 108 PROVISIONS WITH A NEW TECHNOLOGICAL ENVIRONMENT

At this stage the analysis of the comparison of Convention 108 provisions and its Additional Protocol of 8 November 2001 regarding supervisory authorities and transborder data flows with a new technological environment as described in the first part of this report. This comparison can check whether these texts still respond adequately to new challenges and still guarantee adequate protection for individuals with regard to the processing of personal data. The objective of this second part of the analysis is therefore to update potential gaps in the protection.

The analysis, focusing on the text of the Convention, logically follows the same structure.

Clearly, a set of documents which have been discussed or adopted in various international fora on the subject have fed the content of the following pages. In particular, documents have been taken into account from organs of the Council of Europe itself, the European Union (Directives, opinions of the European data protection, Commissioner documents of the European Group of Data Protection Authorities (called Group of article 29), the OECD and APEC has adopted the most recent regional text on the subject. The Madrid Resolution has also fueled this timely discussion. This text, resulting from a concerted work of data protection authorities from more than fifty countries led by the Spanish Agency for Data Protection, therefore integrates data protection values and principles guaranteed on five continents. It aims therefore to provide a model incorporating universal data protection standards. Finally, the case-law of the European Court of Human Rights and the Court of Justice of the European Union was also taken into account when it could clarify the analysis.

1. Object and purpose of the Convention

1.1. THE PURPOSE OF THE CONVENTION: DATA PROTECTION

1.1.1. Data and Privacy protection

It is interesting that Convention 108 has, from the outset, assimilated data protection to respect for every individual "*his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him*".

The Convention states explicitly in Article 1 that data protection is not limited solely to the protection of privacy. Other rights and freedoms are taken into account, such as freedom of movement, that of insuring, housing, finding a job, information seeking and expressing oneself transparently, etc.. Thus, the creation, within inter-firm networks or inter-administration, *a priori* database profiling of service users can lead to discrimination when looking for housing, searching for information, applying for insurance by or purchasing a book. Another example is the gradual replacement of traditional payment methods by payment using credit cards whose issuers are an oligopoly would require a reflection on the potential impact on citizens by removing or either blocking a credit card in terms of freedom of movement, or analysing the uses of the card in terms of global surveillance activities of the individual.

If the issue of data protection is not limited solely to the protection of privacy, the link with the latter, however limited. Data protection is an offshoot of the right to respect for private life taken in the dimension of personal autonomy or even the right to self-determination which is linked, more than in the sense of confidentiality requirements attached to the traditional notion of privacy. Data protection is the right to "informational self-determination." Convention 108 clearly reflects this approach by strengthening the capacity of citizen oversight for the processing of their data by granting a right to information and a right of access to data held by others and by setting limits on the right to process data in the hands of both public and private actors (legitimate purpose, proportionality, security ...). Elements of a more negative and restrictive approach, where privacy is considered a defensive concept, however, are found when sensitive data are involved (Article 6 of the Convention), principles prohibiting rules guaranteeing the protection of citizens against breaches of confidentiality of such data.

It is in this sense that the Parliamentary Assembly of the Council of Europe has sought to supplement its resolution 428 (1970). Indeed, the right to respect for private life under Article 8 of the European Convention on Human Rights was established by the Assembly in January 1970 in the Declaration on the means of mass communication and human rights contained in this Resolution as "the right to conduct his life as we understand it with minimal interference." Nearly thirty years after the initial adoption of this text, the Assembly stated that, "To account for the emergence of new communication technologies for storing and using personal data, should be added to this definition the right to control its own data. "

The Charter of Fundamental Rights of the European Union, which became legally binding since the entry into force of the Treaty of Lisbon, took the option – to say the least - to distinguish the concepts of private life (Article 7) and data protection (Article 8).

By empowering the right to respect for private life, the right to data protection requires consideration, on the one hand of power imbalances between the person concerned and the person processing the data, imbalances caused by data processing capabilities available to the latter and dramatically exacerbated today due to technical developments and, on the other hand, the impact that data processing can have on the various rights and freedoms mentioned above. Technologies, more by choice of configuration than necessity, generate and preserve the "footprints" of the use of services and allow, through processing capabilities incommensurate with those prevailing a decade ago (what about twenty-nine years ago ...), knowledge of the individual and his behaviour, individual or collective, personal or anonymous. In other words, their use increases the imbalance in the relationship between those who have the information and individuals concerned or not. On the basis of information collected, decisions that are collective (e.g., setting the rate of reimbursement for treating a disease) or individualised (e.g., refusal to grant credit or a bank service) will be taken.

To sum up, Convention 108 has not fallen into the trap of reducing the data protection field of the protection of private life, a pitfall particularly damaging if this field is only considered, as is sometimes the case, in the classic line of "right to be left alone". It is a requirement of confidentiality unfortunately. Having that said, **would it not rather be about highlighting the extent of the concerns expressed by the concept of right to data protection? Must we consider a loophole the fact that the Convention does not explicitly mention in the definition of data protection contained in Article 1 the aspect of the individual's control of personal data that concern him?**

The explicit mention of this aspect may have pedagogical virtues suitable in particular in cases where Convention 108 is called to serve as a signal for non-members of the Council of Europe, countries that wouldn't have the knowledge of the evolution that the concept of "private life" has known within the

case-law of the European Court of Human Rights, as well as among the institutions of the Council of Europe and within the European Union. This is especially important considering that it is stated in the Preamble to the Convention that the signatories to the Convention recognise "the need to reconcile the fundamental values of respect for private life and the free flow of information [...]". Private life is here the only value given to justify for the protection scheme devised. It is therefore crucial that this concept is appreciated in its "modern" meaning and specific to the matter.

The mention of this control or of this informational harnassing in the name of self-determination would clearly demonstrate that the Convention is not just a defensive instrument, designed to guarantee data confidentiality or to prohibit the processing of certain sensitive data, but it reflects a more positive approach in that it is the manifestation of the right to informational self-determination.

1.1.2. Data protection and human dignity

There is no mention in the Convention of the protection of human dignity. **The evocation of human dignity is a reminder that a human being is a subject and can not be reduced to a mere object of surveillance and control of another.**

The European Court of Human Rights did not hesitate to support its reasoning explicitly in terms of respect of private life on human dignity. It has indeed stated that "the very essence of the Convention is respect for human dignity and human freedom. Under Article 8 of the Convention in particular [...]". The Court of Justice of the European Communities (now Court of Justice of the European Union) also highlighted the value of dignity as inherent to individuals, to be legally protected. In a case involving a transsexual, the court proclaimed, "To tolerate such discrimination would be tantamount as regards such a person, to a failure to respect the dignity and freedom to which he or she is entitled, and which the Court has a duty of safeguard.

French law on data protection proclaims from the beginning that, "It must serve every citizen. [...] It shall infringe neither human identity, nor fundamental rights or private life or individual or public freedoms." We can see expressed in this phrase a strong concern close to respect for human dignity, the idea that a human being can not be subjected to the machine but that it instead should be at his service and that it can undermine the core values of individuals.

Directive 95/46 of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data garantees, the right not to be subject to a decision taken by a machine. This right of every person not to be subjected to a fully automated individual decision is in the name of human dignity.

It will be proposed in the chapter on additional guarantees for those concerned to include this expression of supremacy to be accorded to human dignity. However, it could also be considered to include the latter in the values underlying the rules of data protection under the Convention.

This reminder of the fundamental value of dignity as data protection or private life is without doubt necessary in view of certain uses of technology. Information systems are increasingly carrying out comprehensive monitoring of populations and individuals, creating a system of transparent behaviour of people which may be contrary to human dignity. Similarly, the phenomenon of profiling that leads to

deducing information without the knowledge of persons concerned in order to make them implement decisions of any kind can seriously impair the dignity of the profiled individuals.

Dignity is also clearly and repeatedly invoked in the draft recommendation concerning the protection of data in the context of profiling. Two recitals are very explicit: “14. Considering that the use of profiles, even legitimately, without precautions and specific safeguards could severely damage human dignity, as well as other fundamental rights and freedoms, including economic and social rights ; 20. Considering that the protection of human dignity and other fundamental rights and freedoms in the context of profiling can be effective if, and only if, all the stakeholders together to contribute a fair and lawful profiling of individuals;” .

1.1.3. Data protection, support or questioning of other freedoms

That private life or in a broader sense data protection is a guarantee of our liberties goes without saying. Thus, to speak of freedom of expression and association, how can we imagine that they can survive if the person knows that their communications are monitored and that a person can at times speak anonymously if technology systematically keeps records of their messages? The freedom to gain knowledge implies that information is not filtered, that we cannot be lead, through profiling, whithout our knowledge or despite ourselves, to information that other people want us to consume. Worse, the same profiling technique may lead the person behind the profiling to deny a consumer certain services or information for which they believe it is not profitable enough to allow access. These examples could be multiplied vis-à-vis individual freedoms enshrined in the European Convention on Human Rights. Data protection is undoubtedly the support for many other freedoms and guarantees.

Sometimes, however, the concern for protection of data hampers the development of other freedoms. In particular, **data protection must be balanced with the need to protect freedom of expression and opinion.**

The preamble to the Convention implicitly recalls: "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", however no provision of Convention 108 explicitly enshrines the need for this balance. The Convention claims to express this balance. Article 9 while allowing for exceptions and restrictions on the protection system (except for obligations associated with data security), provides that an exemption is allowed if, prescribed by law, it is necessary in a democratic society for the protection of rights and freedoms of others. At the forefront of these rights and freedoms most certainly features the freedom of expression. The system of cross-border flows (Article 12 and Additional Protocol) does not benefit from the possibility of exception. It is nevertheless allowed for each state to authorise a transfer of data normally forbidden, when legitimate interests prevail. Again one can easily imagine that freedom of expression is among the legitimate interests mentioned. If the system of exceptions can probably resolve the friction between free speech and data protection, nevertheless it would perhaps not be superfluous to specifically invite states to try to reconcile the two conflicting interests. European Directive 95/46, while offering a derogation in the same line as Convention 108, specifically calls on states to adopt exemptions and exceptions for treatments "made solely for purposes of journalism or literary expression and the arts " to " reconcile the right to private life with the rules governing freedom of expression".

This concern not to negatively impact, through data protection, freedom of expression and opinion has so far been met by certain provisions protecting the working conditions of journalists in particular in the online world. However, it increasingly appears that it is essential to strike a balance between data protection and freedom of expression in general. This reflection is particularly relevant since the advent of the Internet, discussion forums, blogs and social networks. Indeed, using these media is a common way today for people to express themselves, to share their activities and relations with others. It is both the Internet as a place and means of expression as citizens and so-called "Web 2.0 for fun." It is unthinkable on several points to observe the normal rules of data protection in connection with such communications.

The enforcement of data protection laws with the multiple obligations they entail vis-à-vis third parties (obligation to report, etc..) poses a tricky problem with respect to freedom of opinion and expression that could well be restricted.

The Linqvist case decided by the Court of Justice of the European Communities illustrates this point. On the Internet can we talk about personal, associative or professional relationships without being subject to the requirements of the law on protection of personal data? The Court reiterated the duty, given the circumstances, to take into account the proportionality of the restriction on the exercise of the right to freedom of expression which the enforcement of rules aimed at protecting the rights of others entails. The formula is vague and refers to a judgment of proportionality. This ruling can hardly be on an equal footing with journalistic expression whether in traditional format or on the Internet, for which rules have gradually been identified and the freedom of expression of everyone, whose existence necessarily refers to that of others. On this last point, however, the ECJ has recently passed judgment granting the derogation system originally forseen for “press” for any public disclosure of personal data.

Technical developments that emerged after the adoption of Convention 108 also led to the application of **data protection rules affecting the privacy of correspondence or communications. This friction is caused by the use of electronic mail and other electronic exchanges**. In this form, correspondence is transformed into automated data processing. The rules of transparency, right to access and right of correction are therefore applicable when it is not the case when in conventional paper mail format (which, if lacking data structuring, would not even pass as a file covered by protection rules in other Party-States that have expanded the scope of the Convention to non-automated files). Accordingly, these protection rules permit others mentioned in the electronic exchanges to be informed about the contents of the exchanges, which produces a clear violation of privacy of correspondence or communications. A system of appropriate exceptions should take into account this confrontation between data protection and privacy of correspondence or communications.

The use of traffic data also produces a breach of privacy of communications. This use should be strictly supervised.

Some data protection system rules also involve a **risk of infringement of freedom of scientific research**. Research, primarily medical, uses data that is - mostly - coded in such a way that is difficult but not impossible to link to a particular individual. Scientists are therefore faced with having to comply with the rules on the protection of personal data, rules that are often unworkable for them.

Let’s also think of the various rights of the individual concerned such as the right of access to data or correction thereof. It is indeed impossible for the researcher or his employer to respond to access requests since they do not know the individuals connected to the data (they only work with codes and

only a third-party who holds the key to the code). If the definition of "personal data" goes as far as to encompass any data on individuals identified by someone (in this example, the doctor at the data source but not the researchers themselves, who only have encoded data), this definition and, conversely, the underlying notion of anonymous data may be too severe and become an obstruction to research. Concepts should therefore be defined realistically.

1.2. SCOPE

1.2.1. Broadening ratione personae?

Should rules protecting profiles, beyond the protection of individuals, be forseen? Profiling means two steps: first, by determining a set of characteristics about an individual or a community of individuals linked to one or more behaviours carried out or expected and, secondly, subsequent treatment of those individuals or communities based on the recognition of these characteristics.
The question of the legal framework of profiling has led to the development of a draft recommendation. It will therefore not be discussed further here.

1.2.2. Restriction

Convention 108 does not restrict its application found in the laws of all member States of the European Union (at the invitation of Directive 95/46). It concerns data processing performed "**by a natural person in the course of a purely personal or household activity**". This processing is therefore excluded from the Directive and all relevant national texts that have implemented it.
Canadian law on Personal Information protection and Electronic Documents Act also provides for such exclusion. Article 4 § 2 (b) stipulates that the protection scheme does not apply "b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose. "
The APEC Privacy Framework introduced a similar restriction in its application through an exception on the definition of personal information controller. So, excluded from this definition is any individual "who collects, holds processes, or uses personal information in connection with the individual's personal, family or household affairs".
The Madrid Resolution accepts that national laws provide for an application for processing exclusion performed by an individual as part of activities exclusively connected to their private life and family (Article 3, § 2).
The importance but difficulty in applying such an exception in today's technological environment, mainly Web 2.0, is being reserved for developments in Section 7, below.

2. Definitions

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

Under Article 2, indent a. of the Convention, personal data must include "any information relating to an identified or identifiable individual ("data subject")". This definition has become classic and included in most of the data protection instruments. It should be noted however that the APEC Privacy Framework's approach differs from this by personal data only being aimed at identifying data (directly or indirectly). It

is stated "The APEC Privacy Framework applies to personal information, which is information that can be used to identify an individual. It also includes information that would not meet this criteria alone, but put together with other information would identify individual". This approach is more restrictive.

2.1.1. Identity: an ambiguous concept underlying the definition of personal data

The concept of personal data is based on the identification or the "identifiability" of individuals related to the data. In principle, regulation of data protection is applicable only if the data processed can be referred to a specific person. Yet the notion of identity is not obvious when confronted with certain new realities. Thus, is a RFID tag that traces a a garment personal data since it relates, at least directly, to an object, as well as the IP number which ultimately relates to a computer and not a specific user?

The notion of identity is ambiguous (see what is said on this point in the first part of this report presented in an attachment).

Identity has the annoying tendency to be interpreted restrictively by industry. Such an interpretation has the advantage of avoiding data protection rules because it removes the presence of personal data.

As an example of this restrictive interpretation, one can cite the case of the desire to merge the databases of Abacus and DoubleClick. We can also be surprised that the merger between "anonymous" profiles from DoubleClick and the nominative database of Abacus was technically possible. It simply means that DoubleClick who claimed not to collect any information on identifiable individuals nevertheless had an anchor to make the link. This link is probably the famous cookie identifier that DoubleClick has installed on millions of personal computers. All that is needed is on invisible hyperlink on an online nominative form for DoubleClick to make this connection.

A current trend in the industry is therefore to consider anchors and simple biographical data associated with them as data pertaining to an unidentifiable individual. Stable contact points over time are generally accepted as being personal data. In other words, surveillance and tracking of a person or goods that they own or use are not primarily seen as an invasion of privacy if the person is not identifiable and remains anonymous (that is to say if we do not know their name or if we do not know how to contact them. As if our behaviour was not a constituant in itself of our identity.

2.1.2. The "Identifiable" character

A problem avises in the scope of the term "identifiable" attached to an individual to make a "subject". The Explanatory Report to Convention 108 indicates that what was meant by "identifiable person" is a person who can be "easily" identified, which does not include the identification of people "by very sophisticated methods"." This clarification is no longer sufficient. The criterion of complexity of methods used to identify a person is not sufficiently informative. From a technical point of view, today, "very complex" methods are no longer necessarily out of reach.

The draft Recommendation on profiling does not use the criterion of complexity method of identification but rather of the magnitude of the means to be implement and in order to identify individuals. Thus, the text states: "An individual is not considered "identifiable" if identification requires unreasonable time or manpower".

The appropriate criterion should be found which is essential given that this criterion is key to the notion of personal data and, by contrast, anonymous data. For example, if the person holding the identification of a given subject is bound by professional secrecy and can not disclose this information under penalty of criminal sanction, will the data be considered as identifiable? Probably not. But will it still be if, duty to secrecy is not criminal but contractual?

The concept of personal data deserves to be clarified in terms of the forms it has been known to take as a result of technological developments. These notably include taking account of the practices of Internet service providers.

In the context of the thought process, we note that considering data as the cookie, IP address or Global Unique Identifier as "personal data" entails the application of the Convention provisions and can from there lead searching the identity of the persons concerned, even if only to allow access rights, even if this wasn't necessary for the purpose of the master file's activity. Moreover, applying provisions such as the obligation to inform the person concerned might not be possible without identification.

However, not treating the IP address and the GUI as personal data would be problematic given the risk that subsequent use of this data poses in terms of individual profiling or even the possibility of contacting them. In this regard, with the combination of tools to monitor traffic on the web, we can easily identify the behaviour of a machine and its user behind it. The personality of the individual can thereby be recreated to enforce certain decisions on him. Without even asking about the "identity" of the individual, that is to say their name and address, we can characterize them in terms of socio-economic, psychological, philosophical or other criteria and enforce certain decisions on them to the extent that the individual's contact point (their computer) does not necessarily require the revelation of their identity in a narrow sense. In other words, the ability to act vis-à-vis an individual no longer necessarily requires the ability to know his identity.

What is important now in the new technological context is rather individualisation than identification. Should the definition of personal data be made to evolve or appoint a definition that no longer includes data about a person that can be identified but that can be identified?

It is interesting to note that even if they give a similar definition of personal data, the OECD Guidelines provide clarification of the notion in the Explanatory Memorandum which removes the identifiability of the person concerned. Thus, it is said: "In principle, personal data convey information which by direct (e.g. civil registration number) or indiect linkages (e.g. an address) may be connected to a particular physical person" (emphasis added).

Similarly, Directive 2002/58 on privacy and electronic communications provides a definition of traffic and location data (see below) which in both cases avoids mentionning a link to an identified or identifiable individual. By applying these definitions, it suffices that a link be made with a terminal, an object, and through that to a person, the owner of the terminal, even if not identified or characterised, for Directive 2002/58 to apply.

2.1.3. Biological and biometric data

The European Court of Human Rights noted that fingerprints, DNA and cell samples all constitute, "personal data within the meaning of the Council of Europe 1981 Convention for the protection of individuals with regard to automatic processing of personal data". This position is not obvious. Blood or buccal samples would therefore be personal data? One might rather think that a cell sample contains data without being data itself.

It would be appropriate to clarify the notion of personal data in the presence of biological and biometric data.

2.1.4. Traffic and location data: a special system?

Should we understand traffic and location data as personal data requiring specific regulations and therefore as needing to be defined in the list in Article 2?

This data is defined by EU Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as follows:

• "'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
• '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".

The special status of location and traffic data can be explained by the hazardous nature of systematic processing of such data revealing travel, the usual entourage, consumption and life patterns. In addition, users of electronic communications services, except in the case of value added services, are a position of relative weakness, since network implies the generation, storage and transmission of much technical data whose meaning and potential use are beyond them and which are not easily traced (the opaqueness of how networks operate).

As an illustration of issues related to geolocation data, the OECD provides the following example: "A mobile operator uses a Global Positioning System "GPS" or triangulation (from signals generated from the devise) to locate mobile users. The company sells location and subscriber information to marketing companies for use in sending tailered advertisments or notices to the mobile subscriber. The mobile subscriber has not understood nor has she authorised transfer of such personal information. She might be charged for the notices (e.g. text, messages about neerby sales, or Internet time for pop-up messages"). She is disturbed by the tracking and concerned that the information could be picked up (stolen or bought) by criminals".
It is also possible to locate an individual by following traces they leave, for example traces related to the use of a credit card or public transport electronic tickets. These traces are nevertheless not included as location data in the sense used herein.
However, it is indeed location data that is used to provide tracking services of registrants (groups of friends or strangers interested in meeting people who are geographically close), which have multiplied like Find a friend, requiring the continuous positioning of registrants.

In view of the issues of location data, Directive 2002/58 a priori limits the processing of such data, with one exception: with consent of the person concerned duly informed and revocable at any time.

The OECD considers that it would make sense that companies "*provide consumers with clear disclosures about any location information that is being collected and the intented use of such information*", as they, "provide consumers with the opportunity to limit the sharing of data with third parties (except in emergency situations), and to revise their decisions about whom such data can be shared with. "
In the United States, the possibility for an operator to share with third parties geolocation information relating to subscribers is limited by laws relating to the use of proprietary network information concerning the customer (Customer Proprietary Network Information or CPNI). Thus, Article 222 of the Federal Communications Act prohibits the disclosure or use of location information from wireless devices, obtained by an operator through its provision of telecommunications services, without the express prior consent of the subscriber. We can only dispense with the consent of the subscriber in specific emergency situations (to be able to answer an emergency call from a subscriber). In addition, the CAN-SPAM Act (Controlling the Assault of Non-Sollicited Pornography and Marketing) prohibits the sending of mobile service commercial messages directly to wireless devices via the Internet without the express prior authorisation of the recipient.

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

The definition of processing does not cover data collection. This basic operation is expressly excluded from the definition of processing in the explanatory report (§ 31). Yet it is important for collection to come under the protection provisions. Admittedly, Article 5 stipulates that data must be obtained fairly. Furthermore, when information is gathered from the Web or through an Internet protocol, it is always stored – at the very least in the computer's RAM. Since data storage itself constitutes processing, data processing here occurs through the mere fact of collection.

Is this deliberate omission therefore actually a defect?

It should be pointed out that the European Court of Human Rights has expressly included data collection, separately from storage, among operations interfering with privacy. Thus it noted in its *Antunes Rocha* judgment that "the collecting, storing and possible release of information relating to an individual's "private life" come within the scope of Article 8 § 1 of the Convention (see the *Leander v. Sweden* judgment of 26 March 1987, Series A no. 116, p. 22, § 48, and *Rotaru v. Romania* [GC], no. 28341/95, § 43, ECHR 2000-V). Even public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities" (*Rotaru*, ibid.) and where "the authorities' decision to gather information about the applicant constituted interference with her 'private life' within the meaning of Article 8, irrespective of how the information was gathered."[3]

Should other operations be added to the list used to define automatic processing? What about data release, matching or interlinking?

As for the concept of "automated data file", what it represents is different from what is understood by "filing system" in Directive 95/46. The "automated data file" of Convention 108 means "any set of data undergoing automatic processing", whereas "filing system" in the Directive covers "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis". For the Directive, data have to be structured if they are to be considered a filing system. This condition is completely absent from the Convention's definition.

[3] ECtHR, *Antunes Rocha v. Portugal*, judgment of 31 May 2005, Application No. 64330/01, § 65.

Moreover, the Directive's concept of a filing system applies in an entirely non-technical context, unlike the Convention's concept of an automated data file.

The use of two similar terms differing in scope in two texts both to be used as a benchmark by a group of states is likely to create confusion and is definitely undesirable.

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

Article 2d of Convention 108 defines the controller of the file as "*the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them".*

By "controller of the file", Convention 108 "*means only the person or body ultimately responsible for the file, not persons who carry out the operations according to the instructions given by the controller of the file".*[4]

This definition of "controller of the file" ought to be reviewed.

It appears from this definition that Convention 108 considers the "controller of the file" to have a decision-making role at several levels: the controller must decide, on the one hand, the purpose of the file that he or she "creates" and, on the other, the data that will go into it and the operations to be applied to them. The emphasis is therefore on the controller's end role.

It seems, however, that this view does not actually reflect today's environment, since nowadays the role of "controller of the file" no longer attaches to just the file being processed but covers the entire processing procedure, which has become the main element. It would therefore seem logical to shift the concept of "controller of the file" towards just "controller". As the Article 29 Data Protection Working Party has pointed out, moving from the concept of "file" to the concept of "processing" makes it possible to shift from a "*static definition linked to a file to a dynamic definition linked to the processing activity*".[5]

Such a change would also make it easier to include the principle that the controller is responsible for the entire data-processing sequence; this would offer greater protection to the data subject, since the latter would have a single contact who would have control over data from collection until destruction, including anonymisation.

Moreover, practice has shown that in some circumstances the "controller of the file" may in fact be two or even three people, a situation for which Convention 108 makes no allowance in its present form. Cloud computing and e-health platforms are two cases in point. It would perhaps be helpful to assume, as Directive 95/46 does, that two or more people will be working together, even if this inevitably raises the question of the law applicable (see below).

It is next necessary to **clarify the criterion used in the current text of the Convention:** "competent […] to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them" (Article 2d). This clarification might be done in the spirit of the Convention's explanatory report, in which it is specified that the Convention "means only the person or body ultimately responsible for the file, not persons who carry out the operations

4 Convention 108, explanatory report, § 32.

5 Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, p. 12.

according to the instructions given by the controller of the file".[6] The criterion of "ultimately responsible for the file" is undoubtedly a good one, since it coincides with what has emerged in practice, namely the desire for the controller to be the person actually in control of the data processing and with the real power to take decisions about that processing.

The Madrid Resolution clearly opted for a single criterion for determining the person with the power to take decisions about data processing. It states that "responsible person" means "any natural person or organization, public or private which, alone or jointly with others, decides on the processing" (Article 2d).

The APEC Privacy Framework also uses a single criterion to determine the reference person for processing. It is in fact the criterion of control mentioned above. By "personal information controller" the Privacy Framework means "a person or organization who controls the collection, holding, processing or use of personal information" (Part II, Definitions, § 10).

This clarification would counter the criticism aimed at Convention 108 in the context of Directive 95/46 because of the existence of two parallel criteria. Using more than one criterion to determine the controller could evidently lead to more than one person being identified as such, and therefore to problems arising from concurrent application of different national laws if the criterion for the law applicable relates to the controller and to his or her establishment (as is the case in Directive 95/46).[7] Yet in the definition adopted in the 1981 version of Convention 108 we find a threefold criterion, which is supposed to reflect the way in which responsibility for the file is exercised: it covers power to decide on the purpose of the automated data file, the categories of data and the operations to be applied.

Subsequently **we may consider the expediency of including in the Convention additional concepts to cover traditional or new players in this field.**

Such players would primarily be the **processors**, a concept which denotes the persons, in the broad sense, who work under the instructions of a controller (or controller of the file) to perform tasks that the latter is unable to carry out, such as security tasks. The processor is therefore a person external to the controller of the file, in charge of delegated (usually technical) aspects of data processing. Processors play a leading part in the cloud computing context, for example.

Directive 95/46 defines a processor as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (Article 2e).

The Madrid Resolution, for its part, states that "'Processing service provider' means any natural person or organization, other than the responsible person that carries out processing of personal data on behalf of such responsible person" (Article 2e).

Where it does exist, this concept is not unproblematic to apply, since it is not always easy to distinguish between the concepts of controller (or controller of the file) and processor. This is particularly true in the case of a complex organisation such as a multinational or consortium.

Among the new players are **network operators**, including Internet access providers.[8] They are the necessary interface between the network user as data subject and the many Internet players who may

---

6 Explanatory report, § 32.

7 For criticism of this sort, see D. Korff, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Working Paper No. 2, 20 January 2010, pp. 60 ff.

8 See Y. Poullet, "Pour une troisième génération de réglementation de protection des données", in *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain – Challenges of Privacy and*

process the data generated, consciously or unconsciously, by network use. They could have certain obligations, such as providing notification of risks associated with network use, guaranteeing the security of their services, allowing restrictions on calling-line identification, etc.

Technical providers (including browser providers) also play a part in the new landscape. They could be made subject to requirements regarding technical standards and made accountable for compliance with these standards (see "privacy by design" below).

3. Protection principles

3.1. ARTICLE 5: QUALITY OF DATA – INAPPROPRIATE HEADING

Article 5 of the Convention, headed "Quality of data", is a key provision containing the gist of the protection principles. The article's heading is definitely inappropriate, since its content covers more than just quality of data. Points c and d are the only points relating to the quality of data (which must be adequate, relevant and not excessive in relation to their purposes, as well as accurate and up to date). The rules concerning fair and lawful collection (Art. 5a) and the purpose principle (requiring use of data compatible with the purposes of storage, and a limited storage time – Art. 5b and e) cannot be regarded as data-quality requirements. Furthermore, the Convention's explanatory report clearly states: "The different provisions of this article aim at the fulfilment of two fundamental legal standards. On the one hand the information should be correct, relevant and not excessive in relation to its purpose. On the other hand its use (gathering, storage, dissemination) should likewise be correct."[9]

If the Convention is to be used as an international model for data protection rules, it is important to ensure that the wording is clear and meaningful; its educational purpose must not be overlooked.

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data contain the purpose specification principle and the use limitation principle in addition to the data quality principle, while the UN Guidelines for the Regulation of Computerised Personal Data Files[10] set out the principle of lawfulness and fairness, the principle of accuracy and the principle of purpose specification.

3.2. PROPORTIONALITY PRINCIPLE

The Convention contains no express formulation of the proportionality principle, according to which the infringement of the data subject's interests cannot be disproportionate to the controller's interest in processing the data. The only specific expression of this principle is the requirement that personal data shall be "not excessive" – data which, even if relevant, cannot be processed because this would have an excessive effect on the data subject in relation to the controller's interest in processing them. The obligation to restrict data-gathering to adequate and relevant data may also be seen as an expression of the proportionality principle, inasmuch as this requirement is designed to reduce interference to what is

---

Data Protection Law, Perspectives of European and North American Law, M.V. Perez-Asinari and P. Palazzi (eds), Cahiers du CRID, No. 31, Brussels, Bruylant, 2008, p. 54.

9 Explanatory report, op. cit., § 40.

10 UN General Assembly, Resolution 45/95 of 14 December 1990.

strictly necessary. The European Data Protection Supervisor said as much in one of his opinions, in which he stressed the importance of striking an appropriate balance between the fundamental rights of the data subject and the interests of the various players involved, implying that the amount of personal data processed should be as small as possible.

Legal theory holds that **the requirement of "legitimate" purposes laid down in Article 5b of the Convention coincides with the proportionality requirement**. To be legitimate, a purpose cannot cause injury greater than the benefit from the processing.

Canada's Personal Information Protection and Electronic Documents Act contains an interesting formulation regarding acceptable processing purposes. Under section 5.3 any private organisation "may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". Conflicting interests are therefore weighed for a notional individual rather than an individual in a specific situation, since it is obvious that, when considering acceptable purposes, a reasonable person will weigh the arguments for and against processing and the implications that this processing might have for his or her situation and interests. It should be pointed out that, contrary to the Canadian example, the balance of interests that must be used to determine proportionality should not be limited to a personal standpoint but must also encompass the bigger picture, including the interests of society as a whole.

It would probably be wise, and at the very least instructive, to indicate clearly in the wording of the Convention the requirement for compliance with the proportionality principle, since it is now crucial to include this obligation, which can serve as a defence against the risks inherent in some technological developments (such as the unsuspected processing that abounds on the Internet) and against the (unreasonably?) widespread use of data subjects' consent for processing their data. While the existence of consent implies that processing is legitimate, weighing conflicting interests and determining a balance offers a welcome safeguard, given the flaws too often attaching to consent (data subject inadequately informed, consent inferred from failure to change default settings, etc).

The proportionality requirement should not be limited to processing purposes but also apply to every operation carried out on the data.

With regard to fingerprint and DNA information, the European Court of Human Rights has called for careful "balancing [of] the potential benefits of the extensive use of such techniques against important private-life interests".[11]

From its very first judgment in this field, the Court of Justice of the European Union established that Article 8 ECHR had to be construed in the light of Directive 95/46, which meant ascertaining whether, in the case of data processing, it complied with the proportionality principle contained in paragraph 2 of the Directive.[12]

---

11 ECtHR (GC), *S. and Marper v. the United Kingdom*, 4 December 2008, Applications. Nos 30562/04 and 30566/04, § 112.

12 CJEC judgment of 20 May 2003 (Österreichischer Rundfunk and others), C-465/00, C-138/01 and C-139/01: "So, for the purpose of applying Directive 95/46, […] it must be ascertained, first, whether legislation such as that at issue in the main proceedings provides for an interference with private life, and if so, whether that interference is justified from the point of view of Article 8 of the Convention" (§ 72); the Court stated that it should be determined whether the Austrian provision at issue was "consistent with Article 8 of the Convention, as regards its required proportionality to the aims pursued" (§ 80). "The interest of the Republic of Austria in ensuring the best use of public funds […] must be balanced against the seriousness of the interference with the right of the persons concerned to respect for their private life" (§ 84).

3.3. CONSENT AND LEGIMITATE BASES FOR PROCESSING

3.3.1. Consent

Convention 108 makes no official provision for consent by the data subject. Unlike Article 8 of both Directive 95/46 and the Charter of Fundamental Rights of the European Union, and unlike the Madrid Resolution, it does not enshrine consent as the legitimate basis for data processing.

Should this be considered a defect at a time when systematic use of consent as the basis of legitimacy for some types of processing occurring in connection with the data subject's use of Web 2.0 and other services is coming under criticism?[13]

The form and circumstances of consent are also a source of considerable concern: circumstances such as failure to object to conditions of data use offered by the service provider on a subsidiary web page, failure to remove the tick from preticked boxes and failure to change default settings are argued to equate to consent.

The opacity of networks, the fact that many data processing operations escape data subjects' notice and the fact that many people fail to realise the true implications of processing are cause for concern with regard to implied consent.

Inasmuch as modern networks are interactive, it is easier to claim consent as the legitimate basis for processing rather than other more traditional grounds such as balance of interests.

This therefore leads some people to hold that consent in itself is sufficient to justify processing. It should here be recalled that the Platform for Privacy Preferences (P3P) developed by the World Wide Web Consortium (W3C) was also based on an Internet user's being able to negotiate with a service provider that did not meet his or her privacy preferences and arrive at an agreement that would serve as a legitimate basis for the processing in question.[14] Although such negotiation has never been used on a large scale – through electronic agents, for example – P3P is indicative of the industry's determination to be able to negotiate with the data subject the use that can be made of his or her data. Privacy protection might thus, to some extent, be negotiated.[15]

However, protection of privacy is not a purely private matter but brings into play social considerations and requires the public authorities to be able to take action and exercise a degree of supervision.[16]

---

13 Article 29 Data Protection Working Party and Working Party on Police and Justice, WP 168, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adopted on 1 December 2009, §§ 65-68.

14 In addition to the opinion issued by the Article 29 Data Protection Working Party (*Opinion 1/98 on the Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp11_en.pdf), see J. Catlett, "Technical Standards and Privacy: An Open Letter to P3P Developers".

15 On contractualisation of data processing through use of technology, see P.M. Schwartz, "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices", *Wisconsin Law Review*, 2000, pp. 749-788 and M. Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)", *Stan. Tech. L. Rev*., 2001, 1, available at: http://stlr.stanford.edu/pdf/rotenberg-fair-info-practices.pdf.

16 See Schwartz, *ibid*.

3.3.2. Other legitimate grounds for data processing

The Convention does not specify in which cases data processing can be deemed legitimate. It confines itself to requiring its purposes to be legitimate but does not clarify in which cases the processing itself is recognised as legitimate. The drafters of Directive 95/46 anticipated cases of processing that would be admissible because legitimate. They compiled a list of these cases in Article 7 of the Directive in order to make life easier for users of personal data and offer them a measure of legal certainty. These are cases in which the proportionality rule is, in principle, notionally respected. It should still be ascertained whether conflicting interests have been balanced in reality, under the "legitimate purpose" requirement contained in Article 6b of the Directive (the equivalent of Article 5b of Convention 108).

Should the Convention include a list of cases in which data processing is deemed legitimate?

3.4. "INCOMPATIBLE" PROCESSING

The **"compatibility"** principle requires any use of data to be compatible with the purpose for which they were stored. There is a consensus that this means that what is done with the data should not run counter to the reasonable expectations of the data subject.

The APEC Privacy Framework offers the following clarification of compatible use: "The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for 'compatible or related purposes' would extend, for example, to matters such as the creation and use of a centralised database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an organisation for the purpose of granting credit for the subsequent purpose of collecting debt owed to that organisation."[17]

The acceleration of technological progress and the infinite potential for new types of processing offered by the software and data available on the Internet vindicate the need to consider regulating subsequent use and processing and their compatibility with the initial purposes of storage, and consider how to enforce the prohibition of incompatible processing.

Thus RFID technology, which was initially seen by consumer goods companies as a means of combating shoplifting, has become a powerful tool for analysing consumer behaviour, profiles, etc. A science writer's uploading of his or her curriculum vitae and publications to publicise his or her work can be used to classify that person politically or philosophically. Publication of court decisions in huge databases has an academic purpose and helps to make the law better known, but the possibility of searching for names of parties and types of case could be used to create blacklists (for example, a list of employees who have brought proceedings against their employers or been dismissed by them).

Any proposed regulation must take account of the value of subsequent types of processing.[18] Undoubtedly, coding or even anonymisation of data should be obligatory in so far as possible (data minimisation principle, see below), or consent should be requested. Failing this, it should be accepted that the controller of a file who wishes to carry out subsequent processing must be required to give

[17] Principle IV: Uses of Personal Information, § 19.

[18] Thus a health-care database, having initially been used for therapeutic purposes, may subsequently be used for the purposes of scientific research; or a bank may offer its customers a new service based on better use of the data relating to them.

detailed reasons for its legitimacy in terms of the balance of interests, and must inform the data subjects, collectively if not individually.

The rules laid down by the APEC Privacy Framework for subsequent uses of data incompatible with the purposes for which they were stored are as follows: incompatible use is normally out of the question except in cases where there is consent by the individual whose personal information is collected, when necessary to provide a service or product requested by the individual, and in cases covered by a law or any other legal instrument.[19]

The Madrid Resolution, for its part, considers "unambiguous consent" to be the only case in which data can be processed in a way incompatible with the purposes for which they were collected.[20]

As for technical solutions, it is possible – through search engines, for example – to provide users with the means of defining for themselves what they take to be "compatible" purposes. Thus "no robot" tags on web pages prevent their being recognised by search engines. Another example of a technical solution is when information brokers offer their services to select possible uses of Internet users' data for marketing purposes, etc.

3.5. DATA MINIMISATION PRINCIPLE

Through its requirement to restrict data processing solely to data that are adequate, relevant and not excessive, Convention 108 limits the gathering of personal data. This requirement can be seen as one facet of the data minimisation principle. But the principle goes further, since it suggests that, whenever possible, personal data collection be minimised (i.e. kept to the strict minimum) or eliminated.

It is mainly through anonymisation or pseudonymisation and through privacy-enhancing technologies (PETs) that this minimisation principle is meant to be applied. But, leaving aside the proven limitations of such technology,[21] it is possible to honour the principle very effectively by means of relatively low-tech solutions, such as requiring the default settings of various applications to strengthen, rather than weaken, privacy protection with regard to the amount of personal data processed. This may mean that, by default, a browser will reduce as far as is possible the quantity of information sent to websites after an Internet user's visit, or a social network will not allow the data that it holds to be viewed by everybody.

All national data-protection authorities of EU member states have called for this aspect of the minimisation principle to be henceforth enshrined in legislation,[22] as has the European Data Protection

---

19 Principle IV: Uses of Personal Information, § 19.

20 Article 7, § 2.

21 "Supplementary and alternative means to enhance data protection, including technical means such as encryption, anonymisation, identity management tools and other (supposedly) Privacy-Enhancing Technologies (PETs), are still rather under-developed, often weak in their implementation and effect, and too often applied in a way that makes them ineffective. Some are little more than fig-leaves. Others (like anonymisation) are increasingly defeated by technological advances. They also often do not tackle the issues at the right moment, in particular the design stage, or are user-unfriendly. In the new technical environment, renewed - and more critical - attention will have to be given to these measures." (*Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, Final Report, p. 17)

22 Article 29 Data Protection Working Party, WP 150, *Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications*, 15 May 2008; Article 29 Data Protection Working Party and Working Party on Police and Justice, WP 168, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adopted on 1 December 2009, § 53.

Supervisor.[23] The European Commission has taken steps to promote privacy-enhancing technologies enabling the processing of personal data to be reduced.[24]

The Madrid Resolution, for its part, links the proportionality principle to the requirement to keep to the minimum necessary the data processed.[25]

4. Sensitive data

Special categories of data afforded stricter protection are identified on the basis of the higher risk of injury to individuals entailed by their processing. The main risk is unlawful or arbitrary discrimination arising from these data. Moreover, the UN Guidelines for the Regulation of Computerised Personal Data Files[26] emphasise this risk, with a paragraph on sensitive data called "Principle of non-discrimination".[27] The Madrid Resolution also clearly indicates the connection between the special rules for sensitive data and the risk of unlawful discrimination. However, it also refers to the risk of such data affecting data subjects' private lives as well as, quite simply, the serious risk that these data might pose to the data subject in the event of misuse.[28]

The definition of sensitive data set out in Article 6 of the Convention is extremely broad, because they are described as "*revealing* racial origin, political opinions or religious or other beliefs" (authors' emphasis). This means that the category includes surnames unquestionably revealing racial origin, as well as any photographs of a person; an on-line purchase of a book about the Koran might reveal religious beliefs, etc. Yet it is unthinkable that names, photographs and certain purchases should systematically be treated as sensitive data covered by particularly strict protection rules. It is only when it is specifically the sensitive aspect of the data that is selected by the controller (persons of African, Arab, Jewish or Japanese origin on the basis of their surnames; Tutsis or Roma or Aborigines on the basis of their photos) that there is cause to apply protection rules, which are warranted mainly by the high risk of discrimination based on the data processed.

On the one hand, it is laudable to take account of data "revealing" sensitive characteristics of individuals, since this makes it possible to treat as sensitive those cases in which the data do not immediately appear to be so. Thus an Internet user's Google searches for websites offering travel to Rome, together with that user's purchasing of religious books, reading of a papal encyclical, etc, could be considered to reveal a religious opinion.

---

23 EDPS *Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, 18 March 2010. In particular, "the EDPS recommends the Commission to […] propose to include a general provision on PbD [privacy by design] in the legal framework for data protection" (§ 38).

24 Communication from the European Commission on promoting data protection by privacy-enhancing technologies, 2 May 2007, COM(2007)228 final.

25 Madrid Resolution, Article 8, § 2: "In particular, the responsible person should make reasonable efforts to limit the processed personal data to the minimum necessary."

26 United Nations General Assembly Resolution 45/95 of 14 December 1990.

27 Principle 5, Principle of non-discrimination: "Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled."

28 Before providing a non-exhaustive list of data held to be sensitive, Article 13, § 1, of the Madrid Resolution states: "The following personal data shall be deemed to be sensitive: a. Data which affect the data subject's most intimate sphere; or b. Data likely to give rise, in case of misuse, to: i) Unlawful or arbitrary discrimination; or ii) A serious risk to the data subject."

On the other hand, **specifically taking account of whatever reveals a sensitive characteristic means putting into this category of information an enormous quantity of data which in many cases are not being processed for their sensitive aspect**. This is excessive and could well make the concept of sensitive data meaningless in terms of practical application. One answer might be to revise the definition by introducing the following distinction: sensitive data will cover "personal data processed for the racial origin, political opinions or religious or other beliefs that they reveal".

It should be asked whether two additional special categories might pertinently be added to the list of sensitive data in the light of new risks arising from technological development:

- Identification numbers (whether or not associated with identity in the narrow sense) which can be used to link multiple data and databases and are becoming widespread in both the public and the private sectors;

- Biological and biometric data. The European Court of Human Rights has clearly stated why these data cause particular concern with regard to privacy protection. It has thus held[29] that, given the use to which cellular samples could conceivably be put in the future, the systematic retention of such material is sufficiently intrusive to constitute an interference with the right to respect for private life. Furthermore: "In addition to the highly personal nature of cellular samples, the Court notes that they contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his or her relatives."[30] As for DNA profiles, the Court considers them to contain substantial amounts of unique personal data which, even if objective and irrefutable, allows the authorities to go well beyond neutral identification (DNA profiles can be used for familial searching with a view to identifying a possible genetic relationship between individuals).[31] With regard to fingerprints (and this argument would probably hold for other physical identifiers such as irises, profiles, etc), the Court has also noted, "It is accepted […] that, because of the information they contain, the retention of cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints."[32] However, it has held that fingerprints contain unique information about the individual concerned and that their retention without the latter's consent could not be regarded as neutral or insignificant. Accordingly, retention of fingerprints may in itself give rise to important private-life concerns and therefore interfere with the right to respect for private life.

In a study for the Council of Europe in 1999, S. Simitis already considered that genetic data ought to be included in the list of sensitive data. He thus reported: "There is […] no better example for the need to update lists than genetic data. They were hardly noticed when the first lists were put together. By now, however, there can be no doubt that no other data provide such comprehensive information on the persons concerned. Never before were the risks of the processing of personal data therefore so evident. Irrespective of whether the opportunities to be employed, the chances to obtain health insurance, or the limits of a rapidly expanding commodification of the individuals are at stake, the accessibility of genetic

29 ECtHR, *Van der Velden v. the Netherlands*, decision of 7 December 2006, Application No. 29514/05.

30 ECtHR, *S. and Marper v. the United Kingdom*, op. cit., § 72.

31 Ibid., § 75.

32 Ibid, § 86

data determines the answers. No list of sensitive data can henceforth disregard genetic data without questioning its seriousness."[33]

5. Security

5.1. SECURITY OBLIGATIONS

Article 7 of the Convention considers security in a very narrow sense: basically data destruction and breach of confidentiality. The definition could usefully cover the three aspects of security in the broad sense (integrity, availability and confidentiality) and span the nine principles of the 1992 OECD Guidelines for the Security of Information Systems (accountability, awareness, ethics, multidisciplinarity, proportionality, integration, timeliness, reassessment and democracy).

Moreover, lack of network security and increasing opportunities for unlawful conduct make it necessary to compel electronic communications service providers to warn network users of the risks associated with using their service.

Lastly, the importance of self-regulation should be underlined: development of security standards; auditing methods; IS approval systems, etc. The organisational and technical security of information systems must become an integral part of data protection policy.

Security measures must not only prevent unauthorised access but also allow data subjects to check any access to data that has taken place, since it is only this information about who has accessed their data that enables data subjects to determine the effectiveness of security measures and exercise control over their own data. This was the gist of the judgment by the European Court of Human Rights in *I v. Finland*, where the Court found against Finland for having allowed a public hospital to introduce a data security system that stored records of only the five most recent data consultations, and which also deleted all access records once the data had been archived.[34]

The Court of Justice of the European Communities pointed out in its *Rijkeboer* judgment[35] that data protection means that the data subject may be certain that his or her personal data are disclosed to authorised recipients. In order to carry out the necessary checks, the data subject must have a right of access to information on the recipients or categories of recipient of personal data and to the content of the data disclosed not only in respect of the present but also in respect of the past. This entails an obligation to retain for a certain period of time information about the recipients of data and the specific data consulted or disclosed.

In its reasoning in the *I v. Finland* judgment, the European Court of Human Rights underlined that the confidentiality of certain data of particular importance to data subjects (such as medical data) therefore

---

33 S. Simitis, "Revisiting Sensitive Data" (1999), Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), Strasbourg, 24-26 November 1999.

34 "[…] the impugned health records system was such that it was not possible to retroactively clarify the use of patient records as it revealed only the five most recent consultations and that this information was deleted once the file had been returned to the archives. Therefore, the County Administrative Board could not determine whether information contained in the patient records of the applicant and her family had been given to or accessed by an unauthorised third person" (ECtHR, *I. v. Finland*, 17 July 2008, app. no. 20511/03, § 41).

35 CJEC, 7 May 2009 (Rijkeboer), Case C-553/07.

required stricter measures, since **the security requirement would vary according to the nature of the data, the circumstances surrounding their processing and the risks to which the latter might expose the data subjects**. Along the same lines, Directive 2002/58 concerning the protection of privacy in electronic communications stipulates, in Article 4 on data security: "[…] Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented."

The APEC Privacy Framework similarly indicates the possibility of varying the level of security required. Principle VII (Security Safeguards) states: "22. Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. *Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment*" (authors' emphasis). The Madrid Resolution has adopted similarly flexible security requirements: "[…] These measures depend on the existing risk, the possible consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out, and where appropriate the obligations contained in the applicable national legislation." (Article 20, § 1, second sentence).

5.2. CONFIDENTIALITY

Data confidentiality has traditionally been dealt with under the heading of security.

Since electronic communications now entail processing data (concerning the persons who are communicating), **the obligation to ensure data confidentiality converges with the requirement for confidentiality of communications**. These converging confidentiality requirements are explained by the fact that interactive network technology now allows the user to communicate with other network users for personal purposes.

The confidentiality requirement must cover both the content of communications and the accompanying technical, traffic and location data.[36] These data prove the existence of, or an attempt to establish, communications and indicate sender and recipient, date and time, volume of data sent, nature of any attached files, user's geographical position, etc.

However, there have to be limits to the confidentiality of communication data. The European Court of Human Rights has emphasised the need for legislators to provide a framework reconciling the confidentiality of Internet services with the prevention of disorder or crime and the protection of the rights and freedoms of others. In one case before the Court,[37] an advertisement of a sexual nature about a young boy was posted on an Internet dating site, but the Finnish legislation protecting confidentiality of communications that was in force at the time could not be used by the police and courts to require the Internet service provider to identify the person who had posted the advertisement. The Court found that there had been a violation of Article 8 ECHR inasmuch as the confidentiality requirement had been given precedence over the child's physical and moral welfare, and Finland had thus failed to protect the applicant's right to respect for his private life.

---

[36] See Directive 2002/58, Article 5, paragraph 1. See also ECtHR, *Copland v. the United Kingdom*, judgment of 3 April 2007, § 44.

[37] ECtHR, *K.U. v. Finland*, judgment of 2 December 2008.

5.3. SECURITY / DATA BREACHES

The Madrid Privacy Declaration, a civil society statement adopted on 3 November 2009 to establish "global privacy standards for a global world" urges countries to, amongst other things, "**ensure that individuals are promptly notified when their personal information is improperly disclosed or used in a manner inconsistent with its collection**".

It is thus necessary to notify data subjects if an unauthorised third party, such as a hacker, has accessed personal data by illegally hacking into a server. This requirement also covers situations in which personal data (on CD-ROMs, USB keys or other portable devices, for example) has been lost or inadvertently or maliciously disclosed by an authorised user in breach of the purpose-specification principle or his or her duty of confidentiality (such as a banking information file sent to tax authorities in a third country by a sacked employee in revenge, accidental posting on a website of a list of members of a political party, or a drug alert e-mail from a pharmaceutical company showing the names and addresses of everyone taking the drug).

In the data protection field, there are considerable advantages to this obligation to notify data or security breaches: "Notices of security breaches may help individuals take the necessary steps to mitigate any potential damage that results from the compromise. Furthermore, the obligation to send notices informing of security breaches will encourage companies to improve data security and enhance their accountability regarding the personal data for which they are responsible."[38]

Originating in the United States, where most states have adopted legislation in this field, this concern with privacy breaches is now echoed in EU legislation. Thus Directive 2002/58 on the protection of privacy in electronic communications has been amended by European Parliament and Council Directive 2009/136/EC of 25 November 2009 in order, amongst other things, to insert a special provision concerning "personal data breach".[39] Providers of publicly available electronic communications services are now required to notify subscribers and individuals of any breaches of their data.[40]

---

38 *Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, *OJEU*, 6 June 2009, C 128/28, § 10.

39 Personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community" (Article 2 (h) of amended Directive 2002/58).

40 Article 4, paragraph 3, of amended Directive 2002/58: "In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

The fact that the requirement to inform individuals of security breaches is limited to providers of publicly available electronic communications services (that is, telecommunications companies and providers of Internet access) has been criticised. Both the European Data Protection Supervisor[41] and the Article 29 Data Protection Working Party have stressed the need to include providers of information society services within the scope of the obligation to notify security breaches (the examples cited above show how relevant such inclusion is). The obligation should therefore ideally apply to on-line banks, on-line businesses, on-line providers of health-care services, etc. Both consider that "broadening the scope to include information society services in general would increase their accountability, and would contribute to raising awareness among the public. This would undoubtedly contribute to mitigating security risks."[42]

Limiting security breach notification to subscribers has similarly been criticised, since every individual whose data have been compromised by a security breach ought to be notified of the fact.

The Madrid Resolution includes in its "Security measures" (Article 20) the duty of those involved in any stage of the processing to inform data subjects of any security breach that could significantly affect the latter's pecuniary or non-pecuniary rights. Data subjects must also be notified of the measures taken to resolve the breach.

When adopting its *Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce,*[43] the OECD judged that, with the growth of mobile commerce, there would be a need for further protection measures in addition to those contained in the 1980 OECD Privacy Guidelines and the 2002 OECD Guidelines for the Security of Information Systems and Networks. Among these measures was an invitation to mobile operators to implement data security policies and measures to prevent unauthorised transactions and data breaches and to provide consumers with timely and effective methods of redress when their data were compromised and/or they suffered financial loss.

THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS[44] ESTABLISHED A **RESPONSE PRINCIPLE**, ACCORDING TO WHICH "PARTICIPANTS SHOULD ACT IN A TIMELY AND CO-OPERATIVE MANNER TO PREVENT, DETECT AND RESPOND TO SECURITY INCIDENTS". THE INTERCONNECTIVITY OF INFORMATION SYSTEMS AND NETWORKS INCREASES THE POTENTIAL FOR RAPID AND WIDESPREAD DAMAGE FOLLOWING A SECURITY INCIDENT. IT IS THIS INCREASED RISK THAT THE *RESPONSE PRINCIPLE* IS DESIGNED TO ADDRESS.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach."

41 *Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC*, op. cit., §§ 22 ff.

42 Article 29 Data Protection Working Party, WP 150, *Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)*, 15 May 2008.

43 OECD, Seoul, June 2008.

44 *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, 25 July 2002.

6. ADDITIONAL SAFEGUARDS FOR THE DATA SUBJECT

6.1. OBLIGATION OF TRANSPARENCY/INFORMATION

Article 8 of the Convention provides "additional safeguards for the data subject". These safeguards are required to correspond to subjective rights in national legislation. The Convention does not set down any specific obligation on controllers of the file except that of satisfying and giving effect to the rights of data subjects.

However, the protection system no longer settles for safeguards based mainly on the initiative of the data subject alone. Given the particularly opaque environment of present-day information systems, it is vital to place obligations with regard to active transparency on the persons responsible for processing. The data subject cannot inquire into, or inform him or herself about, processing whose existence he or she does not even suspect. How many "standard" data subjects would imagine that the words entered into a search engine may be recorded for months and linked to an identifying pointer?[45] Or that they are filmed by cameras which are miniaturised and powerful enough to be located some distance away? Or that their company keeps records of every use of magnetic keys/cards in order to follow their movements? Or that the security gate they walk through reads the RFID tag in their passport? Today, unfortunately, there is any number of examples of such situations in which data subjects have no idea that their data are being processed, unless someone tells them. **So it is important that a clear obligation be placed on the persons engaged in such processing to inform the persons whose data are processed.**[46]

Indeed, the Madrid Declaration expressly sets out, in the universal protection regime which it aims to establish, a series of obligations to be placed on persons collecting data. Civil society, via the signatories to the declaration, "(1) reaffirm[s] support for a global framework of Fair Information Practices *that places obligations on those who collect and process personal information* and gives rights to those whose personal information is collected"[47].

The APEC Privacy Framework, the most recent legal instrument to be adopted at international/regional level, lays such an obligation to inform – the *Principle of Notice*[48] – on *personal information controllers.* The commentary on this principle offers the following clarification: "15-17. The Notice Principle is directed towards ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used. By providing notice, personal information controllers may enable an individual to make a more informed decision about interacting with the organization. One common

45 See the observations above on the concept of personal data.

46 It might be considered that the obligation to inform is inherent in Article 8a, states being free to decide what form to give to the obligation contained in this clause, which requires that "Any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file". The explanatory report observes: "There are States where the name of the controller of the file is listed in a public index. In other States which have no such publicity rule, the law will provide that the name of the controller of the file must be communicated to a person at his request" (§ 51). Apart from the fact that a systematic obligation to inform (as distinct from an entry in a public register) is not mentioned in the examples of implementation of the principle set down in sub-paragraph a, the statement of this principle is decidedly not sufficient to indicate the duty of spontaneous transparency which is indispensable in the technical reality of today.

47 Madrid Privacy Declaration, cited above (authors' emphasis).

48 Principle II Notice.

method of compliance with this Principle is for personal information controllers to post notices on their Web sites. In other situations, placement of notices on intranet sites or in employee handbooks, for example, may be appropriate."

The Madrid Resolution, for its part, lays down an "openness principle" (Article 10). It places a highly detailed information obligation on the person responsible for processing.

The aim here is to improve the situation of data subjects and so offer them the possibility of "informational self-determination" at a time when such control is tending to diminish by reason of the twofold opacity of the way in which terminals and networks operate. Recognition of new rights is an essential corollary of information system users' loss of control over their information environment.

6.2. RIGHT OF ACCESS

The right of access afforded by the Convention could be enhanced in several ways.

First of all, **over and above communication of the data proper, access for data subjects could also cover access to the data source.**[49] This information is in fact crucial, because it is often the data source that puzzles and worries the data subjects (how did they obtain this information, who passed it on to them?). Moreover, knowing the data source makes it possible to check the lawfulness of its communication or collection and perhaps to take proceedings against the first holder of the data (enabling the leak to be stopped if he or she unlawfully divulges the data in question). Finally, where problems arise in connection with the quality of the data and the need for rectification, it is then possible to get it corrected at source and so avoid the subsequent propagation of errors.

The right of access could also be enhanced by **the right of every person to access the logic** underpinning any automated processing of data relating to him or her (see point 6.5 below).

Next, there should be a guarantee that the data subject is able to enjoy the same technical facilities in exercising his or her rights (right of access, but also right of rectification and right to object) as those enjoyed by the persons responsible for processing[50]. So he or she must be enabled to contact the person responsible for processing via the network if the processing takes place on the Internet. This is the **right to reciprocal advantages**, requiring anyone using technology to make available to the Internet user electronic means of upholding his or her interests or rights where these may be damaged by the use of these electronic means.

Similarly, in order to facilitate exercise of the right of access (as well as other rights), it should be **permissible to re-use the identification data** used by the person responsible for processing (even where, in some cases, no name is given) in order to exercise one's right, rather than requiring identification in the form of proof of identity. Identity proved in this way will in many cases not correspond to the

---

[49] Such a right of access is guaranteed by Article 12 of Directive 95/46: "Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: […] communication to him in an intelligible form of the data undergoing processing and of any available information as to their source […]". It is also provided for in the Madrid Resolution (Article 16 § 1).

[50] Y. Poullet, "Pour une troisième génération de réglementation de protection des données", in *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law, Perspectives of European and North American Law*, M.V. Perez-Asinari and P. Palazzi (eds), Cahiers du CRID, No. 31, Brussels, Bruylant, 2008, pp. 57 ff.

identifying data kept on record (a cookie, for example, which need not go so far as to indicate the civil identity of the data subject, but still establishes the individual's identity to the necessary extent).

6.3. RIGHT TO OBJECT

Like other international instruments (OECD Guidelines, United Nations Guiding Principles[51] and APEC Privacy Framework), **the Convention does not provide a right to object for the data subject.** However, as far back as 1995 European Directive 95/46 included this right in the list of subjective rights intended to enable individuals to exercise control over what happens to their data, i.e. to implement their informational self-determination. Directive 2002/58 on privacy and electronic communications also took up this right in different forms (see below). Finally, the Madrid Resolution likewise includes this right in its list of rights of the data subject.

This right is justified where the data processing is not based on the consent of the data subjects. Not having been able to express their views at the start of processing, the latter can resort to this right to put their arguments to the controller of the file and so persuade him or her to desist from processing their data. It is a particularly important right in cases where the person responsible has him or herself weighed up the interests at stake *beforehand* and concluded that the result was a balanced one and that he or she could legitimately process the data. Thanks to the right to object, the data subject has an opportunity to challenge the outcome of that weighing up, at least in his or her own case.

Clearly, in the present-day technological context, with a massive growth in the processing of data without the knowledge or consent of the data subjects, it is important to restore a balance between the persons involved by securing the right of data subjects to have their say and refuse the recording and use of their data when they become aware of them. It may also be the case that the persons in question were indeed informed of the processing envisaged, but took some time to appreciate the full extent of what was being done with their data or the possible implications of that processing for other interests. In such cases also, the right to object offers an opportune solution.

This right is recognised by the Article 29 Working Party as a core element of data protection and is accordingly included in the list of protection principles which must feature in any system of data protection claiming to be "adequate". Thus, working paper No. 12 on defining the conditions for recognising the adequacy of protection systems in third-party states outside the European Union observes, in the list of minimum conditions for recognition of an adequate level of protection: "In certain situations he/she should also be able to object to the processing of the data relating to him/her"[52].

The right to object is especially relevant in the field of direct marketing, where massive recourse is had to the balance of interests, in order to justify data processing, rather than to the prior consent of the data subjects. Moreover, this is a field pinpointed by the Article 29 Working Party as needing recognition of the right to object: "Where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage"[53]. Where marketing takes forms that are particularly intrusive or costly to the consumers targeted (via automated

---

[51] A form of right to object might be seen in the "*right…to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries*", this right being linked to the *Principle of interested-person access* (Guidelines for the Regulation of Computerised Personal Data Files, already cited).

[52] Article 29 Working Party, WP 12, Transfers of personal data to third countries : applying Articles 25 and 26 of the EU data protection directive, 24 July 1998.

[53] Article 29 Working Party, ibid.

calling[54], fax or electronic mail), it is no longer a right to object (opt-out) that should be guaranteed, but the obtaining of consent from the consumers targeted (opt-in)[55].

The economic model according to which the Internet operates raises questions about the place to be accorded to the right to object and the impact it may have. The basis of that model is that most of the services offered are seemingly free of charge, being financed by targeted advertising fed by huge quantities of personal data collected either fairly or in a more opaque manner. The right to object could enable an individual to reject this model which leads to the processing, cross-linking and interconnection of his or her data and to prefer a model which is charged for, restoring his or her control over the information he or she communicates.

Similarly, but outside an economic model based on the intensive processing of data for direct marketing purposes, objection to the processing of one's data might also force the designer of a service imposing personal data processing on the user to develop a version of his or her service which operates without processing personal data. For example, think of electronic public transport tickets. Anyone not wishing to leave a trace of his or her every movement in an operator's hands should be able to object to this system, which would place an obligation on the operator in question to implement a "non-identifying" version of the service. That version would have to be accessible on conditions which do not strip it of all interest to potential users. The example of the electronic Paris metro ticket illustrates this hypothesis where an "identifying" service and a "non-identifying" service are on offer side-by-side[56].

In a different field from direct marketing or market research, the rule laid down in Directive 2002/58 which allows the user of a calling or connected line to prevent presentation of identification of the calling or connected line is a further illustration of the objection principle.[57]

Until a short time ago this text contained another manifestation of the right to object. According to Article 5 § 3 of the directive, everyone had to be clearly informed of any remote use of his or her terminal (via cookies or spyware, for example), and to be able to *object* easily and free of charge. Today, data storage or access to data already stored in a user's terminal are permitted only on condition that the user *has given his or her agreement*, after being duly informed, in particular about the end-purpose of the processing.

Furthermore, enabling the purchaser to deactivate RFID tags attached to objects he or she has acquired[58] is another expression of the objection principle.

The right to object would also find application to cases in which traffic or location data are processed[59].

---

54 Automated calling and communication systems without human intervention.

55 See Directive 2002/58, Privacy and electronic communications, Article 13 on unsolicited communications for purposes of direct marketing.

56 See 6.7 below (The right to anonymity).

57 Article 8 of Directive 2002/58: "Presentation and restriction of calling and connected line identification: 1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis. […] 4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user".

58 See 6.6 below (The right not to be tracked).

6.4 THE RIGHT NOT TO BE SUBJECTED TO AN INDIVIDUAL DECISION TAKEN BY A MACHINE

It is not desirable for a decision affecting an individual to be dependent only on the conclusions of a machine[60]. However, technology today is more and more often used in such a way as to rely on a computer and on the algorithms it applies in deciding what is to be done with an individual (whether or not he or she is to be considered as a tax evader, a marketing target, a potential terrorist passenger, etc). Thus, "the new technologies bring further, newer threats: Increased, and increasingly automated analyses of ever-increasing, and ever-more-easily-accessible data carry the risk of individuals becoming mere objects, treated (and even discriminated against) on the basis of computer-generated 'profiles', probabilities and predictions, with little or no possibility to counter the underlying algorithms. Unless strong data protection is maintained, decisions with 'significant effect' (such as a decision to deny you a job, or to not even invite you for an interview; to be stopped at a border, and possibly denied entry into a country; to be subjected to intrusive surveillance, and possibly arrested, etc) will increasingly be taken 'because the computer said so' - without even the officials or staff carrying out the decision able to fully explain why"[61].

Following the example of Directive 95/46 (Article 15)[62] , **it should be prohibited for an individual decision significantly affecting a person to be taken on the sole basis of automated data processing designed to assess certain aspects of his or her personality.** Unless one prefers to opt for the approach taken by the Madrid Resolution, which does not set out this right as such but provides for it in the form of the right to object to decisions which produce legal effects based solely on automated processing of personal data (Article 18 § 3).

Such a prohibition should of course be subject to limitations or exceptions where this is warranted in view of the context and the risks in play. For example, it used to be common practice in the world of commerce to use automated assessments of consumer profiles in connection with contracts for granting loans or taking out insurance. Recourse to the technique of profiling now extends far beyond these limited commercial contexts and feeds on impressive quantities of data gleaned from every possible source, as explained above. A distinction should perhaps be drawn according to context.[63] Purely automatic processing is also used to decide success or failure in certain examinations (eg. the theoretical part of driving tests, competitive examinations for civil service posts). However, the exceptions regarded as justified should go hand in hand with measures to safeguard human dignity vis-à-vis machines, making provision at the very least for the data subject to state his or her views *effectively*.

6.5. THE RIGHT TO KNOW THE LOGIC UNDERPINNING ALL DATA PROCESSING

In the present-day technical context, there is a right which does not appear in the Convention but which is of great interest, especially in view of the exponential growth of the profiling phenomenon. **It is the**

---

59 See in particular Articles 6 and 9 of Directive 2002/58 and the OECD's "Policy guidance on emerging consumer protection and empowerment issues in mobile commerce", Seoul, June 2008, pp. 22-23.

60 Cf. the observations concerning human dignity, above.

61 LRDP Kantor Ltd in association with the Centre for Public Reform, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, Final report, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf January 2010, § 22.

62 See the commentary on this provision by L. Bygrave, "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law & Security Report*, 2001, volume 17, pp. 17–24.

63 See the draft recommendation on profiling.

right to know the logic which underpins any automated data processing.[64] This guarantee, secured in Directive 95/46, has a potential scope which prompted Marc Rotenberg of the EPIC (Electronic Privacy Information Center, Washington) to say: "There is a giant sleeping in the EU directive. That is the right to know the logic of a data processing".[65]

This right was highlighted in the draft recommendation on profiling. It is referred to in the introductory paragraphs: "17. […] considering that every person should know the logic involved in profiling; whereas this right should not affect the rights and freedoms of others, in particular, not adversely affect trade secrets or intellectual property or the copyright protecting the software;". Thus this proposed text establishes the right of access to this information (point 5.1.b of the appendix).

Alongside this right of access to the logic involved in processing, but with the same aim of enabling the data subjects to check the basis of decisions affecting them, involving processing of their data, it was suggested by Canadian Professor Pierre Trudel, a recognised authority in the field, that **in the specific context of networks, which permits greater interactivity and dialogue, the legal framework should in future make it obligatory for organisations to communicate to the persons concerned the data taken into account in an individual decision.**[66] That would make it possible to ensure the accuracy of the data; he argues that, when any personal data are used, the public bodies[67] must check the information which they have accessed with the person concerned. Where necessary to ensure data quality, the information must be made available so that the persons concerned can verify its content and, if appropriate, exercise their right of correction.[68] So what is advocated is a duty to make available spontaneously data which have been used in reaching a decision. From this standpoint, it is not the logic (the computer program or the reasoning and criteria) applied to the data which has to be communicated, but the data taken into consideration themselves.

6.6. THE RIGHT NOT TO BE TRACKED

As the Internet of Things evolved, a new right made its appearance in legal theory and in the official documents adopted by certain organisations; it could be seen as a new interpretation of the *right to be left* alone.[69] This is the *right not to be tracked.* It is a right that has arisen mainly in response to the exponential development of the use of RFID chips, and has also been referred to as the "right to silence of the chips". It "expresses the idea that individuals should be able to disconnect from their networked environment at any time".[70]

---

64 The European Directive, which secures this right in Article 12, adds; "at least in the case of [...] automated decisions".

65 Marc Rotenberg at the International Conference on Privacy and Data Protection "Re-inventing Data Protection?", Brussels, 12 and 13 October 2007.

66 P. Trudel, "Hypothèses sur l'évolution des concepts du droit de la protection des données personnelles dans l'Etat en réseau", in *Défis du droit à la protection de la vie privée*, *Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law*, *Perspectives of European and North American Law*, M.V. Perez-Asinari and P. Palazzi (eds), Cahiers du CRID, No. 31, Bruxelles, Bruylant, 2008, p. 547.

67 This idea was being discussed in the specific context of the state within a network, but could also be envisaged in the case of all those involved in networks (note added by ourselves).

68 P. Trudel, *op. cit.*, p. 547.

69 The first occasion on which *privacy* was defined gave rise to the famous expression, "*the right to be left (or let) alone"* (Warren & Brandeis, "The Right to Privacy", 4 Harv. L. Rev., 193 (1890).

70 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – The Internet of Things: an action plan for Europe, COM(2009) 278 final, 18.6.2009, Line of Action 3 – The 'silence of the chips'.

In its recommendation on the use of RFID tags, the European Commission recommends various approaches to the utilisation of RFID applications in a lawful, ethical and socially and politically acceptable way while ensuring the right to privacy and the protection of personal data. Point 11 of the Recommendation states: "Retailers should deactivate or remove at the point of sale tags used in their application unless consumers, after being informed of the policy referred to in point 7, give their consent to keep tags operational. Deactivation of the tags should be understood as any process that stops those interactions of a tag with its environment which do not require the active involvement of the consumer. Deactivation or removal of tags by the retailer should be done immediately and free-of-charge for the consumer. Consumers should be able to verify that the deactivation or removal is effective".[71]

The European Data Protection Supervisor recommends, with regard to the use of RFID tags in commercial practice, that an opt-in principle should be established so that all RFID tags attached to consumer products are deactivated by default at the point of sale.[72]

6.7. THE RIGHT TO ANONYMITY

It is symptomatic that many of the things one does on the Internet leave traces in the hands of various people. Unlike what happens in the real physical world, it is impossible to move along Internet highways, go into virtual shops, read the newspaper or react to a commercial advertisement, etc, without this being known about. This permanent transparency, which would probably not be tolerated in the real world, is bound to raise questions.

Many texts of a non-binding kind advocate the "right" of the citizen[73] to remain anonymous when making use of services offered via the new technologies. Recommendation No. R(99)5 of the Committee of Ministers of the Council of Europe [74] sets out the same principle: *"Anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy"*, and emphasises in this connection the value of the *"privacy-enhancing technologies"* available on the market.

The **concept of anonymity should doubtless be redefined**, and by the same token other terms such as "non-identifiability" should be preferred in so far as this concept of anonymity remains ambiguous. The aim very often is not absolute anonymity, but the functional "non-identifiability" of the author of a message vis-à-vis certain persons.[75]

---

71 Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009)3200 final, Official Journal 16.5.2009, L 122/47.

72 European Data Protection Supervisor, Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 18 March 2010, No. 56-70.

73 In this connection, 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 (eds), Cahiers du CRID, No. 13, Brussels, Bruylant, pp. 211 ff.

74 Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways; text available on the Council of Europe website. Similarly, Recommendation 3/97 of the Article 29 Working Party entitled" Anonymity on the Internet". Cf. also the opinion of the Belgian Privacy Commission on electronic commerce (Opinion no. 34/2000 of 22 November 2000, available on that Commission's website http://www.privacy.fgov.be), which rightly observes that there are ways of authenticating the sender of a message without necessarily obliging him to identify him or herself.

75 On this point, see J. Grijpink and C. Prins, "Digital Anonymity on the Internet, New Rules for Anonymous Electronic Transactions?", 17 *CL&SR*, 2001, p. 378 ff.

Anyone using modern means of communication should have the option of remaining non-identifiable, either by third parties involved in conveying the message or service providers in the communication chain, or by the person(s) to whom the message is addressed, and should be provided free of charge, or at least at an affordable cost, with the means of exercising that option.

However, the anonymity or functional "non-identifiability" required is not absolute. Against individuals' right to anonymity must be set the higher interest of the state, which may impose limitations where they constitute measures necessary to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences. The balance between legitimate crime control and data protection might be found in systems of "pseudo-identity" attributed to an individual by a specialist service provider through whom - but only in cases specified by law and in accordance with procedures laid down by law - the link might be established between the real identity of the user and his or her pseudonym.

The Madrid Declaration calls for further research into techniques which might be applied to ensuring anonymity. It recommends "comprehensive research into the adequacy of techniques that deidentify data to determine whether in practice such methods safeguard privacy and anonymity" (point 8).

Safeguarding the right of individuals to anonymity means not just ensuring that they are offered techniques of data "deidentification", so as to permit anonymous network navigation in particular. It also means securing to individuals the right to opt for an alternative to the services offered which does not impose user identification. This should apply, for example, in the case of public transport tickets. Some towns are changing over to magnetic ticketing systems for their underground railway and bus networks. Where such systems entail identification of season ticket holders or passengers purchasing tickets, they should allow for the possibility of persons who do not wish to leave traces of their every movement with the transport company to acquire an anonymous ticket, perhaps by purchasing it at a reasonable special price (if justified by the costs of providing this alternative).

7. Article 9 – Exceptions and restrictions

As was explained above concerning restrictions on the scope of the Convention, **a general exception should be added**, according to some authors, **in respect of the processing of personal data for "family/personal or domestic" purposes.** The reasoning is sound: it is not possible, in the name of data protection, to infringe the privacy of a person processing data on his or her own account. However, the scope of this exception must, as is shown by the *Linqvist* case decided by the ECJ (cited above), allow for the fact that private thoughts posted on a website unquestionably lie outside the private or domestic sphere of the persons concerned and are made accessible to an indeterminate and infinite number of people.

The relevance and scope of such an exception have assumed great importance with the development of Web 2.0 and the exponential use of the Web, with its blogs, social networks, Twitter, and individuals now supplying content themselves (often including personal data in the form of information, photographs or videos). The Internet of Things referred to earlier perfectly illustrates this mix of personal and family purposes and the use of a public mode of expression which runs counter to the "private" nature of the data shared. The consequence of this state of affairs is that it is not easy purely and simply to accept or reject the application of such an exception in the new technological environment.

"The overall problem is that the granting of a full exemption from data protection requirements to anyone who uploads materials to the Internet as a private individual would lead to easy circumvention of the rules and, in an age of user-generated content, would fundamentally undermine data protection (and privacy) itself; yet the full imposition of the law to all such individuals would seem excessive and, because of the sheer numbers, would be largely unenforceable. The question - the challenge - is then perhaps whether a middle way [can] be found?"[76]

Point 2 should provide for exceptions linked to the need to safeguard freedom of expression or opinion (principle of fair balance between data protection and/or freedom of expression). The wording of such an exception will have to be carefully weighed up, since the specific rules governing the press in many countries of the world, permitting partial or complete exceptions to the principles of data protection (in European states and Canada, for example), need to be reviewed in the Internet context. With the deployment of Web 2.0 has come a watering-down of the concept of press and a blurring of that of journalist, the publication of, and commentaries on, news and information of public interest no longer being the preserve of journalists and newspapers in this new environment.[77]

Point 3, concerning statistics and research, contemplates only the risks relating to the protection of individual data on the basis of research or statistics. But statistics and scientific research call for certain precautions, even when their subject is data which are anonymous or have been rendered anonymous, in so far as they introduce the possibility of applying the profiles thus created to individuals.

8. Responsibility

Convention 108 contains no provision on responsibility for complying with the protection rules that it lays down.

In contrast, the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data lay down the *Accountability Principle*, according to which "A data controller should be accountable for complying with measures which give effect to the principles stated above". Thus the aim, initially, is to stipulate that it is the responsibility of the controller of the file to guarantee that the protection principles are complied with.

The time that has elapsed since that text was adopted shows **how important it was to make file controllers more accountable**. For this is the key to taking data protection requirements really into account within organisations. "Ensuring compliance before the fact is less expensive, and imposes less burden on data subjects than having to pursue enforcement actions in court or otherwise".[78]

In a very recent document adopted by the Article 29 Working Party, the European Commission is invited to rewrite the accountability principle set out in Directive 95/46 and to stress the fact that taking

---

[76] D. Korff, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, EC Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, WP 2, 20 January 2010, p. 8.

[77] See the discussion of this issue in relation to the ECJ's judgment, which raised many questions.

[78] OECD Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Working Party on Information Security and Privacy, Report on Compliance with, and Enforcement of, Privacy Protection Online, DSTI/ICCP/REG(2002)5/FINAL, 12 February 2003.

responsibility for observing the protection rules entails taking concrete measures. Consequently, the Article 29 Working Party proposes that accountability should in future be backed up by an obligation to be capable of demonstrating that one has taken such measures: "a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request. In practice this should translate into scalable programs aiming at implementing the existing data protection principles (sometimes referred to as 'compliance programs')".[79] Likewise: "**the accountability principle would require data controllers to have the necessary internal mechanisms in place to demonstrate compliance** to external stakeholders, including national DPAs. The resulting need to provide evidence of adequate measures taken to ensure compliance will greatly facilitate enforcement of the applicable rules".[80]

The Madrid Resolution contains a provision of clearly comparable intent. Article 11 thereof, headed "Accountability principle", requires the person responsible, as well as taking all necessary measures to comply with the protection rules, also to set in place internal mechanisms such as to demonstrate that those rules are actually complied with. The accountability principle is furthermore backed up by rules on liability whereby the persons concerned can be compensated for any material or non-material damage caused by failure to comply with the protection rules.

The matter could also be considered in the framework of Convention 108.

9. Taking account of "privacy by design"

It is necessary to start to think about privacy when you think about the idea you will design, not at the time of implementing it.[81]

The "privacy by design" principle appears increasingly to be an inescapable requirement today in the effort to ensure effective protection for privacy and personal data. **This requirement that concern to protect privacy be integrated from the very earliest design stages into the systems, products and services created** was repeatedly mentioned during the Internet Governance Forum in September 2010.[82]

---

79 Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173 of 13 July 2010, paragraph 3.

80 Article 29 Working Party, WP 168, paragraph 79.

81 Joseph Alhadeff, Vice-President for Global Public Policy and Chief Privacy Officer for Oracle Corporation (Washington), at the Internet Governance Forum, Workshop "The Future of Privacy", Vilnius, 14 September 2010.

82 Hugh Stevenson, Deputy Director for International Consumer Protection Office of International Affairs, U.S. Federal Trade Commission: "The first is we [the US Federal Trade Commission] encourage businesses to integrate privacy and security into their systems at the outset. I think that's responsive to one of the comments here on the important of incentives of privacy and system design. […]"; Ellen Blackler, Executive Director, AT&T; Rosa Barcelo, legal adviser to the European Data Protection Supervisor: "Another right we will support is the right to privacy by design. This right will be required, not only the data protection principles taken into account in the technology but also in the whole organisation, in the beginning from the moment when the standards are written to the end of the process"; Joseph Alhadeff, Vice-President for Global Public Policy and Chief Privacy Officer for Oracle Corporation (Washington); the Internet Architecture Board (IAB); Jon Peterson (Neustar), Hannes Tschofenig (Nokia Siemens Network), Bernard Aboba (Microsoft), "Position Paper: Improving Privacy on the Internet and the Role of the Standards Community" for the "Future of Privacy" workshop: "From the long experience of the Internet Engineering Task Force (IETF), the authors believe that an important initial step is to consider privacy while designing protocols and architectures, rather than as something to bolt on as an afterthought.

In the view of participants from every part of the world, this makes an appropriate contribution to the protection of data and privacy.

On several occasions the European Commission has underlined the necessity of such a principle, notably in the case of particular applications (as with the Internet of Things: "Past experience with the development of ICT shows that they are sometimes neglected during the design phase, and that integrating features to safeguard them at a later stage creates difficulties, is costly and can considerably reduce the quality of the systems. It is therefore crucial that IoT components are designed from their inception with a privacy- and security-by-design mindset and comprehensively include user requirements").[83] The Article 29 Working Party and the European Data Protection Supervisor have also argued the need for this to be made a legal requirement.

For its part, the OECD has done much to encourage recourse to technology in order to foster data protection. The Ministerial Declaration of 1998 observed that technologies to protect privacy could play a decisive part in enabling Internet users to exercise greater control over personal information about them and to exercise their freedom of choice with regard to the uses made of their data. The governments of the OECD member states undertook to encourage the use of technologies for enhancing privacy. They called on the OECD to co-operate with industry and business as they strive to ensure the protection of privacy on global networks.[84]

This brings us to another aspect of the question of taking privacy into consideration at the stage of technical product configuration. It is a comment made by the authors of a study commissioned by the European Commission on the new challenges to the protection of privacy in the light of technological developments. The authors point out that imposing default parameters to protect privacy on players offering social networking sites or blogs would afford a solution to the problem of limiting exceptions for personal use (cf. the observations above on these limitations where public channels of expression such as the Internet are used). The authors state that it should be possible to apply data protection rules more flexibly to relatively minor Internet activities. There is a problem with seeking to subject individuals using the Internet in a normal way to the full impact of all the rules applicable to "controllers". In their view, the best way of solving the problem is to regulate the services used by such individuals - social networking sites, sites hosting blogs, etc. These hosts should be obliged to assign default parameters and tools which respect privacy to their sites and services. Ordinary users making use of these sites without modifying the default parameters should be confident that they are not infringing any data protection laws; if the default parameters do not protect privacy and personal data, the site which defined those parameters must take the main responsibility for this.[85]

Over and above the general obligation to take into account and incorporate the requirements of data

---

[…] Technical work needs to be backed-up by laws and appropriate disincentives to violate them. Providing the right incentives for companies to consider privacy friendly design will be a game changer.", etc.

[83] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – The Internet of Things: an action plan for Europe, 18 June 2009, COM(2009)278 final.

[84] OECD, Ministerial Declaration on the Protection of Privacy on Global Networks, 19 October 1998. See also the OECD Forum on technologies to protect privacy, 8 October 2011; OECD, Privacy Online: OECD Guidance on Policy and Practice, Paris, 2003, pp. 273-383.

[85] LRDP Kantor Ltd in association with the Centre for Public Reform, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, Final report, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, January 2010, § 35.

protection (transparency of data collected, what is done with them, who has had access, obtaining of informed consent, etc) into products and services, two particular facets of that obligation have been highlighted:

9.1. THE PRINCIPLE OF DATA MINIMISATION

See the observations on this subject in point 3 above concerning protection principles, the principle of data minimisation being presented as a possible new protection principle.

9.2. PRIVACY IMPACT ASSESSMENTS

It has also been requested that, before a product or service (such as RFID tags) is developed and launched, the designers should be required to carry out an assessment of the privacy and data protection impacts which the product or service in question may have.[86] In the view of the European Commission, the level of detail of the assessment must be appropriate to the potential risks to privacy entailed by the application.

These privacy impact assessments could be regarded as a manifestation of the balancing of rights and interests which should precede the launch of any data processing (cf. point 3.2 above). This obligation to keep a written record of the balancing operation guarantees that all the interests at stake have really been taken into account and would make it easier, if appropriate, to challenge the result of the balancing operation.

As a minimum, impact assessments could be made mandatory in the case of products, services or data systems which might well have a significant impact on the population.

A similar approach has been adopted in Australia, where "The Government now proposes that the Privacy Commissioner will be able to direct federal government agencies (but not companies) to provide to the Commissioner a PIA [Privacy Impact Assessment] on a 'new project or development' that the Commissioner considers will have a 'significant impact' on the handling of personal information, and to report to the Minister (query whether also the public) if the agency fails to do so (AusGov, 2009: 47-4)."[87]

It is interesting to note the approach taken by the authors of the Madrid Resolution on these matters. That text brings together, in a provision headed "Proactive measures", a set of organisational, technical and other measures to contribute to protection within a "new and modern framework". These measures include the adaptation of technology to data protection legislation[88] and the carrying out of privacy

---

[86] European Data Protection Supervisor (see his Opinion in Official Journal C 101, 23.4.2008, pp. 1-12); European Commission (Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009)3200).

[87] G. Greenleaf, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Country Study B.2 – Australia, January 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B2_australia.pdf, p. 33.

[88] "States should encourage, through their domestic law, the implementation by those involved in any stage of the processing of measures to promote better compliance with applicable laws on the protection of privacy with regard to the processing of personal data. Such measures could include, among others: […] e. The adaptation of information systems and/or technologies for the processing of personal data to the applicable laws on the protection of privacy with regard to the processing of personal data, particularly at the time of deciding on their technical specifications and on the development and implementation thereof." (Article 22).

impact assessments,[89] as well as the application of procedures for preventing, detecting and reacting to security failures, the appointment of "data protection or privacy officers", the implementation of training programmes within organisations, the carrying out of audits to check that protection rules are complied with, and the adoption of codes of conduct.

10. Specific protection for minors' data

Convention 108 does not contain any provision specifically protecting data relating to minors. However, because of the particular risks they are exposed to on the Internet and those connected with the use of their mobile phones, **minors do perhaps require special protection**. They are targeted by marketing operations and invited to join certain social networks or groups, to subscribe to certain services, to use certain applications, etc. But at the same time they lack discernment and critical judgment, fail to appreciate the implications of their decisions, take short-term decisions on impulse, and so on.

In its *Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce*,[90] the OECD gave particular attention to the question of the greater risks of commercial exploitation of minors in the context of mobile commerce. In the section headed "Protecting children's personal data", the OECD makes the following recommendation:

"Countries could explore adapting existing laws and rules protecting children on line to the mobile environment. For example, in the United States, federal law restricts the collection, use, or disclosure of personally identifiable information from and about children under the age of 13 in online services. This includes notification about privacy policies; verification of parental consent for collecting personal information from children (with limited exceptions); parental review and deletion of personal information from their children; and requirements for procedures to protect the security of the data".[91]

The difficulty with minors' consent to the processing of their data was already raised in the 2004 report on "Information self-determination in the Internet era".[92] This pointed out, for example, that the consent of under-age individuals to the processing of their personal data raises some awkward issues. Consent must come from a person with legal capacity. Consent expressed by a minor is insufficient without parental authorisation, which does not prevent the minor from having to be associated with that consent in so far as his or her capacity for understanding permits, or even his or her independently expressed consent being required in addition to parental consent.

The development of interactive services on the Internet has made these principles highly relevant in recent times. Children are among the favourite targets of sales operations of all kinds on the Internet, and many different ways of collecting information are employed in getting them to yield personal data – competitions, membership forms, etc.

89 "Article 22. […] f. The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing."

90 OECD, Seoul, June 2008.

91 *Ibid.*, p. 24.

92 Cited above.

It appears necessary, therefore, to check that parental consent has been given for the supply of such information. American law, the Children's Online Privacy Protection Act (COPPA) of 1998[93] states that any service provider collecting information from minors is subject to the principle of "verifiable parental consent", 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 disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child."

11. Specific protection in the case of processing presenting particular risks with respect to rights and freedoms

Technical developments observed since Convention 108 was adopted have shown that certain kinds of processing present particular dangers to the data subjects.

This may be processing envisaged in the public sector, with the combined risks of covering the entire population of a country, or substantial sections of that population, and at the same time being compulsory and wholly excluding any refusal to permit one's data to be processed whatever legitimate justification may be offered. The risks of interconnected files are especially present in the public sector if the same identification number is used for several files. So these risks exacerbate the dangerousness of files or of data processing where the above features exist and where the use of a non-specific identification number is envisaged.

Private sector processing may also present particular risks, for example the introduction of a new technical tool (eg. RFID tags, new mass surveillance systems, facial recognition, body imaging, biometric identifiers, etc) which may well damage the interests, rights and freedoms of the persons to whom the tool is applied.

It would be a good idea to make provision for a precautionary measure prior to the implementation of such processing. Such a measure could take the form of a prior check carried out by the data protection authority or an obligation for the organisation, institution or private agency planning the processing to carry out a privacy impact assessment (see point 9.2 above).

12. Legal remedies

Following a number of ideas which have been put forward in recent years, **thought should be given to the desirability of introducing into Convention 108 the possibility for a legal entity to take legal action in response to infringements of data protection rules.**[94]

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

[94] See in particular LRDP Kantor Ltd in association with the Centre for Public Reform, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, Final report, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, January 2010, §§ 109-111.

"…one needs to realize that in the area of privacy and data protection the damage inflicted upon a person individually considered, is usually not sufficient in itself for him/her to initiate legal action before a court. Individuals normally do not go to court on their own because they were spammed or because their name was wrongly included in a directory. This amendment would permit consumer associations and trade unions representing the interest of consumers at a collective level to take legal action on their behalf before courts."[95]

Similarly, "as mentioned above, entitling legal entities such as consumer associations and PPECS [public providers of electronic communications services] to file lawsuits fosters the position of consumers and it promotes overall compliance with data protection legislation. If breaching companies are facing a higher risk to be sued, they are likely to invest more in complying with data protection legislation".[96]

Over and above the question of the effective upholding of individuals' rights, the decision to recognise the capacity of legal entities to take legal action in this field would undoubtedly have the effect of improving respect for the protection principles in practice.

Recourse to arbitration might also be envisaged in view of the real advantages it affords to injured parties (less costly than many legal challenges, quick decisions, etc).

13. Law applicable to the protection of data and privacy – transborder data flows

13.1. A CONTEXT DIVIDED IN THREE WAYS

Before discussing what law is applicable, it is important to mention the characteristics of the new technical context that have an impact on the answer to this question. These characteristics result from the fact that the context is one divided in three ways.

Mass daily use of the Internet (webmail, social networks, e-commerce platforms, etc) generates countless transborder data flows. Developments in information technology, such as cloud computing, make possible an actual relocation of IT and information resources. Data – financial, personal, commercial, etc – are processed where this will be economically and technically most efficient and are accessible from anywhere in the world via the Internet. For some time now, the services of the information society[97] have been offered to everyone on line from one or more countries and come in as many varieties as there are needs and clienteles: individuals acting for private or professional purposes; small, medium and large companies; non-profit associations; public administrations; trade unions, campaigning politicians; hospitals; universities, etc. Accordingly, the context of the services concerned differs, firstly according to *location* (the location of their providers, their target group, their means of

[95] Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJEU, 6 June 2009, C-128, p. 39, § 89.

[96] *Ibid*., § 92.

[97] In Community law, they are defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services", Article 1(2)(a) of Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 217 of 5 August 1998.

processing, of access to the service, etc) and, secondly, according to their *nature*, depending on the parties and data involved (public bodies, individuals acting for private purposes, multinationals, etc).

Inevitably, such a context raises the question of the international jurisdiction of the courts or public authorities (police [criminal, financial, etc], data protection authorities, etc) and the matter of identifying the law governing the various conceivable factual situations[98]. When drawing up and interpreting the legal rules resolving these questions, various key objectives have to be reconciled, including the territoriality principle, international consistency, the need to guarantee the effective protection of the rights (fundamental or otherwise) of certain parties and the need for legal certainty.

Convention 108 and its Additional Protocol – binding international treaties – govern the automatic processing of personal data and transborder data flows associated therewith. In the light of the international nature of the situation previously described, the Convention harmonises the legislation of forty-three[99] of the forty-seven Council of Europe member states, while the Protocol, which is much more recent (2001), has been signed by forty-one states, thirty of which have subsequently ratified it[100]. Moreover, all Council of Europe member states are bound by Article 8 ECHR, which is particularly relevant here. Mention should be made in passing of the provision that non-members of the Council of Europe may accede to Convention 108 (Article 23) and, subsequently, to the Additional Protocol (Article 3(2)).

Twenty-seven of the forty-three states that are members of Convention 108 also belong to the European Union, where, in particular, Directives 95/46 and 2002/58 harmonise their legislation on the processing of personal data[101]. To these states may be added Iceland, Norway and Liechtenstein, which are also required to comply with these directives under the European Economic Area Agreement.

Otherwise, the binding rules on data protection are strictly national in origin. If need be, the OECD's (non-binding) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data may provide a source of inspiration beyond the aforementioned instruments. Finally, data protection provisions are explicitly included in the rules of the World Trade Organisation (WTO). For example, international trade in services may be restricted on data protection grounds; Article XIV(c)(ii) of the General Agreement on Trade in Services provides that the agreement shall not prevent the enforcement by member states of measures relating to "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts". Improper application of this exception could be identified by a panel and give rise to the imposition of WTO sanctions.

The context also divides in a third way associated with the often international span of technological developments (especially the internet and related services), with different legal orders and cultures needing to address identical or similar situations.

In such a context, the flexibility of an international instrument like Convention 108 helps to guarantee the co-existence of different layers of regulation and to enable the law to address in a fair and appropriate manner the complex and changing situations brought about by current (and future)

98 The discussion mainly focuses on the question of determining the law applicable.

99 Turkey and Russia have signed but not ratified Convention 108, whereas San Marino and Armenia have not signed it.

100 The Protocol has not yet been signed by Armenia, Azerbaijan, Georgia, Malta, San Marino or Slovenia. It has not yet been ratified by Belgium, Denmark, Finland, Greece, Iceland, Italy, Moldova, Norway, Russia, Turkey or the United Kingdom.

101 See also the European Charter of Fundamental Rights.

technologies. It is states that – possibly under the supervision of an international judge – specify the protection of the individuals concerned and ensure its effectiveness via their legislation, courts and national data protection authorities. Consideration should be given to the benefits of the possible harmonisation of the rules of private international law in this area and to determining what role could be played by the Council of Europe in this respect.

13.2. SYSTEM OF TRANSBORDER DATA FLOWS [TDFS]: ABSENCE OF LEGAL RULES APPLICABLE TO DATA PROTECTION

Transborder data flows are governed by Article 12 of the Council of Europe Convention and Article 2 of the Additional Protocol.

For example, between parties to the Convention the sole aim of protecting privacy cannot in principle result in a prohibition of transborder data flows to the territory of another Party or their subjection to administrative authorisation. An exception to this rule is permitted by the Convention (Article 12(2)(a) and (b)): "insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection" or "when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph". In the first case, a state can limit TDFs relating to certain categories of data or processing if the country of destination does not guarantee "equivalent" protection. In the second case, which involves an anti-circumvention provision, TDFs to a third state are only indirectly taken into account.

The EU member states "shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under" Directive 95/46 (Article 1(2)). The rule is thus stricter between EU states.

The Additional Protocol to Convention 108 applies to transborder data flows to a state (or an organisation) not party to the Convention (not "subject to the jurisdiction of a Party to the Convention"). It only permits such flows if the state (or organisation) that is not a party "ensures an adequate level of protection" (Article 2(1) of the Protocol). However, this requirement does not apply to a data transfer in two specific cases: 1) "if domestic law provides for it because of specific interests of the data subject"; 2) "because of legitimate prevailing interests, especially important public interests" (Article 2(2)(a) of the Protocol). The data subject's consent could thus play a role, as provided for by Directive 95/46, work on which began in the light of developments. However, a cause for concern will, incidentally, be the risk that *in practice* this consent is only one contractual clause among others deemed contractual merely through the use of the service offered. On the other hand, there is no need to provide adequate protection "if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law" (Article 2(2)(b) of the Protocol).

The EU member states are also required to apply the rules of Directive 95/46 relating to these flows to states outside the EU that may also be parties to Convention 108. Article 25 of Directive 95/46 also establishes the principle of the need for adequate protection to be afforded in a third country of destination for data, and Article 26 lists a number of exceptions to this principle, including the data subject's unambiguous consent and contractual guarantees. In this context, it is important to emphasise with regard to states that are not members of the EU but are parties to Convention 108 that failure to accede to its Additional Protocol could – if there are no similar rules in domestic law – constitute a

serious gap in the protection provided[102]. The absence of "procedural mechanisms in place to ensure that the basic principles are rendered effective" could also be a crucial factor[103]. In short, the mere fact that a state is a party to Council of Europe Convention 108 – and even to the Protocol as well – is not considered to provide a guarantee of adequate protection, although it will in practice probably do so in many cases.

It is, incidentally, interesting to note that, as things stand, an adequacy analysis to be carried out pursuant to Directive 95/46 does not enable account to be taken in the non-member state of destination of the rules on processing "in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State) and the activities of the State in areas of criminal law"[104]. This is, however, possible in the context of the Additional Protocol to Convention 108[105].

The aim of Convention 108 in the regulation of transborder flows, however, is "to reconcile the requirements of effective data protection with the principle of free flow of information, regardless of frontiers, which is enshrined in Article 10 of the European Human Rights Convention" (explanatory report, § 62). The main objective is to avoid the free flow of information being jeopardised by "forms of protectionism" (explanatory report, § 20). Accordingly, "there shall not be permitted between Contracting States obstacles to transborder data flows in the form *of prohibitions or special authorisations* of data transfers between Contracting States" (explanatory report, § 67) (authors' italics). This wording shows that the Convention prohibits any "administrative supervision".

However, on the one hand the aim is not to prevent a state from taking "certain measures to keep itself informed of data traffic between its territory and that of another Contracting State, for example by means of declarations to be submitted by controllers of data files" (explanatory report, § 67). On the other hand, as pointed out above, states are permitted to regain this control for specific categories of personal data or processing[106].

The system of rules set up is thus all in all relatively complex, but it should be added that, apart from the content of the provisions mentioned, Convention 108 and its Protocol *do not regulate the impact that the applicability of the law of a contracting state, rather than that of another state, might have on the processing of personal data*. This applies in the context of TDFs both to third states and to other contracting states. On the subject of the latter, the explanatory report to the Convention (§ 10) thus

---

102 Article 29 Working Party (WP 12), Transfers of personal data to third countries. Applying Articles 25 and 26 of the EU Data Protection Directive, 24 July 1998, p. 9.

103 *Ibid*.

104 Article 3(2), 1st indent, of Directive 95/46 excludes these matters from the scope of the directive.

105 At EU level, Decision 2008/977/JHA concerns the processing of data in the context of police and judicial co-operation by the competent authorities – see Article 1(2) of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, of 27 November 2008. It can clearly not apply to a case in which competent foreign authorities obtain personal data on EU nationals from databases managed by service providers situated in the third country in question and under its jurisdiction. This question might usefully be considered in an adequacy analysis. This would be the case, for example, with the "third party doctrine" in the United States, which could be considered in an adequacy analysis conducted on the basis of the Council of Europe Convention.

106 Although this control is permitted between Contracting States to the Convention, we believe this applies even more in the context of the Additional Protocol vis-à-vis third states. The Protocol prohibits the authorisation of flows when there is no guarantee of adequate protection in the state of destination. It does not prohibit the banning of certain specific data flows even when the third state of destination guarantees adequate protection.

recognises that "it may not always be easy to determine which State has jurisdiction and which national law applies", stressing that "the 'common core' (of the Convention) will result in a harmonisation of the laws of the Contracting States and hence decrease the possibility of conflicts of law or jurisdiction" (§ 20). Thus, **Convention 108 and its Protocol** do not eliminate these conflicts. They **determine neither the law applicable to data protection nor the courts with jurisdiction in disputes in this area**. The already mentioned division of the technology context increases the importance of these rules. In these areas – the applicable law and the competent court – it is the legal order of the European Union that appears the most advanced as far as its harmonisation is concerned.

13.3. LAW APPLICABLE TO DATA PROTECTION: ARTICLE 4 OF DIRECTIVE 95/46 AND REGULATION 864/2007 ("ROME II")[107]

In the context of the law applicable to data protection, Article 4 of Directive 95/46 is the provision that goes furthest in harmonising the rules determining the data protection law applicable to the processing of personal data[108]. This provision determines the cases in which member states have to apply their domestic law. Together with Articles 25 and 26 governing TDFs, it determines the spatial applicability of European data protection[109].

First of all, however, in principle it only determines the cases in which member states *must* apply their domestic legislation. In other words, if a member state is not required to apply its domestic law, the Directive does not determine what law it must apply, unless it is interpreted as enshrining a true bilateral conflict of laws rule stating what law in the EU legal order is applicable to a given situation, or unless unilateral reasoning is applied. It should be borne in mind that in both cases only laws applicable in the situations covered by the spatial scope of Directive 95/46 would be specified[110].

So what about the possible applicability of domestic law other than in the cases excluded from the spatial scope of Directive 95/46? As the Group 29 Working Party points out, "there are situations which fall outside the scope of application of the directive. This is the case where non-EU established

[107] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199 of 31.7.2007.

[108] With regard to the law applicable to data protection and, especially, Article 4 of Directive 95/46, see in particular C. Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)", *International Journal of Law and Information Technology*, 2010, no. 18 (2), pp. 176-193; C. Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)", *International Journal of Law and Information Technology*, 2010, no. 18 (3), pp. 227-247; J.-P. Moiny, "Facebook au regard des règles européennes concernant la protection des données", *Revue Européenne de Droit de la Consommation*, 2010, no. 2, pp. 255-270; F. Rigaux, "Libre circulation des données et protection de la vie privée dans l'espace européen", in *La protection de la vie privée dans la société de l'information, L'impact des systèmes électroniques*, P. Tabatoni (ed.), vol. 2, P.U.F., Paris, 2000, pp. 25-40.

[109] On the subject of the determination of its territorial applicability by derived Community law, see S. Francq, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé,* Bruylant/L.G.D.J., Brussels/Paris, 2005.

[110] In this case, for the situations that fall within the spatial scope of Directive 95/46 the latter would ultimately determine what law is applicable for each processing operation. If this provision is transposed by member states to the letter (naturally *mutatis mutandis*), then each processing operation falling within its spatial scope should in principle be subject to the law of a sole member state (eg the law of the state where the data controller's place of business is located in the framework of the activities of which the processing of personal data is carried out). It would be logical, owing to the harmonisation effected by Directive 95/46, for member states mutually to recognise their relevant regulations. However, it should be noted that this harmonisation does not prevent differences of national laws in view of the leeway allowed to member states by Directive 95/46. This clearly applies all the more in the case of the States Parties to Convention 108.

controllers direct their activities to EU residents which result in the collection and further processing of personal data. For example, this is the case of on-line vendors and the like using specific advertisements with local flavour, websites that *directly target* EU citizens (by using local languages, etc). If they do so without using equipment in the EU, then Directive 95/46/EC does not apply"[111] (authors' italics). What about the role of domestic law in these cases?

Secondly, depending on the data processing done and on the data controller's places of business, the same data controller could be required to comply with different national laws, so application may prove a complex matter. In addition, the choice of law criteria taken into account, namely the use of resources (equipment) in the territory of the Community for the purpose of carrying out the processing in question and the place of business in the framework of which the processing occurs, cause serious interpretation and application difficulties in the "divided" context described in our introduction. Accordingly, a recent study commissioned by the European Commission states that "(t)he rules in Article 4(1)(a) are quite simply utterly confused and impossible to apply in the new global-technical environment"[112]. In addition, taking into account the location of the equipment used for processing data does not necessarily prove relevant in the light of technological developments[113]. The study goes on: "The rules in the Directive on applicable law are also effectively impossible to apply to non-EU/EEA companies and organisations that are active in Europe - especially if they are active on the Internet (as they almost all are, and certainly will be)"[114].

Thirdly, and finally, and this point is linked to the previous one, the implementation of Article 4 of Directive 95/46 ultimately depends on its transposition by member states. This Article thus does not fully resolve the question of the law applicable to data protection within the legal order of the European Union.

It is interesting to note that, as far as the determination of the applicable law is concerned, data protection does not follow the same rules here as privacy itself – which is in particular protected by Article 8 ECHR[115]. Nor, moreover, is the law applicable to non-contractual obligations arising from a breach of the fundamental right to privacy determined by the "Rome II" Regulation, which determines the law applicable to non-contractual obligations in general[116]. In other words, it is the domestic law of the member states that decides. In Belgium, for example, in line with the unilateral approach adopted in the Directive, the Law on Privacy determines its territorial scope unilaterally, whereas the Belgian Code of Private International Law states which law governs an obligation resulting from a breach of privacy, which it does by means of a multilateral rule that, for every case, specifies the law applicable (foreign or

---

111 Group 29, WP 168, "The Future of Privacy", Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009, pp. 10-11.

112 LRDP Kantor Ltd, in association with the Centre for Public Reform, "Comparative study on different approaches to new privacy challenges, in particular in the light of new technological developments", Final Report, January 2010, p. 29, para. 37, available at

http://ec.europa.eu/justice/polics/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf,.

113 For example, in the context of cloud computing, the location of the means of processing (especially computation and memory resources) may be dictated, in real time, by the search for the optimum efficiency of the service and the best allocation of the service provider's computing resources.

114 LRDP Kantor Ltd, in association with the Centre for Public Reform, *op. cit.*, p. 30, para. 39.

115 It may be pointed out that, to a certain extent – as data protection is not limited to the protection of privacy – the regulations protecting individuals against the processing of personal data give Article 8 ECHR horizontal effect. See below with regard to the possible impact of that article on the rules of private international law.

116 See Article 1(2)(g) of the "Rome II" Regulation.

Belgian)[117]. In other words, the identification of a breach of privacy based on the horizontal (at any event, indirect) effect of Article 8 ECHR and the redressing of that breach could be governed by the law of an EU member state, whereas data protection aspects would be subject to the application of the law of a non-EU member. Similarly, the contractual relationship between a consumer (the data subject) and a service provider (the data controller) could be governed by the law of the consumer's habitual residence[118], whereas data protection aspects could be subject to the application of the law of a non-EU member.

Finally, within an area where rights are harmonised in principle and where states are duty bound mutually to recognise their laws, the question of the law applicable to data protection remains complex and does not necessarily guarantee legal certainty, to the disadvantage of both data subjects and data controllers. This applies all the more to the relations between the States Parties to Convention 108, as well as to those between the States Parties to the ECHR. Also worth emphasising is the potential role of Article 8 ECHR with regard to the rules determining the law applicable to data protection and the protection of privacy.

13.4. The impact of Article 8 ECHR on the determination of the law applicable to the protection of privacy and data protection

Above all, it is necessary to bear in mind the legal links mentioned above (cf. section 1.1.1. of this report) between data protection and the protection of privacy. The European Court of Human Rights has ruled on several occasions that Article 8 ECHR applies to the processing of personal data[119], referring, moreover, to Convention 108, which is interesting on two counts: first and foremost, it implies that the European Court of Human Rights may decide to sanction a State Party to the ECHR for its conduct for reasons connected with its regulation of the processing of personal data. Notwithstanding the fact that the application of Convention 108 and its Protocol does not fall within the Court's jurisdiction. It should be noted that the Treaty of Lisbon provides for the European Union to accede to the ECHR[120], which will strengthen the Court's role vis-à-vis the EU[121], whose acts could then be challenged before it. This also

---

117 See section 99 of the Law of 16 July 2004 on the Code of Private International Law, *Moniteur Belge* of 27 July 2004, and section 3 *bis* of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, *Moniteur Belge* of 18 March 1993.

118 See Article 6 of Regulation (EC) no. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)), OJ L 177 of 4.7.2008; J.-P. Moiny and B. De Groote, "'Cyberconsommation' et droit international privé", *Revue du Droit des Technologies de l'Information*, 2009, no. 37, pp. 5-37.

119 See in particular Eur. Ct. H.R., 16 February 2000, *Amann v. Switzerland*, Application No. 27798/95, 16 February 2000; Eur. Ct. H.R., 4 May 2000, *Rotaru v. Romania*, Application No. 28341/95; Eur. Ct. H.R., 31 May 2005, *Antunes Rocha v. Portugal*, Application No. 64330/01; Eur. Ct. H.R., 10 October 2006, *LL v.. France*, Application No. 7508/02; Eur. Ct. H.R., 4 December 2008, *Marper v. the United Kingdom*, Applications Nos. 30562/04 and 30566/04; Eur. Ct. H.R., 2 September 2010, *Uzun v. Germany*, Application No. 35623/05.

120 "[t]he Union shall accede to the [Convention]. Such accession shall not affect the Union's competences as defined in the Treaties" (Article 6(2) of the Treaty on European Union). The accession talks began on 7 July 2010, see http://www.coe.int/t/dc/files/themes/eu_and_coe/default_en.asp?

121 See Parliamentary Assembly, Committee on Legal Affairs and Human Rights, M.-L. Bemelmans-Videc (rapporteur), "The accession of the European Union/European Community to the European Convention on Human Rights", 18 March 2008, p. 8, para. 12, available at

http://assembly.coe.int/Documents/WorkingDocs/Doc08/EDOC11533.pdf,.

implies that states that have not yet signed and/or ratified these instruments are nonetheless still, on the basis of Article 8 ECHR, bound by rules concerning the processing of personal data.

For example, the Court could, in pursuance of Article 8 ECHR, be asked to scrutinise[122] (and perhaps sanction) a state because one of its courts has applied a foreign law in a particular case in which Article 8 ECHR had been misinterpreted to the detriment of the individual litigant concerned[123] – an individual who is "within the jurisdiction" of the state within the meaning of Article 1 ECHR[124]. "As soon as the state exercises its powers, […], it must act in compliance with the Convention"[125]. In this type of case, the foreign law could be departed from by applying a public policy exception mechanism. Logically, if this "foreign law" is the law of another Council of Europe member state, then the application of this exception should be limited (especially if that state is also a party to Convention 108, and even more so if it is a member of the European Union). The application of such an exception would mainly be required in the case of a state that is not party to Convention 108 and does not guarantee adequate protection. In these cases, one would imagine that the "common core" of Council of Europe Convention 108 should be applied to the dispute in question, failing which the European Court of Human Rights, which could rule that the common core of that Convention is guaranteed by Article 8 ECHR, might impose a penalty. The same would apply to all the data protection rules developed by the Court on the basis of Article 8.

13.5. CONCLUSION: A RULE DETERMINING THE APPLICABLE LAW IN CONVENTION 108?

The purpose of Convention 108 is "to secure in the territory of each Party for every individual, whatever his or her nationality or residence, respect for his rights and fundamental freedoms, and in particular right to privacy, with regard to automatic processing of personal data relating to him" (Article 1 of the Convention). It does this by guaranteeing a common minimum legal framework for data protection, which, as explained above, could have a number of gaps. We have surely already shown the complexity of the issues of private international law that arise in this area, especially with regard to questions concerning the applicable law.

Common rules of private international law would, of course, contribute to achieving the aforementioned objective. On the one hand, they would increase legal certainty and, as a result, definitely help to improve the effectiveness, in practice, of the substantive rules[126]. Clearly, a lack of clarity with regard to

---

122 On the subject of this scrutiny, see in particular. P. Mayer, "La Convention européenne des droits de l'homme et l'application des normes étrangères", *Rev. crit. dr. internat. privé*, 1991, p. 664.

123 With regard to the influence of the ECHR on the conflict of law rules, see in particular L. Gannagé, "A propos de l'« absolutisme » des droits fondamentaux", in *Vers de nouveaux équilibres entre ordres juridiques – Liber amicorum Hélène Gaudemet-Tallon*, Paris, Dalloz, 2008, pp. 265-284.

124 On this subject, see the arguments put forward by S. Karagiannis in "Le territoire d'application de la convention européenne des droits de l'homme, *Vaetera et nova*", *Revue trimestrielle des droits de l'homme*, no. 61, 2005, pp. 33-120. See in particular Eur. Ct. H.R., 23 March 1995, *Loizidou v. Turkey* [GC], Application No. 15318/89; Eur. Ct. H.R., 12 December 2001, *Bankovic and Others v. Belgium and other Contracting States*. [GC decision], Application No. 52207/99; more recently, Eur. Ct. H.R., 29 March 2010, *Medvedyev and Others v. France* [GC], Application No. 3394/03.

125 G. Cohen-Jonathan and J.-F. Flauss, "Cour européenne des droits de l'homme et droit international general", *Annuaire français de droit international*, no. 47, 2001, p. 438.

126 Where the European Union is concerned, it has recently been pointed out on the subject of Article 4 of Directive 95/46 that "(a)ll these problems are serious and hamper internationally operating companies and organisations, making it more difficult for them to comply with data protection rules and principles. These problems are greatly enhanced in the new, generally internationalised socio-technical environment, and in relation to the

the legal rules applicable could prejudice effective application of substantive rules by considerably, and perhaps excessively, complicating the lives of companies. So in the European Union, whose regulations pursue the creation of a single market, a common rule is all the more necessary.

Furthermore, it is possible in a domestic court for a gap to appear in the protection of individuals if the judge had to apply less protective foreign law (inadequate protection). In such a case, a public policy exception mechanism would make it possible to avoid, in litigation before the domestic courts, the application of a foreign rule depriving an individual of all or part of the "common core" of Convention 108 or of the rights guaranteed on the basis of Article 8 ECHR.

However two major difficulties arise concerning the possible definition of rules determining the law applicable in the context of Convention 108. On the one hand, is it *politically* conceivable that the Council of Europe member states might agree on the adoption of such a rule? It should first be pointed out that when the Madrid Declaration was adopted there was no agreement on matters of private international law, and that, at all events, the adoption of such a rule requires co-ordination with the European Union. The differences between the substantive law of the States Parties to the Convention are in any case likely to cause difficulties in this connection.

On the other hand, the multiplicity of situations, individuals and legal questions involved in data protection disputes complicates the task of drawing up rules governing issues of private international law. As far as the applicable law is concerned, a rule providing for alternative choices of law would probably be helpful. This rule should in particular take into account the different legal orders involved (European, Council of Europe [ECHR], Council of Europe [Convention 108 and Additional Protocol] and international in the broad sense [relations with third states]). An instrument like Convention 108 needs to be flexible enough to enable states (and their organs) to grasp the three-way division outlined in our introduction and arbitrate judiciously between the rights, freedoms and interests of the individuals concerned, while at the same time considering the interests of society as a whole. In all cases, the domestic judge must have the tools necessary to grasp situations that may be very different, and it is in principle up to him or her in a specific case to interpret the rules, whatever their origin (if need be under the supervision of an international court (the ECJ, or the Eur. Ct. H.R where the application of Article 8 ECHR is concerned). Accordingly, at issue here, more fundamentally, are the *theoretical and practical* feasibility of drawing up a common rule for specifying the applicable data protection law.

In the light of all the above considerations, **we may query whether the absence of rules specifying the applicable data protection law constitutes a deficiency of Convention 108;** the private international law of member states is required to determine this matter. The more the laws of states become harmonised, the less serious the consequences of the interplay of these rules will be. On this subject, it should be pointed out once again that states which are not Council of Europe members may accede to Convention 108 (Article 23) and then to the Additional Protocol (Article 3(2)). At all events, the judge will ultimately always declare a particular law applicable in a dispute. However, a debate on the rules determining the data protection law applicable is no less helpful, and is even essential, with a view firstly to providing individuals with more effective protection, and secondly to strengthening legal certainty for data controllers. Accordingly, a **recommendation of the Committee of Ministers** of the Council of Europe would at the very least provide timely fuel for the debate and be helpful in the attempt to harmonise the provisions on the law applicable.

Internet in particular (but not only)", LRDP Kantor Ltd, in association with the Centre for Public Reform, *op. cit.*, p. 30, para. 42.

At the end of this report, it is important to put forward a point for discussion that is not directly linked to the question of the law applicable, but could doubtless have an impact on it, namely the **possibility of stating in Convention 108 itself that the latter, or at the very least some of its provisions (clearly specified), has/have a direct effect enabling them to be directly relied on in domestic courts**[127]**.** In this case, account should be taken of the conditions normally accepted for acknowledging that provisions contained in an international instrument have direct effect.

13.6. ADDITIONAL ASPECTS CONCERNING TRANSBORDER DATA FLOWS

The following points need to be added to what has been said about transborder data flows in the previous paragraphs.

In the new technological environment, **it is essential to clarify what is meant by TDFs**. In particular, it is important to state whether the term "transfer" employed in Article 2 of the Additional Protocol[128] covers the making available, distribution and publication of data. This clarification is essential in respect of the making available of data on websites[129].

Article 2 of the Additional Protocol[130] adopts the concept of an "adequate level of protection" as a criterion for acceptance of transborder data flows. It would no doubt be helpful to add that **determining adequacy presupposes an evolving interpretation**, since adequacy is not established once and for all, but depends on interpretations of the Convention by the Strasbourg Court in its case-law and on new rules adopted (recommendations, additional protocols).

The explanatory report to the Additional Protocol provides this clarification concerning the assessment of adequacy: "27. The level of protection should be assessed on a case-by-case basis for each transfer or category of transfers made. […] 28. An assessment of adequacy can similarly be made for a whole state or organisation thereby permitting all data transfers to these destinations. In that case, the adequate level of protection is determined by the competent authorities of each Party." **A full statement should be made regarding the tier of authority responsible for assessing the adequacy of the protection afforded by a third state**. Overall assessments are carried out by the "competent authorities", but there is no provision for case- by case assessments.

---

127 It should be noted that the Principality of Andorra already acknowledges that Convention 108 has direct effect. This has in particular enabled some gaps in that state's legislation on the protection of personal data to be plugged. It was after taking this direct effect into account that the Article 29 Working Party accepted that Andorra provided an adequate level of data protection. Cf. Article 29 Working Party, Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra, WP 166, 1 December 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp166_en.pdf

128 "Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer."

129 Cf. the Lindqvist case decided by the ECJ, which provided an opportunity for a discussion of the term "transfer" in the context of the internet and resulted in an ill-considered response by the Court of Justice on this point: ECJ, 6 November 2003, (Lindqvist), C-101-01, *Rec.* p. I-12971. For a critical review of this judgment, see. C. de Terwangne, "Arrêt Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles", note under "C.J.C.E.", 6 November 2003, *R.D.T.I.*, 2004, no. 19, pp. 67 ff.

130 "Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer."

14. Supervisory authorities

Recent assessments of the data protection authorities that have been set up have been mixed:

"DPAs have great insight and knowledge, and provide helpful guidance on the law – but they are not effective in terms of enforcement: 'Policing' of data protection compliance by DPAs is generally weak and ineffective."[131]

"This comparative report highlights the main deficiencies of the current system of personal data protection in the 27 EU Member States. Shortcomings are identifiable in the lack of independence, adequate resources and sufficient powers of some Data Protection Authorities."[132]

Lessons should undoubtedly be drawn from these statements, and it is necessary to consider whether legislative responses could redress the situation, especially by setting criteria to guarantee the authorities' independence. The responsibilities of those authorities should perhaps be **extended**, for example by giving them **power to issue an opinion (compulsory of not) when any rule with a impact on privacy is drawn up**.

The Madrid Declaration reiterates the need to provide "support for independent data protection authorities that make determinations, in the context of a legal framework, transparently and without commercial advantage or political influence". The Madrid Resolution is more precise on the characteristics that such authorities should have (Article 23(2).

The European Data Protection Supervisor also draws conclusions about the present situation: "The new challenges for data protection require stronger supervision, in a more uniform and effective way. The new framework should therefore guarantee uniform standards as to independence, effective powers, an advisory role in the legislation making process and the ability to set their own agenda, in particular by setting priorities regarding the handling of complaints. International co-operation among data protection authorities should likewise be reinforced."[133]

The discussion could also relate to the **advisability of introducing a category of data protection officer**, alongside the supervisory authorities. These officers would act as mouthpieces for those authorities within organisations, institutions, companies, etc, and thus perhaps act as guarantors of better compliance with the principles and rules of data protection within their own bodies.

Finally, there are calls from all quarters for **the strengthening of dialogue and international co-operation, especially between supervisory authorities**.

In its Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of 12 June 2007, the OECD recommends that "Member countries co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:

- Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.

---

131 LRDP Kantor Ltd, in association with the Centre for Public Reform, *op. cit.*, p. 52, para. 104.

132 Comparative Legal Study on Assessment of Data Protection Measures and Relevant Institutions, report commissioned by the EU's Fundamental Rights Agency (FRA), Summary, 2009, para. 8.

133 P. Hustinx (EDPS), "30 years after: the impact of the OECD Privacy Guidelines on the protection of privacy", joint ICCP-WPISP Roundtable, Paris, 10 March 2010, Session 3: The Privacy Guidelines in the Current Environment, available at www.oecd.org/dataoecd/50/18/44946479.doc

- Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.
- Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.
- Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy."

Similarly, the Madrid Resolution includes a very detailed paragraph on establishing and improving co-operation and co-ordination between supervisory authorities with the aim of achieving more uniform protection (paragraph 24).