Data protection and online networks

Louveaux, Sophie; de Terwangne , Cécile

Published in:
Computer Law and Security Report

Publication date:
1997

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

DATA PROTECTION

DATA PROTECTION AND ONLINE NETWORKS

Cécile de Terwangne
Sophie Louveaux

This article examines the application of the EC Data Protection Directive to the protection of personal data in open networks such as the Internet. It identifies a number of problems which have yet to be resolved.

Introduction

The 'information highway' creates threats and challenges in relation to the protection of personal data. Privacy was once defined as "You know it when you lose it". The threats online networks create for privacy are not properly measured by the information highway users. Users do not realise that privacy is at stake. Action must be undertaken to render the user aware of the reality and to address the dangers with concrete and practical solutions so as to avoid the possibility that the user, in order to protect his privacy, simply logs off the network.

Certain dangers can be easily identified. It is clear that online services expand the volume of personal data at stake. Moreover consumers become increasingly remote from organizations which process their data. Different categories of actors intervene in the online game (mainly access providers and information or service providers) and actors have become increasingly numerous (the Internet consists of more than 40 million users throughout the world accessing more than 4 million Internet sites). Such a situation dilutes the responsibility for data security and data protection and multiplies the risk of breaches in security and protection. What's more, the security concern is increased by the fact that multimedia technologies offer higher risks of distortions of reality. Digitalization enables one to obtain the picture of two persons side by side even though they have never actually met.

Moreover, the Net facilitates the quick transmission of information to any other computer system connected to the network. Personal data (even sensitive data such as data about health, political opinions or religious convictions) can be communicated to countries without an adequate data protection level. The transmission which was once mainly active: it was the data subject who decided to transfer certain information, becomes more and more passive: information is made available but one does not know to whom, where to and to what purpose.

Other risks, less evident but equally real, exist. Unlike the traditional and isolated database, the international dimension of the network entails the possibility of an interconnection between information located in different places and provided for various purposes. The danger lies in that it is technically feasible to gather all the personal data related to a given individual that are present on the Net. Search engines using robots to rake the network and to create indexes render it possible to search for any occurrence of a name anywhere in the text of any Web page or in any news posting. One can thus achieve a comprehensive profile of a person (and know for example that he has written articles against nuclear tests, that he is presently unemployed and looking for a job – he made his curriculum vitae available – and that he is involved in newsgroup discussions concerning gay issues). Even if the information was made publicly available by the user by putting it in public areas of the network, he does not necessarily expect his whole life story or personality to be reconstituted, or his messages to newsgroups to be read by anyone outside those with whom he shares a common interest, or – even more preoccupying – he does not expect the information to be used for purposes completely divergent from the initial purpose for which it was provided for.

The last data protection concern we will mention derives from the fact that the use of Internet services is not anonymous.

Internet services generally work with point-to-point connections. A certain amount of information is necessary in order to establish the transmission in itself and to bill the service rendered. Every electronic mail message contains a header with information about the sender and the recipient of the message (name and mail address, time of mailing,...), information will be recorded as to the timing of the message, the length of time of the communication,...

The use of the network generates personal data relating to the users. Users are bound to leave an electronic trace which can be used to develop a profile of personal interests and tastes. The information behaviour of the senders and recipients can be traced and supervised at least by the service provider to whom the information is transmitted. The more the Internet is used for commercial purposes, the more interesting it will be for service providers and other bodies to get as much transaction-generated data about the users of the net. A number of apparently casual uses of the Net will be able to be linked together to create a very complete personal profile of the individual concerned. Individual A orders a pizza via the Net (this reveals not only his taste for Italian food, but will also reveal data concerning the time of the use

of the service enabling localization of the individual); he then fills up at a petrol station using his credit card; makes a booking for a late night movie,...

Three types of approaches can be envisaged. The first is given by security technologies[1]; the second comes from anonymity (encryption and privacy enhancing technologies) and a third one is expressed in data protection rules. As the two first solutions involve mostly, if not only, technical ingredients, they will not be retained for this paper[2]. We will limit our analysis to the data protection rules.

A particular legal instrument deserves a special attention since it is the last-born in the family, hence supposed to be the most advanced. Moreover it is legally binding and it has a particularly wide scope: the European Data Protection Directive.

Protection afforded by the European Directive[3]

The European Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4] was adopted on 24 October 1995. This text lays down a number of principles with regard to the protection of the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data. The Member States are required to transpose these principles into their national legislation within a time limit of three years from the date of its adoption (i.e. by the 24 October 1998).

How will the protection afforded by the Directive apply to networks such as the Internet? Will individuals effectively be guaranteed an appropriate level of protection as regards their personal data when making use of the services offered? We propose to examine the main lines for the protection of the rights and freedoms of the individuals as laid down by the Directive and their application to networks such as the Internet.

I. Definitions and identification

The protection afforded by the Directive applies to the processing of personal data. One of the first difficulties encountered when trying to apply the Directive is to effectively determine when one can consider personal data as being processed.

A. Personal data

The Directive adopts a very broad definition of the term 'personal data' so as to include any information relating to an identified or identifiable person ('data subject'). The person may be 'directly' identified (by reference to his name, for example) or can be 'indirectly' identified by reference to specific characteristics of that person, in particular by reference to an 'identification number', or to one or more factors specific to his 'physical, psychological, mental, economic, cultural or social identity'. Could, therefore, reference to a bank account number, a holiday reservation, fingerprints, be considered as 'personal data' ...

Personal data in the form of sounds or images are also covered by the Directive[5]. This provision is an important step towards the adaptation of processing rules to new technologies and to multimedia applications.

We are able to identify two types of personal data with regard to the use of the Internet:

– User related data.

As already said above, users inevitably leave an electronic trace when entering the Net. This trace takes the form of an IP address, i.e. a series of numbers. It allows the message to reach the desired point of the Net and the information to come back to the user's computer. Such a trace, *in se*, only reveals the identity of the access provider[6] but not that of the user. The access provider is the one who can link the IP address to an identified person or computer (in a company, for example, he knows who is the owner of the computer but not who is the user). Very often, however, the user is asked by the information or service provider to give his name or E-mail address. The latter can then 'put a name' on the IP address and follow the person during all his operations. Data revealing the identification of the data user could be rendered anonymous in the eyes of the recipient of the message via the service access provider (introduction of a code of access rather than his name, for example). This does not, however, mean that the Directive is no longer applicable.

To determine whether a person is 'identifiable', account should be taken of all the means reasonably likely to be used by the controller, or by any other person, to identify the said person[7]. Identification can therefore be carried out either by the controller or by any other person. However, in the latter case, since the data must be considered as relating to an 'identifiable' person in the eyes of the controller, there must be at least a link (contractual, institutional, or any other reasonable link) between the controller and the person who holds the key for identification.

– Personal data contained in the actual content of the message.

This data can relate to the sender of the message himself: he is requested to provide certain personal details in order to obtain a service or information. For example, if he wants to obtain some marketing material through the post, the sender may be requested to give his name, address, ... The data can also relate to a third party to the transmission: an information provider makes available a list of data about certain persons (a directory service, for example). In order to book a flight for his client, a travel agent must introduce the client's name, address and could also include information that will reveal certain preferences (smoker or non-smoker), way of life (vegetarian or not) and some sensitive data such as Muslim, diabetic or handicapped. The data is sometimes made available by the data subject himself who actually seeks a certain form of publicity of his data (an author who wants to make public his latest work, an employment seeker who desires to make known his curriculum vitae via the Internet...).

B. Processing

The definition of 'processing' in Article 2 of the Directive is all-encompassing: any operation carried out on personal data, whether or not by automatic means, is covered by the term. The Directive identifies in a non-exhaustive way some of the operations to which it is applicable. It is therefore possible to say that as soon as data are collected, any use[8] including

collection itself, of such data is an integral part of the processing covered by the Directive. The absence of a distinction between the stages of data collection, use and disclosure, or between processing that occurs within or outside the controlling organization, reflects the changes in technology. These changes include the fact that operations can be carried out by different persons at different moments and in different places, and yet still converge towards the realisation of one common purpose.

A common use of the Internet is to transmit, receive and store messages or sets of structured information (database). In the terms of the Directive, therefore, it is feasible to say that data are being processed.

The use of Internet implies the availability of vast amounts of information to an innumerable number of persons wishing to consult it. Does each consultation by a user imply that the data is being 'processed'[9]? If such is the case, it will imply that each user of the Internet who consults a Web site which contains personal data, will be considered as processing the data. The processing of personal data implies a number of obligations incumbent on the controller and grants a number of rights for the data subject (see below). Does this therefore imply that he must inform the data subjects that he has consulted a Web site containing personal information about them? If the data is neither copied, nor recorded, nor printed what exactly must one notify to the supervisory authority since the consultation has left no tangible trace? And how can one grant the data subject a right of access to information which is at the most stored in a person's mind? A logical problem therefore exists if one considers the sole consultation of data as sufficient to constitute the processing of data in the terms of the directive. A different and more pragmatic approach should perhaps be adopted.

The enumeration contained in article 2.b is underpinned by a chronological order in the list of operations retained. The list begins with the collection of the data and ends with the destruction of the latter. The consultation is not cited at the start of the article, it does not precede the operation of collection. On the contrary, it is placed between the retrieval, use and disclosure by transmission... It therefore seems that the term 'consultation' in the Directive does not cover the simple reading of data, but rather the offering of data for consultation.

The definition of processing as covered by the directive is sufficiently broad to cover any case in which personal data is collected or recorded. In these two cases, contrary to the simple consultation, the processing of the data is materialized. There is therefore no need to regulate cases in which a simple reading of the data is observed. As soon as this reading gives rise to the copying, recording, or any other form of collection or storage of the data, the Directive will apply.

The consultation of the data can therefore be retained as part of the processing of data (data which has been collected, recorded, classified, or even modified are available for consultation for example), but one does not need to consider that the simple reading of data without any further material operation constitutes the processing of personal data as such.

The Directive will not apply to the processing of data by a natural person in the course of a purely personal or household activity (Article 3.2.). Home users of the Internet, in particular, might obtain and use the personal data for a purely personal or household activity (e.g. hobbies or the organization of a private meeting); the principles laid down by the Directive will therefore not apply in these particular cases. The personal nature of the activities mentioned above are evident. However, this is not always the case (is the collection and use of personal data for a university thesis, or the access an employee has to the Internet through his office computer and the server of the company, for example, to be considered as a personal or professional activity?).

C. Controller

According to article 2.d of the Directive, the controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The text designates the controller as the person primarily responsible for the obligations arising from the Directive. The central concept is to specify a single person responsible to the data subjects, and this in order to facilitate provision of information to them as well as to ensure a right of access and guarantee of the effectiveness of the remedies available[10].

The controller is the person responsible for the choices determining the definition and implementation of the processing, and not those persons who perform the processing operations in accordance with instructions from the controller. That is why it is stated that the controller defines the purposes[11]. There is no requirement that the controller be in actual possession of the data; it is the concept of control that is important.

Identification of the 'controller' is one of the primary problems one is faced with when applying the Directive to open networks characterized by their numerous actors:[12]

- Telecommunications organizations provide basic networks for data transfer;
- Access (communications) providers supply services for storage, transmission and presentation. They are responsible for the routing of the message and process traffic data;
- Information (content) providers supply information stored in files and databases to the users (directory services, information databases...);
- Service providers offer their services to users via the Net (banks, travel agents, ...);
- Users access and make use of different Internet services.

These actors are not always clearly identifiable. A same actor may offer different services (telecommunication service and access provider, for example). The main problem linked to the multiplicity of actors is the problem of control over the information and the flows of data and, deriving from that, the problem of liability.

Recital 47 of the Directive suggests that where a telecommunications or electronic mail service is used for the sole purpose of transmitting messages which contain personal data, the controller should be the person from whom the message originates and not the person providing the service. This person will be deemed to be the controller only in respect of any additional personal data processed for the rendering of the service (traffic data).

This provision must be further examined. A telecommunications organization or a network access provider will not be considered the controller as regards information placed on the network by his clients. This can be justified by the fact that the telecommunication organization or access provider does not, and should not, actually process the personal data contained in the message by themselves, but only as a part of the message as a whole. They do not actually define the purposes and means of the processing of the message or service. They will, however, be regarded as the controller when processing user-related personal data for the billing of the service, for example, since in that case they are processing personal data for a purpose defined by them.

As regards the other actors involved in the use of the Internet, a distinction must be made according to the type of service.

As regards the use of the Internet for the sending of E-mails, the person from whom the message originates can be qualified as the 'controller'. He defines the type of data contained in the message and the purposes for which the data are sent (message to a colleague in another university containing information on a common interest). When the E-mail is used for discussion forums, the controller should be the entity responsible for centralising the applications to the forum (the moderator of the forum, for example). Indeed it is this entity which defines the means and purposes of the forum (a medical institution decides to create a discussion forum on a certain type of disease, in order to stimulate scientific discussion on this theme).

Concerning services providing information, it seems to us that at first sight an enquirer consulting information services on the Internet cannot always be qualified as a controller. One must look at the purpose behind the consultation. If the user of the service merely consults the data for the purpose defined by the initial information provider, he cannot be considered as the controller since he merely consults the data for a purpose already defined and via indicated means. In this case, it is the service provider who is to be qualified as the controller for the personal information he provides. Indeed, he defines the means and purposes of the information he publishes on the Internet (display of personal information on the members of a gay association in order to be able to inform them of gay happenings, for example). If, however, the enquirer consults the data with a view to making a specific use of the data, if he proceeds to copy the data onto his own disk and to process it for purposes incompatible with the purposes for which the data was originally collected, then he may be considered as the controller[13] (recording of the same data with a view to stigmatising all homosexuals, for example).

A service provider on the Internet ought also to be qualified as the controller as regards the personal data he processes in order to render the service. Indeed he defines the data necessary for the service and defines the means and purposes of the processing (processing of the sender's name and address in order to send him solicited information or goods).

II. National law applicable

A particular difficulty can be raised with regard to the applicability of the Directive. Which activities, carried out in the context of a global network fall under the scope of the Directive and must respect its provisions as transposed by Member State laws?

The application of a law to a particular situation is usually determined by the nationality of the actors or the territory in which the facts occur. However, these criteria are no longer applicable in the cyberworld: the reality is transnational; information runs along wires and has no fixed location.

The Directive has adopted an interesting approach, taking into account up to a certain point, the developments in technology. The text no longer focuses on the old notion of 'a file' as mentioned in the original proposition of the Directive, based on a precise physical location of the data (on a floppy disc, or the hard disc of an identified computer,...), but rather concentrates on the concept of 'processing' of the data without the need for the data being necessarily extracted and assembled in a given spot. The geographical location of the data is no longer of interest in this case, and it is the controller of the processing who will determine the applicable law.

The controller must necessarily be established on a certain territory[14]. If this territory is that of a Member State, the national law of the State transposing the Directive will apply to the processing of data in the context of activities of the controller established in the Member State (article 4.1.a). If a Danish company opens an Internet site presenting its staff's personal details, it will need to comply with the Danish data protection law. If a Spanish hotel complex which offers a reservation system via Internet, requires the interested parties to introduce their personal data in order to book, the Spanish data protection law, in compliance with the directive, will apply to the processing of the data whether it relates to a French, Russian, American, or Japanese client.

In short, all the controllers established in the territory of the European Union will need to comply with the directive, as implemented by their national law when they process personal data.

Controllers established outside the territory of the Union are not, in principle, covered by the Directive. However, the European legislator does attempt to address the problem of the circumvention of the protection afforded by the Directive by the delocalization of the establishment of the controller. In order to avoid such a situation, the text of the Directive provides that a controller established outside the Union, but who for purposes of processing of personal data makes use of equipment, automated or not situated on the territory of a Member State, must comply with the data protection legislation of the said Member State (article 4.1.c.).

In the context of the Internet, such a solution initially appears impractical. It leads to the extension of the application of the Directive to every user of the Internet who collects personal data for a specific purpose from a data base or Web site located within the territory of the Union.

Indeed, according to the Directive, it is when one 'makes use', in order to process personal data, of equipment situated in a Member State, that the processing is subject to the law of the said Member State. Yet if it is quite clear that one makes use of equipment located on the territory of a Member State when one issues a questionnaire in a State in order to obtain personal data on consumer habits or when one questions the database of the central register of commerce of a country in

order to obtain the data relating to the members of a specific sector, it is not easy to locate the actual equipment which one makes use of in the context of the Internet.

The Internet is constituted by information which is not easily located geographically, even if the persons and sites are identified by 'addresses'. These addresses are in fact keys. The locks behind these keys are, however, not necessarily geographically stable. When an address appears on a closed network, the site can be 'lodged' anywhere on any computer linked to this network. In the context of a local company network, for example, the address of the site could correspond to a computer belonging to the director or to the computer consultant. If the internal network links together addresses dispersed throughout the world, the electronic address, could even correspond to a post in Singapore or in Venezuela.

In order to find the corresponding geographical location of a Web site, two solutions are proffered:

- Either to locate the actual machine, the computer which ensures the presence of the information on the given site. However, the information could be kept by an intermediary whom one has solicited in order to keep hold of the data one wishes to offer on the Internet. In this case, the electronic address corresponds to a mail box opened for the occasion, but does not reveal a direct link with the source of the information.

- Or to identify the person responsible for providing the information and to retain his location. Thus if a university produces on its own Web site, a bibliographical database of the works of its members, one would consider that the site is located where the university is established. This solution offers the advantage of being coherent with the criteria adopted by the Directive concerning the processing carried out by controllers located in the territory of the European Union.
  We must, however, underline that it is not always easy to determine the exact location of the information provider. Yet it is this location that determines the national law applicable and the country in which the controller will have to name a representative. How can one know to which country such – existing – addresses correspond: 105473.8880@compuserve.com or http//www.telepathic.com? And how could a person from Taiwan know whether the town of Gävle mentioned as the point of location of an information provider is situated in Sweden or in Estonia (or indeed whether Community law applies)?
  Furthermore, in order to locate forums or other exchange groups one should refer to the establishment of the controller of the forum.

Once the equipment has been located within the territory of the European Union, the Directive will apply as soon as the equipment is used in order to process personal data. As already mentioned, the term 'processing' of personal data as defined in Article 2.b. of the directive is very broad and covers a vast number of activities, each one of them could constitute the 'processing' of the data. The very copying of data corresponds to the collection of the data and is in itself a processing of personal data according to the Directive.

As a consequence, the person who, via the Internet, downloads personal data from a Web site opened by a service provider established on the territory of a Member State, processes the data by making use of equipment situated on the territory of a Member State. He will be qualified as the controller and in such a case, he must respect European legislation and name a representative.

This scenario is of course excessive.

The only way in which Article 4.1.c. may be effective is by giving it a teleological reading. The *ratio legis* of the article can be summarized as aimed at avoiding the circumvention of the protection afforded by the European Directive and, more generally, at avoiding situations where the data subjects are left without any protection[15]. The aim of the authors of the Directive is to ensure that the persons who should normally fall within the scope of the protection of the Directive, are effectively protected even when outside the European Union.

A rational solution to the problem of the applicability of the Directive can be deduced from the joint reading of Article 4.1.c and Articles 25 and 26 regulating transfer of personal data to third countries.

One can consider that a first solution to the preoccupation of the authors of the Directive is to be found in the system put into place as concerns the transfer of data to third countries (see below). In the context of the regulation of these transfers, the requirements laid down by the European Directive are to be respected by all the actors for the operations carried out on data originating in Europe. An adequate protection of the data sent outside the borders of the Union is required.

The dispositions of Article 4.1.c aim at covering situations in which data subjects are deprived, by an artificial manoeuvre, of the benefit of the protection afforded by the Directive and situations which fall outside the scope of any protection whatsoever, even that concerning transborder data flows. In this sense, two categories of situations fall, in our opinion, within the scope of article 4.1.c:

- firstly, the situation in which a controller deliberately seeks at avoiding the application of the Directive by delocalizing his establishment to a third country, whilst making use of equipment located within the territory of the Union in order to process personal data concerning data subjects located within the Union;

- secondly, the situation in which the transfer is exclusively carried out by a controller located in a third country. This is the case when data is collected through the use of cookies[16], without the data subject's awareness. Articles 25 and 26 will not apply in this case since the existing rules on the transfer of data to third countries only apply when the sender of the data is located on the territory of the European Union. One cannot qualify the person subject to cookies as the sender of data, since the operation is carried out without his knowledge. In order to fill in this gap in the protection afforded, article 4.1.c regains its full authority. It is the full regime of the protection afforded by the Directive which must apply to the processing of data obtained through the use of cookies, and not the more flexible regime of the transfer of data to third countries .

The principle criteria, therefore, which determines the applicability of the Directive to controllers situated outside the territory of the European Union must not be limited to the use of equipment on the territory of a Member State. This use is only one element in the analysis of the context in which the operations are carried out. A more global analysis must be carried out in order to determine that the controller is 'abnormally' established abroad even though his activities are mainly centred in Europe, or that one finds oneself in the presence of a situation lacking any protection whatsoever.

A German pharmaceutical company which establishes itself in Budapest and which collects data relating to medical prescriptions from a pharmaceutical network located within a Member State, in order to target European health professionals, is evidently trying to circumvent the provisions of the Directive and Article 4.1.c. should apply.

Similarly a company which collects data relating to the use of credit cards by Europeans in Europe (shopping in Paris, cinema in London, restaurant in Milan,....) and which sends the data to its subsidiary in the US in order to process it to obtain complete personal profiles of credit card users in Europe, should also fall under Article 4.1.c. The same is not true of an individual who, in order to obtain information necessary for his profession, accesses from the US a Web page issued by a provider situated within the Community[17].

III. Respect for the principles laid down in the Directive

A. The Purpose Limitation Principle:

- Personal data must be processed fairly and lawfully (Article 6).

'Fair' processing implies a maximum of openness. An individual's personal data cannot be processed for any hidden or occult reasons. The purposes behind the processing of the data must be explicit and clearly specified. Personal data may only be collected in a transparent way (this principle is guaranteed by the right of information. granted to the data subject in Articles 10 and 11).

In most cases the use of cookies is made without the knowledge of the person concerned not only as concerns the collection of the data, but also as concerns any further use of the data. In this case, therefore, the data is not being processed 'fairly'[18].

'Lawful' processing implies the respect of the national provisions taken in compliance with Chapter II of the Directive:

- Personal data must be processed for legitimate purposes

The purposes for which personal data are processed must be legitimate and must be determined at the time of collection of the data (Article 6.1 .b). The evaluation of the legitimacy of the purposes depends on the appreciation of the courts or of specialized data protection authorities.

It must be pointed out that in a same transmission of information, a number of different actors can intervene. Each one of them can be considered as pursuing a specific purpose for which he will be considered as the controller. For example, the access provider records data relating to the users of the network in order to bill the communication; the service provider records data in order to render the service and bill it accordingly. The control of the legitimacy and compatibility of the purpose must be assessed for each one of them:

- Personal data may not be further processed in a way incompatible with the purposes for which the data was collected.

As regards the services providing information on Internet, enquirers of a database will assume that the personal data that they may be requested to give when accessing the database, will be used only for purposes compatible with the nature of their enquiry. Any intended non-obvious use or disclosure will need to be displayed on the relevant screens so as to inform the data subject prior to his use of the Internet.

Given the access possibilities, the scale of the Internet and the 'public places' it offers (forums, newsgroups,..) the danger is that it will be impossible to control the reuse of the data by persons who have accessed them. How can one be sure that the data downloaded from the Net will be used in a way compatible with the initial purpose? If the secondary purpose is not compatible with the initial purpose, the processing must be considered as a new one and the data subject must be informed of the change. However, the link between the new data user and the data subject risks, in many cases, being too remote to enable the former to enter into contact with the data subject in order to allow him to control the reuse of his personal data. In the case, for example, of data collected from a bibliographical database or from a Web page giving the name and position of members of a company, it can be difficult to obtain data subjects' (E-mail) address so as to inform them. This situation could, however, be covered by Article 11.2. which specifically provides that the duty to inform the data subject when the data has not been obtained from him, will not apply when the provision of such information proves impossible or would involve a disproportionate effort.

In principle, user-related data may only be processed by the access provider in order to transmit the message and bill the transmission. Any further use (processing of data to obtain user profiles, for example) is not compatible with the initial purpose for which the data was collected. It may be done but it must be considered as a new processing and due information must be given to the data subject.

In the case of the provision of a service via the Internet, respondents could expect the use of any personal information supplied by them to be limited to the purposes indicated in the message (for example, please send me information about a new product); any further use would not be compatible with the initial purpose. A teleshopping service provider will collect personal data relating to his clients. He can use this data not only to render the service in itself, but also to establish personal profiles of his clients to target his clientele or to sell the data to a marketing company. In such a case, he will need to inform the data subject of the new purpose and ensure that this purpose is considered as legitimate in the eyes of the Directive.

B. Social justification Principle

Article 7 of the Directive lays down the grounds justifying the processing of personal data. These grounds correspond

to the circumstances considered by the European Community as allowing the processing of personal data. In order to be lawful, the processing of data must rely on one of these grounds, in addition to the fact that it must respect the obligations deriving from the legitimate purpose principle.

In respect of the use of the Internet three justifications laid down in Article 7 can more precisely be retained:

- "The data subject has unambiguously given his consent" (Article 7.a):

An enquirer making use of the Internet, whether to send an E-mail or in order to consult a database, and introducing his own personal data, could be considered as consenting to the processing of his personal data for this purpose. A member of a discussion forum on the Internet consents to the processing of his personal data necessary for the functioning of the forum when he applies to the forum (name, E-mail address, etc.).

The display of a third party's data on the Internet (for example, the display of the qualifications of the staff of a company), will require their individual and unambiguous consent (when signing their employment contract the employees could consent to the publicity of the directory), unless another ground can be invoked. Express written consent is not required.

The data subject's consent must in any event be freely given[19]: there should be no pressure on the individual to obtain this consent. The consent must also be informed, which means that service providers should inform each potential user of the Net unequivocally about the risks to his privacy (see below, to be informed). This enables the data subject to balance these risks against the expected benefits. Lastly, the consent must be specific, it must relate to particular uses of the data for specified purposes. Any modification of the purpose which is incompatible with the initial purpose, requires a new consent.

It must be repeated that the consent covers specified purposes, whereas an open network offers opportunities to access and reuse the available information for different and perhaps incompatible purposes. In many cases, it might be difficult to inform the data subject of the new purpose (because of lack of address or because of disproportionate efforts involved, for example). In addition, the data subject cannot guess all the virtual reuses of the data and he is not able to control the good-will of the reusers as concerns the respect of the directive. In many cases, the consent will not therefore have the significance it should have.

On the other hand, the interactivity characterizing networks offers a special interest as regards the consent. Instead of a consent given once and for all at the start of a series of operations, interactivity enables you to modulate your consent. A message can appear on the screen at different times announcing "if you want to go further, you must consent to give such or such information". You can accept part of the operations but refuse to give more data at a certain point of the processing, or for a certain part of the service offered. Moreover, you can accept certain reuses announced but not all: you can tick off the cases corresponding to the accepted or refused uses of your personal data. Opting-in or -out methods acquire an immediate and effective dimension through interactivity. The notion of consent can thus take a new meaning.

Free consent also implies that when a user is presented with a screen demanding personal data for further access, the fact that he refuses to go further should not be recorded or held against him.

- "Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (Article 7.b).

A user may be requested to introduce certain personal data in order to obtain a service (tele-shopping, hotel booking...). Only the data necessary for the performance of the contract may be processed. When one can do without personal data for the performance of a contract, one should not require it.

- "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are over-ridden by the interests or fundamental rights and freedoms of the data subject..." (Article 7.f).

This provision justifies the processing of personal data where it is in the legitimate interest of a natural or legal person, provided that the interests of the data subject are not over-ridden. This means that if the interest of a person in receiving personal data prevails over the data subject's interest not having his data communicated, data may be transferred. This is also true even when the data subject's interest in retaining his data is equivalent to the third party interest. It is only when the data subject's interest prevails, that the data relating to him may not be processed or communicated.

Article 7.f. is counterbalanced by the right for the data subject to object to the processing of data concerning him granted by Article 14 of the Directive. This provision states that Member States shall grant the data subject the right, at least in the cases referred to in Articles 7.e. and f., to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. In fact, Article 14.a. is only stating as a right which logically ensues from Article 7.f. Even if a Member State refuses to grant the right to object (as it is entitled to do by Article 14.a itself), the data subject will still be allowed to contest the balance of interests with regard to the Article 7.f. Doing so the data subject will object to the processing of his data by proving his over-riding interest, which is exactly what Article 14.a provides for.

On the other hand, regarding the justification of processing contained in Article 7.f, Article 14.b offers a real interest. This provision warrants unconditionally the right to object to the processing of personal data for marketing purposes. In this case there is no need for the data subject to prove a compelling and legitimate interest. This is a step further with regard to Article 7.f. It is a real counterbalance: the data subject who is not part of the initial weighing of interests can oppose himself to the processing without any justification, at the time when he learns of it. The disadvantage of not being consulted prior to the processing of the data is compensated by the possibility to object at any time without justification.

C. The Prohibition of Processing of Sensitive Data (Article 8)

Subject to a number of exceptions set out in Article 8.2, the processing, of certain categories of data is prohibited according to Article 8.1 of the Directive. This prohibition covers any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Any messages or databases containing such data, will therefore need to find grounds within Article 8.2. in order to be processed.

The data subject's explicit and informed consent is probably the safest course to follow when one decides to publish sensitive data relating to an individual on the Internet (Article 8.2.a). The other most obviously eligible ground to process sensitive data on the Net is when such data have been manifestly made public by the data subject (Article 8.2.e).

D. Data Quality

The Directive provides for certain requirements relating to the quality of personal data (Article 6):

- Personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed.

This provision refers to the concept of data compliance. A legitimate and specified purpose does not in itself authorize use of any data. The criteria of data adequacy are designed solely to ensure a necessary and sufficient link between the information and the purpose of the processing. For each finality, one must question whether or not there is a sufficient connection between the purpose and the data collected. Any irrelevant data must be discarded. For example, enquirers responding to an offer to post some marketing material who are asked to provide their name, address and telephone number, may consider the collection of the telephone number as excessive with regard to this response.

- Personal data must be accurate and, where necessary, kept up to date.

A provider displaying personal data must ensure that this data is accurate. It is recommended in this respect that the data subject is involved in the prior authorization of the publication of data on the Internet and that he is given the possibility to require that inaccurate data be modified (see below, right of rectification). The personal data must be kept up to date. This implies that it be reviewed on a regular basis. For example, the display of the qualifications of current staff implies that in the event of modifications in their status the data be modified accordingly.

- Personal data may only be kept for a certain period.

Personal data may only be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected and/or for which they are further processed. The data introduced by the user of the network in order to obtain a service, may only be kept for the period necessary in order to render the service and may not be stored beyond that period.

It is up to the controller to ensure that the principles governing data quality are complied with. If one qualifies the person from whom the message originates and who is providing the information as the controller, he will need to ensure the quality of the data. However, it is reasonable to say that he can only be responsible for the data at the time when he introduces the data into the network.

III. Rights of the data subject

The Directive grants a number of rights to the data subject. These must be guaranteed by the controller (or his representative, if any).

A. Right to be informed (Articles 10 and 11)

There are two particular occasions when the controller must provide information to the data subject. The first is at the time of collection of personal data (Article 10). The data subject must be informed at least of:

a) the identity of the controller (and his representative, if any),
b) the purpose or purposes of the processing for which the data are intended.

Further information must also be provided if "necessary in the specific circumstances to ensure a fair processing in respect of the data subject". Such information includes: the recipients or categories of recipients of the data, whether replies to questions are obligatory or voluntary and the possible consequences of failure to reply, and the existence of the data subject's right of access to and the right to rectify the data concerning him.

The second occasion when information must be provided to the data subject is where the data have not been directly obtained from the data subject. According to Article 11, he must be informed at the time the data are recorded or, if a disclosure to a third party is envisaged, no later than at the time when the data are first disclosed.

If personal data on users of a service are collected it must be clear to them who is to use the data and what are the purposes for which the data are to be used or disclosed. The display of personal data relating to individuals who are not party to the exchange (e.g. the qualifications of certain staff, the members of a club,...) must be preceded by adequate information of the data subject. This information could take place at the time when the data is collected from the individual.

It must be pointed out that the features of a network facilitate the provision of information. In the hypothesis of data collected from the data subject, a message can appear on the screen at the beginning of the operations, providing the users with the mandatory information. In the case of data not obtained directly from the data subject, for example when one copies and processes the names and addresses of members of a forum, the network offers such technical possibilities that warning electronically all these persons of the secondary use of their personal data proves to be much less time and money consuming than in a 'classical' environment.

The data subject must be informed of the identity of the recipients or categories of recipients. The 'recipient' is defined in Article 2.g. of the Directive as *any* person to

whom the data are disclosed whether a processor (person processing data on behalf of the controller), third party (any person other than the data subject, the controller, the processor and persons who under the direct authority of the controller or processor, are authorized to process the data), a person in a third country,.... Since the use of the Internet involves a number of actors to whom the data are disclosed (telecommunication organization, access provider,...), the controller may be requested to provide information as to the identity of these persons to the data subject if deemed necessary in order to guarantee 'fair processing' of the data.

The text of the Directive does not provide any indication as to what particular circumstances justify additional information being given to guarantee a 'fair processing' of the data in respect to the data subject. Articles 10 and 11 merely state that the additional information must be given "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect to the data subject". The concept of 'fair processing', seems to refer to the requirement of transparency laid down in Article 6. 1 .b.

One situation which could correspond to these 'particular circumstances' is when data are intended to be transferred to controllers located outside the European Community. The specific hypothesis of sending the data outside the protected geographical area calls for better informing the data subject in view of the greater risk the processing presents. The problem is that in the context of open networks, knowing precisely who (or which category of persons) accesses or will access the available information turns out to be rather difficult if not impossible. Another situation in which further information must be given, could be the case of the use of cookies. Because their use is not always apparent to the data subject, the controller could be required to warn the data subject of their presence.

Even though the telecommunication service or access service do not actually process the personal data contained in the message as such (see above), they inevitably know from whom the message originates, to whom it is sent and the time of transmission. This information is not only considered as personal data in the eyes of the directive, it has also been qualified by the European Court of Justice as part of the message to be protected under Article 8 of the European Convention of Human Rights[20]. Information regarding the identity of the telecommunication service or access service could therefore be required.

In a discussion forum on the Internet, the members of the forum could be informed of the categories of recipients to whom the data are transmitted, unless this information can be deduced from the purpose of the forum itself: an individual who is a member of a discussion forum on data protection, for example, could assume that his personal data is communicated to all persons interested by data protection questions (data protection authorities, researchers in the domain, privacy advocates...).

Article 11.2 provides for a derogation to the duty to inform the data subject where "in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort". A person who has collected information from a database on the Internet and not directly from the data subject himself, could make use of this provision. Indeed since he is not in direct contact with the data subject, it will be burdensome for him to provide the latter with the necessary information. This does not mean that the controller will not need to respect the principles laid down in the Directive (the purpose must be legitimate, the data must be relevant...). It does, however, mean that the control by the data subject of the use of his data will be considerably reduced. How will he be able to track his data in order to access it, if he is not informed of the persons in possession of his data? If the exception is understandable in the context of historical or scientific research, is there not a danger that use of the article in the context of the Internet becomes a gateway to the loss of control on the use of his data for the data subject?

B. Right of Access (Article 12)

The Directive grants every data subject the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense, confirmation as to whether or not data relating to him are being processed and information, at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed.

The data subject may also obtain communication to him in an intelligible form of the data undergoing processing and any 'available' information as to their sources. This last part of the obligation is an innovation of the Directive in comparison with most of the national laws existing in the Member States.

The person considered as the controller in an Internet network will only be able to grant the data subject access and information as to the data he processes himself and of which he is still in control. A service provider who displays data relating to his current staff, for example, will be requested to erase the data if the individual concerned is no longer a member of his staff. However, he will only be responsible as regards the display of data he provides and any use that another person makes of the data is beyond his control.

In the context of open networks, the controller will not always be in a position to provide information as to the sources of the data (he may have found personal data on the Internet without any revelation as to the sources of the data). He will be dispensed from giving this information since it will not be 'available'.

Exemptions or limitations to the right of access can be foreseen by the Member States in order to protect notably public safety, the investigation of criminal offences or the protection of the rights and freedoms of others (Article 13.1).

C. Right of rectification (Article 12.2)

Following on from the right of access, the data subject is granted, as appropriate, the right to obtain the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data. It is up to the controller to ensure that this right is guaranteed. In the context of an open network, the controller will only be able to provide this right with regard to the data which he has access to.

The Directive further provides that the controller must notify to the third parties to whom the data have been disclosed of any rectification, erasure or blocking of the data, unless this proves impossible or involves a disproportionate effort. In the context of open networks, where the person providing information is not always in the best position to know who has accessed the data he displays, the notification to these persons of any modifications could in effect prove difficult.

D. Right to Object (Article 14)

As already mentioned above, the data subject is granted the right to object on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided for by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve these data.

This right to object is granted unconditionally as regards the processing of personal data for marketing purposes (see above).

IV. The controllers' obligations and liabilities

A. Security (Article 17)

According to Article 17 of the Directive, the controller is required to put into place the measures so as to avoid any accidental or unlawful destruction, loss or alteration, against any unauthorized disclosure or access and against any other forms of unlawful processing[21]. The rationale of this Article is that the potential danger to the data subject's right of privacy does not only emanate from the controller, who collects, stores, processes and discloses the data for his own purpose, but is also jeopardized if the data subject's data are misused by third parties who have gained access to it, whether authorized (by a processor under the instructions of the controller, for example) or unauthorized.

The security measures can be organisational (designation of a 'security officer', documents handed out to the staff with precise security measures to be respected,...) or technical (computers kept under lock and key or in specially protected areas, introduction of access codes, encryption of certain documents, ...). It is left up to the controller to adopt the necessary measures. The measures are the result of the equation of three variables: the risks of the processing, the nature of the data and the state of the art and cost of implementation of the measures.

The controller will therefore need to assess the risks involved in the processing of the data via the Internet. Several security problems are associated with the Internet; giving anybody in the world access to your computers is a danger in itself. In reality, however, the problems associated with securing the Internet do not differ from those of any other network, except of course that anybody can access it and consequently it is probably correct to assume that the Internet is fundamentally insecure.

The introduction of computers and networks increase the risks, notably the threat of access to the data by unauthorized persons and the unauthorized use of the data by authorized users. Computerization implies standardization of information in both content and format. Content standardization enables secondary users to anticipate the nature of the information and its uses. Furthermore computerization and networks implies the possibility of linkages[22] and the creation of very complete personal profiles.

Account must be taken of the nature of the data. Processing of sensitive data (medical data, for example) will imply the requirement of a higher level of protection.

The security measures adopted will also be dependent on the state of the art and the cost of their implementation. This provision implies that the controller is under the positive obligation to keep himself informed of the new security measures available and to ensure that the level of security is adequate vis a vis the 'state of the art' unless they are prohibitively expensive. A controller could be well advised to have proof that all the decisions relating to security of personal data were founded on professional expertise.

The controller will be required to take such measures either only to allow the transmission of certain kinds of data, or to add security features to the network such as codification of the message. When able to avoid it, data which identifies a person should not be used. In such a case the data should be anonymized. This can be done by using a physical device (e.g. an encryption algorithm held on a smart-card) or a function (e.g. supervised by a trusted third party who holds the true identity). Similarly, E-mail addresses on the Internet could take the form of pseudo-identities (an alternate identity), with real identities only being used in exceptional cases. Before connecting a local computer network (e.g. the network of the company) to the Internet he could also assess the risks for the security of the local network and the personal data it stores. This could result in the setting up of technical measures in order to prevent access to the local network outside predetermined limits (setting up of a 'firewall', for example)[23].

B. Notification (Article 18)

The controller has a last obligation which is that of notification of the processing to a supervisory authority. A notification is only due for automated processing. This obligation is thus pertinent for network use. But the idea is to largely exempt controllers and to reserve the notification procedure for special categories of processing.

C. Liability (Article 23)

The Directive provides every person with a right to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question. In addition, any person who has suffered a damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

The number of actors involved in the transmission of personal data via the Net, may give rise to certain difficulties when trying to assess who is responsible for not respecting the principles of the Directive, notably in the event of an unauthorized disclosure of the data to a third party. Transparency in the network infrastructure can have the effect of obscuring responsibility for personal information.

V. Transfer of Personal Data to Third Countries (Articles 25 and 26)

The Internet facilitates the quick transmission of great quantities of information to any other computer system connected to the network. Personal data can be communicated to countries without any data protection where they can be accessed from all over the world.

The Directive envisages the question of the transfer of personal data to countries outside the European Union in articles 25 and 26. The aim of the Directive is double: firstly, the efforts put into place to afford a level of protection within the Union would be useless if one could circumvent it by transferring the data to a country offering no guarantees to the data subject. Secondly, the free movement of personal data within the Union supposes that the Member States adopt common rules as regards the flows of data outside the Union. The Directive, therefore, provides for a regime prohibiting the transfers to countries which do not offer an adequate level of protection.

Article 25: The Principles

Article 25.1 provides that transfers of personal data to third countries may only take place if, on the one hand, the transfer complies with the national provisions adopted pursuant to the Directive and if the country of destination ensures an adequate level of protection.

The notion of 'adequate' protection is to be linked to the degree of risk a transfer presents. When envisaging the transfer of a list of sexual delinquents to a social association or a list of the members of a political party to a direct marketing company, one must be severe in assessing the adequacy of the protection offered abroad. If, on the other hand, data such as name, position and length of service of employees are sent from the subsidiary company to the parent company, the level of protection will be more easily satisfactory.

The notion of adequacy calls for a functional approach. It implies a search for the fundamental elements of the protection and not a will to export the European legislative model. The protection must be adequately afforded, whatever the form it takes. Specific data protection legislation is not the sole instrument to take into account. For example, the rules governing medical secrecy can be retained as a part of the protection structure.

The adequacy of the level of protection shall be assessed in the light of all the circumstances surrounding the transfer operations. To measure the degree of danger the flow presents, consideration will be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination. Furthermore, in order to assess the level of protection afforded in the third country, one will take into account the rules of law, both general and sectoral in force in the third country in question and the professional rules and security measures which are complied with in that country (Article 25.2).

Open networks such as the Internet pose a particular problem with regard to the European transborder data flows policy.

The Internet is the scene of active and passive transborder flows. Active transborder flows mean conscious flows, decided, spontaneously or on request, by the data subject himself or by the controller. For example a Belgian citizen gives his name and address to a Canadian service provider, an Italian bank transfers information to the USA in order to make a payment for its customer, a subsidiary company sends the personnel file to the head office located in Japan, a French service provider sells his clientele file to a Norwegian marketing company,... Active flows also cover hidden flows. These concern the 'user's data', the electronic trace left when using the Net, already mentioned above, and also the data discretely collected by cookies. Flows can also be passive, that is to say that the data is made available on a site and is liable to be accessed by anyone located anywhere, copied and by this fact transferred to any third country. Flows are passive in the sense that they are potential.

The evaluation of the level of protection afforded by the third country must take place prior to the flow:

- In presence of a conscious active flow, the assessment of the protection is not specific to the use of a network rather than other means of transfer. As in a classical environment, one intends to send data to a given country and consequently evaluates the protection this country offers to personal data.
  Most of the time, this hypothesis corresponds to one of the exceptions admitted by Article 26.1 examined below: either the data subject gives his unambiguous consent to the transfer, or the flow is necessary for the performance of a contract between the data subject and the sender of the data or concluded in the interest of the data subject between the controller and a third party. However, in the first case one must be sure that the consent is freely given and fully informed. This means that the data subject must have knowledge of the country to which his data are sent and of the fact that this country does not offer an adequate level of protection. Let's recall that the real difficulty that sometimes appears is to determine to which country one really sends the data (because of non-revealing Web site or E-mail addresses as illustrated above). In the case of a contract between the data subject and the sender of the data, one must control the real necessity of the transfer.
- As concerns hidden flows, one has to distinguish two hypotheses. The first one concerns the category of hidden flows deriving from cookies. Cookies can operate a discrete collection of data in Europe. This means that a flow of data occurs, but because the data subject ignores it he cannot be considered as the sender of the data. As a consequence, this operation is to be defined not as a transfer, but as a collection made by the recipient of the data. As the controller of the processing (collecting data corresponds to a processing) is established outside Europe, but makes use of equipment situated on the territory of a Member State (when visiting the system of the data subject), Article 4.1.c will apply to the processing[24]. The controller must therefore comply with all the rules provided for in the Directive. Notably, since the Community text prohibits occult processing of data, the controller will have to inform the data subject of the processing he operates on the data.
  The second hypothesis concerns the electronic trace left

when visiting a Web site. Even if this trace is convertible into personal data, it is not to be considered as a transfer since the data subject remains unaware of the flow of his personal information. If the controller located outside Europe processes this data, Articles 25 and 26 will not apply and, in this case, Article 4.1.c will not apply either since the controller is liable to argue that he does not need to "make use of equipment situated on the territory of a Member State" to obtain such data: he only records the data arriving at his site. The data subject is thus left without any protection as concerns the trace he leaves behind. So the only solution in this case is to warn users of the risks of processing beyond their knowledge.

- Finally, as concerns passive flows the obligation to evaluate the foreign protection prior to the flow means that such an evaluation must be done in advance for all connected countries since every country is a potential destination for the information available on the Net. If a country does not offer an adequate protection for personal data, access to the data should be refused to this country, or at least the possibility of downloading the data or transferring it in any other way. One sees in the context of the Internet, the practical difficulty raised if one attempts to respect the provision of the Directive as regards transborder data flows to third countries.
  The difficulty is even more serious when one considers the type of evaluation required by the Directive. The adequacy of the level of protection must be assessed on a case-by-case basis, keeping in mind all circumstances surrounding a given flow. Article 25.2 does not provide for general statements[25]. A third country can be considered as satisfying the conditions as concerns the financial sector or the research activities sector because of specific sectoral legislation or codes of conduct, for example, and at the same time this country can happen not to satisfy the criteria as concerns the medical or marketing sectors.

Article 26: Exceptions

By way of derogation from the prohibition enacted in Article 25, Article 26 lays down a number of derogations enabling the transfer of personal data to countries which do not provide for an adequate level of protection. Thus the transfer may take place if the data subject has given his unambiguous consent to the proposed transfer (the consent must be freely given, specific and informed – see above); if necessary for the performance of a contract or if necessary to protect the vital interests of the data subject.

The transfer of personal data via the Internet to a third country could take place with the consent of the data subject when publicizing data concerning him abroad. He must, however, be made fully aware that his data will be transferred to a country which does not afford adequate protection and of the risks that this could imply.

Transfer of personal data could also take place if necessary for a contract to which the data subject is party (an individual ordering goods in a third country for example, will imply the transfer of the necessary data to provide the goods to him: name, address, credit card number...). Only that data necessary for the performance of the contract must be transmitted. Furthermore, the data subject should be made aware that once the data has been transferred to the third country for the contract in question, there are no means of ensuring that the data will not be further used for other purposes (sold to a marketing company, for example, or used by the controller to establish personal profiles).

Transfer of data may also occur if it is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party. This is notably the case when a travel agency makes a hotel reservation in the context of a holiday booking for one of its clients.

According to Article 26.2., the transfer of personal data may also take place if the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals notably through the use of contractual clauses. Even if it is true that contractual solutions could be a way of affording a certain level of protection to the data subject, they could be problematic in complex information processing networks such as the Internet with multiple parties involved especially in jurisdictions where the individuals concerned do not have legal rights against third parties.

Looking beyond the Directive...

It is apparent from this study, that a number of loopholes are left by the Directive with regard to the protection of personal data in open networks, notably concerning the possibility of guaranteeing the effective enforcement of the rights granted to the data subjects. This lacunae seems to be recognized in the Directive by the powers granted to the Commission to make proposals for amendments with regard to the implementation of the Directive: the Commission shall examine, in particular, the application of the Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary taking into account the developments in information technology and in the light of the state of progress in the information society[26].

Furthermore, the scope of the protection afforded by the Directive is limited to a European level. Even if European standards are harmonized, it is unlikely that the same standards will be adopted around the world. It is clear that Internet involves the transmission of personal data that this creates dangers for the individual's right to privacy beyond the frontiers of the Union.

The elaboration of codes of conduct at different levels (G7, OECD, International Chamber of Commerce...) must not be under-estimated as contributing to protecting personal data within open networks. The European Directive itself calls for the drawing up of codes of conduct which should be encouraged by the Member States and the Commission (Article 27). It must be pointed out that codes of conduct offer the advantage of going beyond the European Union. Furthermore, they offer flexible and adequate solutions to the problems created by an ever changing technology. All our problems are not solved however... codes of conduct may not offer a level of protection considered as 'adequate' in the eyes of Article 25 and following of the Directive enabling the transfer of personal data beyond the boundaries of the Union. Furthermore, codes of conduct do not guarantee effective protection: there is no way of ensuring that they will be

effectively respected. Furthermore, codes of conduct are often unilateral, rather than the result of negotiated consensus between the concerned actors.

In practice, it must not be forgotten that important and effective rules are being imposed by the users of the Internet themselves (e.g. 'Netiquette'). The advantages of self-regulation must not be disregarded. Self-regulation could have an important role to play notably in creating an awareness among the users of the Internet as to the importance of confidentiality of their data and the lack of protection in the network.

Self-regulation could be a means for the users of the Net to discuss and develop adequate protection measures which reflect current technological developments and incorporate new technological safeguards for privacy protection. Such measures would build on the specific experience of the Internet users. The policies adopted could be disseminated easily and quickly to the Internet users and service providers. The Internet in itself could be a way of providing information as to the recommendations adopted.

Cécile de Terwangne
Sophie Louveaux
Centre de Recherches Informatique et Droit, University of Namur, Belgique.

Footnotes

[1]See "Data Protection on the Internet: Report and Guidance", adopted at the 20th meeting of the International Working Group on Data Protection in Telecommunications in Berlin, 19 November 1996.

[2]On anonymity in networks see "Privacy enhancing technologies, the path to anonymity", Registratiekamer, The Netherlands & Information and Privacy Commissionner / Ontario, Canada, August 1995. On security and technological solutions (such as PICS, secure-viewing,...) see Joel Reidenberg, "Governing Networks and Cyberspace rule-making", 45 *Emory Law Journal*, 1996.

[3]Reference in this article is only made to the 'general' directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data rather than to sector specific directives such as the directive (still to be adopted) concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in integrated services digital network (ISDN) and in the public digital mobile networks.

[4]EU Directive 95/46, O.J., 23.11.95, L 281/31.

[5]Recitals 14 and 15.

[6]For a definition of the access provider see part "C. Controller".

[7]26 of the Directives' recitals.

[8]In the broad sense of the term. 'Use' of data is included as such in the list of operations enumerated in Article 2.b.

[9]Article 2.b. defining the processing of personal data, includes as processing of personal data, the mere collection or consultation of the data.

[10]The controller is also responsible for ensuring compliance with the provisions on data quality set out in Paragraph I of Article 6. The controller must also ensure compliance with the obligation to inform the data subject, thus enabling him to effectively exercise his rights. Furthermore, the controller (or his representative) has the obligation to notify the supervisory authority pursuant to Article 18.

[11]Commentary on Amended proposal COM (92) 422 final - SYN 287, p. 10.

[12]See "Data Protection on the Internet: Report and Guidance", op. cit.

[13]In this case. the processing can be considered as having occurred as from the moment of consultation of the data (see definition of 'processing' which includes the consultation in the operations which constitute the processing of personal data).

[14]According to 19 of the recitals, "the establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements", the legal form of such an establishment (branch or subsidiary,....) is not a determining factor.

[15]See Recitals 20 of the directive "Whereas the fact that the processing of the data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided tor in this directive;..." and the Explanatory Memorandum" (Article 4) lays down the connecting factors which determine which national law is applicable to processing within the scope of tne Directive in order to avoid two possibilities: – that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this;(...). COM (92) 422 tinal - SYN 287, 15 October 1992, p. 13.

[16]Cookie is a Netscape feature that assists providers in tracking users activities at Web sites. It enables the retrieval of information stored on the computer of the Internet user, most of the time without his knowledge.

[17]The rules governing transborder data flows will apply in this case (see Chapter V on the transfer of personal data to third countries).

[18]The latest version of the Netscape browser (Netscape 3) proposes an option that can be activated to refuse the entry of any hidden cookie.

[19]The data subject's consent is defined in Article 2.h. of the Directive as "any freely given specific and infonned indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

[20]Article 8.1. of the European Convention of Human Rights: "Everyone has the right to respect for his private and family life, his home and his correspondence". See Malone Case, 2 August 1984, Series A, n82 & 84, (1984), pp.3 1-36.

[21]'Unlawful' processing covers any processing of personal data which does not respect the national provisions adopted in accordance with the Directive. This would be the case, for example, if a controller did not provide for instructions enabling his staff to process the data (see Article 16). 'Unauthorized' processing or destruction covers the cases when the controller does provide for such instructions. but staff process or intentionally destroy the data without the controller's permission. 'Unauthorized' access covers the cases of interferences by third parties to data which they should not have access to.

[22]By 'linkages' we mean the possibility of interconnecting different computer systems enabling them to interact effectively.

[23]On the security in networks see "Privacy enhancing technologies, the path to anonymity", Registratiekamer, ibid.

[24]See above our reading of Article 4.1 .c of the Directive.

[25]Articles 25 (4) and (6), however, provide that the Commission can "find (...) that a third country (does or) does not ensure an adequate level of protection ..."

[26]Article 33.2 of the Directive.