

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Data protection and online networks

Louveaux, Sophie; de Terwangne , Cécile

Published in:
MultiMedia und Recht

Publication date:
1998

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

[Link to publication](#)

Citation for pulished version (HARVARD):

Louveaux, S & de Terwangne , C 1998, 'Data protection and online networks', *MultiMedia und Recht*, no. 9, pp. 451-458.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

CÉCILE DE TERWANGNE/SOPHIE LOUVEAUX

Data Protection and Online Networks

Der vorliegende Artikel möchte nicht die Gesamtheit des von der Richtlinie vorgesehenen Schutzsystems vorstellen. Er möchte vielmehr die spezifische Frage der Anwendung dieses europäischen Textes im Rahmen des Internet beleuchten. Zu diesem Zwecke wird vor allem auf zwei Punkte näher eingegangen: Zuerst wird die The-

matik der materiellen Anwendung der Richtlinie diskutiert. Dies führt dazu, die wesentlichen Definitionen der Richtlinie in den Kontext des Internet zu setzen. Anschließend wird die territoriale Anwendung der Richtlinie sowie die hiermit untrennbar verbundene Problematik der grenzüberschreitenden Datenflüsse behandelt.

1. 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 realize 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 is more, the security concern is increased by the fact that multimedia technologies offer higher risks of distortion of reality. Digitalization enables 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 rela-

ted 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, the user 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, etc.), information will be recorded as to the timing of the message, the length of time of the communication, etc.

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, etc.

Three types of approaches can be envisaged. The first is given by security technologies;¹ the second comes from ano-

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, 19.11.1997.

nymity (encryption and privacy enhancing technologies) and a third 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.

II. Protection afforded by the European Directive

The European Directive³ on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁴ was adopted on 24.10.1995. 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 24.10.1998).

1. 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 to online networks 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 etc., 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 provider⁶ 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, etc. 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 use⁸ 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

2) On anonymity in networks see "Privacy enhancing technologies, the path to anonymity", Registratiekamer, The Netherlands & Information and Privacy Commissioner/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 "II.1 c) Controller".

7) 26 of the Directive 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.

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 the user 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 ma-

terial 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 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, databases, etc.);
- Service providers offer their services to users via the Net (banks, travel agents, etc.);
- 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

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 1 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.

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 centralizing 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).

A service provider on the Internet is to be qualified as the controller for the personal information he provides. He 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).

2. 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 neces-

sarily 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 a room, 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 at first sight 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

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.

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 if 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 the 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 to avoid 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 if 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 principal 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

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 for 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 the 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 final – 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.

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, etc.) 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

3. 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.

a) 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, etc. 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 us recall that the real difficulty that sometimes appears is to determine to which country one really sends the data (because of nonrevealing 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 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

17) The rules governing transborder data flows will apply in this case (see below).

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.

b) 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 etc.). 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.

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 ...“