Some Preliminary Comments on the DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (*)

Herbert Burkert (**)

Table of contents:

1.What is a directive?

The Directive was passed October 24, 1995, almost exactly five years after the initiating proposal of the Commission had been published.

A directive is binding on the Member States as to the results it seeks to achieve, leaving discretion to the Member States as to how to achieve these goals, usually by national legislation. This does not exclude that directives can be very precise also as to the means and thus prescribing the contents of national in rather a detailed manner. The Directive on data protection is such a fairly precise directive. It had to be since one the goals it set out to achieve was to abolish restrictions on transborder data flows of personal data within the Community. To achieve this goal on a high level of protection required to keep national derogations at a minimum.

The Directive is addressed at the Member States (Art.34). They have three years to adapt their legislation (Art.32.1.) or in the case of Italy and Greece to have such legislation for the first time. There is another three year period starting with the entry into force of the new or adapted national legislation within which data processing already under way has to be brought under these new regulations (Art.32.2.) There special adaptation regulations for manual files in as far as they are covered by the Directive at all (cf. below - application area)(Art.32.2. 2nd paragraph).

The question - however interesting - as to what extent the Directive may be directly applicable will most likely remain a theoretical one. There are two types of direct applicability. The vertical direct effect gives a citizen the right to sue the government in a national court forcing it to apply the regulations of a directive in as far as they can be applied to state bodies at all; the horizontal direct effect would allow to sue another (private) party in the national court to obey the obligation set down for that party in the Directive. The former principle is fairly settled in Community Law; the latter is still somewhat controversial. In general, however, the question of direct applicability can only be raised after the time limit for transformation has expired. In addition other requirements have to be met. One of these requirement is that the directive has to be fairly precise. It should in fact be possible to read it as a national law. With regard to most of the regulations of the Directive this requirement indeed would be met. Also incomplete transformations can be challenged directly in the national courts who would refer this question to the European Court of Justice (ECJ).

In addition to incompleteness citizens can challenge, in their national courts, *measures* based on national law transforming the directive on the grounds that the national law is not in conformity with the directive. This interpretation is in the sole competence of the *national court*. The national court, however, may and under certain circumstances has to refer the question to the ECJ whether such a measure (not the national law - this interpretation is solely up to the national court) is in conformity with the directive. Citizens cannot challenge a national measure or a national law *directly* at the *ECJ* for not being in conformity with the directive.

modes

The regulations of the directive, unless, of course, they address directly the Commission, are directed at the Member States. They do this in two modes; either the Member States are obliged to transform the regulation into national law, the <<shall>> - mode. Most of the regulations in the directive are obligatory (cf. <<Member

States shall provide ..., ... shall grant ..., ... shall specify ..., ... shall determine ..., shall take measures .., shall contain ... >>). Some of the regulations of the directive leave discretion to the Member States on what and how to regulate - the <<may>>-mode (cf. <<may ... lay down).

In the interest of brevity in the following text we will not repeat at each instance that the regulations are all addressed at the Member States. The reader should keep this in mind. Also all regulations cited are mandatory except specifically mentioned otherwise.

2. Contents analysis

2.1 Introductory remarks

2.1.1 Special characteristics of the Directive

pieces from national legislation

To those familiar with existing national data protection regulations in the Member States of the European Union it becomes immediately obvious when reading the Directive that it tries to incorporate various specific traits of national legislations or at least to not disavow what has been reached and developed on the national level.

One such example is the unique German model of the internal <<data protection responsible>> a person that has to be nominated by companies above a certain size handling personal information. This person supervises the application of the national law within the company and acts as a contact with the external supervisory authority; the position enjoys certain safeguards within the company structure. If the Directive would no longer have provided for this solution as it was feared at some stage in the drafting process - national transforming legislation would most likely have done away with this position which in the eyes of the data protection authorities and of many observers in Germany had proved to be rather useful. The Directive now even includes an incentive to have such position of a <<personal data protection official>>: If such a person is appointed according to national law, national law may provide for simplification or exemptions from the obligation to notify the supervisory authority (Art. 18 - cf. also below). Other examples are the limitations put on automatic decision making processes (Art.15) that featured prominently in the French data protection law or the reference to Codes of Conduct (Art.27) which has been taken from the Dutch law.

a document of political compromise

Most of all, however, it should be noted that the Directive is a document of a political compromise which means that the document still contains a lot of tensions. The strongest tension results, of course, from the

underlying structural problem of the European Union, a construct torn between market orientation and aspirations of political unity. Other sources of tension with regard to the Directive were differences of interest among the various Community bodies, between these bodies and the Member States, among the Member States, within the Member States and their data protection authorities, among the data protection authorities, all this under the barrage of various industry lobbying groups within and from outside the Community. Many of these conflicts were shifted off into the recitals so as not to <<pollute>> the regulations but the full reach of the Directive can only be understood reading these recitals with the main body of the Directive.

Due to the principle of functional and teleological interpretation in Community law in the case of eventual legal interpretation by the European Court of Justice these recitals will regain their importance in as far as they give indications of the functions and the goals of the regulations.

2.1.2 Exemptions

The Directive contains two types of exemptions: Some of the regulations allow Member States to derogate. This is the <<may>>-mode mentioned above, which can be regarded as an exemption to the binding character of the Directive in general. Usually such derogations are allowed for establishing exemptions from the Directive in national law. These are the exemptions proper. Such exemptions usually modify procedures and/or the rights of the data subjects. To avoid that the power to derogate ends up in a too liberal use of exemptions by the Member States in their national laws thus endangering the high level of protection intended by the Directive, such exemptions are usually still required to contain suitable provisions or measures for safeguarding privacy interests, so as to ensure that such exemptions are being kept to a minimum and do not contradict the spirit of the Directive (cf. Art.8.4, 8.5, 15.2.a., 32.3). At some instances invoking such an exemption in national legislation is linked to an explicit duty to inform the Commission (cf. Art.8.6.).

2.1.3 Interpretation

As in current national data protection laws the Directive contains numerous notions like <<public interest>>, <<legitimate interests>>, <<interests for fundamental rights and freedoms>>. These notions do not add to the clarity of the text, but they help to adjust to situations that cannot be clearly predicted or clearly defined in advance. In the application process national supervisory authorities, national courts, eventually the European Court of Justice, the Commission, and all the other institutions created in the context of the Directive will add material, in their comments, decisions and policies, to clarify these notions and to create typologies that help to make the rules more predictable in their application.

2.2 Analysis

Data protection regulations, and the Directive is no exemption, can best be analysed if an inherent general structure is clarified and then used to organise the regulations around this structure. As elements of such a general structure I suggest the following:

- apl elements and focuses on two selected legal-political problems that may arise in the context of transborder data flows. It closes with a preliminary remark of evaluation.

area,

- obligations of the data controller,

- rights of the data subject,

- institutions of supervision and co-operation,

- regulations concerning transnational data flows,

- any other accompanying regulations not covered by the above.

2.2.1 Application area

types of processing

The Directive is applicable to electronic data processing and manual processing of personal data in as far as personal data form or are going to form part of a filing system (Art.3.1.).

personal data

The Directive is applicable to data relating to natural persons; personal data being <<any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; >> (Art.2.a.).

private/public sector

The Directive is applicable to the private and the public sector. In fact, the Directive no longer differentiates between both sectors but defines the application area negatively: The Directive does not cover activities outside the scope of Community law (in particular data relating to State security matters) and it does not cover processing <<by a natural person in the course of a purely personal or household activity.>> (Art.3.2. second paragraph).

2.2.2 Obligations of the controller

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>> (Art.2.d.).

The controller has material and procedural obligations:

2.2.2.1 Material obligations of the controller

Material obligations can be divided into general material obligations that apply to all kinds of processing of personal data and specific obligation that occur with special types of data collections.

2.2.2.1.1 General material obligations

Data may be processed only if there is a legitimate reason, and the processing has to follow the principles relating to data quality.

legitimacy

The legitimacy of data processing may be based on consent (Art.7.a.), on a contract or a pre-contractual relationships (Art.7.b.), on legal obligations (Art.7.c.). It may also be legitimate, if required by the vital interest of the data subject (Art.7.d.), or if the controller or the third party receiving the data have to carry out the processing in order to fulfil a task in the public interest (Art.7.e.). Finally processing may also be legitimate (and this is a classical example for a balancing clause that provides an entrance door to adaptive interpretation as mentioned above): if the <<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 overridden by the interests for fundamental rights and freedoms of the data subject which require protection...>> (Art.7.f.).

data quality principles

In as far as the processing is legitimate it has to follow certain principles that ensure that the quality of the data is being guaranteed. The controller has to make sure that the following principles are being observed: the processing has to be fair and lawful (Art.6.1.a.); that it is bound by the purpose (finality) principle (Art.6.1.b. and e); that it is adequate, relevant and not excessive in relation to that purpose (Art.6.1.c.). Data have to be accurate and timely (Art.6.1.d.) and should not be kept longer than necessary, with the Member States having the opportunity to pass special regulations concerning data of historical, statistical or scientific use (Art.6.1.e.).

exemptions to the data quality principles

The application of these data quality principles in Art.6.1. may, however, be restricted in the public interest by legislative measures in as far as such a restriction is a necessary measure to safeguard <<national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions, an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters, a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority>>. Further restrictions are possible to safeguard <<the protection of the data subject or of the rights and freedoms of others>> (Art.13.1.).

So not only are certain areas totally excluded from the application of the Directive such as <<processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law, ..>> (Art.3.1.- cf. above) but for the same interests the application of the general principles of data quality in areas that *are* covered by the Directive might be limited.

confidentiality and security

The controller and the processor (the processor being a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller - Art.2.e.) have to ensure the confidentiality of the processing (Art.16), as well as appropriate technical and organisational measures to ensure the security of the processing (Art.17). In particular the relationship between the controller and the processor must be governed by a contract or legal act binding both parties to ensure that the processor shall act only on instructions from the controller and the obligations falling upon the controller are thus also being observed by the processor.

2.2.2.1.2 Specific material obligations

Special conditions are set up for the processing of sensitive data, and with regard to personal data that are used for journalistic purposes.

sensitive data

There are two types of sensitive data addressed in the Directive:

The first type comprises <<personal 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>> (Art.8.1.). Member States have to set up regulations prohibiting the processing of such data.

exemptions to the prohibition principle for sensitive data

Such a harsh principle almost necessarily carries with it a broad range of exemptions. These exemptions come in six types:

Exemptions

- that are in the direct interest of the data subjects,

- exemptions in the public interest,

- exemptions for specific organisations (like e.g. trade unions, religious associations, human rights groups, etc.)

- a sort of logical exemption,

- a special exemption for health data and

- a catch-all exemption.

Exemptions in the interest of the data subject: processing is permitted with the consent of the data subjects (Art.8.2.a.), to protect their vital interests or where they are incapable to give consent (Art.8.2.c.).

Exemptions in the public interest: processing is permitted, if the controller has to fulfil employment law obligations (with restriction on the exemption: <<in so far as it is authorised by national law providing for adequate safeguards>> - Art.8.2.b.).

Exemptions for special organisation as it regards their membership, <<provided that the data are not disclosed to a third party without the consent of the data subjects>> (Art.8.2.e.).

The <<logical>> exemptions refers to such data <<which are manifestly made public by the data subject or [are] necessary for the establishment, exercise or defence of legal claims>> (Art.8.2.e.).

The exemption for health data relates to <<processing of [...] data [that] is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules

established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.>> (Art.8.3.)

The catch-all exemption, finally, is set down in Art.8.4.: <<Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those [already described] either by national law or by decision of the supervisory authority.>> If such exemptions are adopted into the national legislation, the Commission has to be notified (Art.8.6.).

data relating to offences etc.

The second category of sensitive data relates to <<criminal convictions or security measures>>. The processing of such data <<may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.>> (Art.8.5.). Where such a derogation is made, again the Commission has to be notified (Art.8.6.). Member States may extend the principle of control by an official authority also to <<data relating to administrative sanctions or judgements in civil cases>>.

data for journalistic purposes

To adequately balance privacy interests and principles of freedom of expression Member States are required, in their national laws, to provide for derogations concerning the processing of sensitive information, and the rights of the data subject but also (as an exemption to an exemption) limiting the exemptions that can be set up in the public interest (Art.9).

2.2.2.2 Procedural obligations of the controller

notification

The controller has to notify the supervisory authority <<before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.>> (Art.18.1.)

simplification and exemptions

This procedure can be simplified or exemptions from notification can be granted if

- the processing falls within a category adequately described in a general manner and that categories are not << ... likely to affect adversely the rights and freedoms of data subjects ...>> (Art.18.2.).

- a personal data protection official is appointed by the controller with certain responsibilities (Art.18.2.) (cf. above).

Member States can totally exclude the notification obligation for public registers (Art.18.3.). They can provide an exemption or a simplification for those organisations that legitimately process sensitive information with the consent of the data subjects (Art.18.4.). Non automatic processing can also be excluded from notification or subjected to simplified notification.

contents of notification

The contents of such notifications is described in Art.19.

2.2.3 Rights of the data subject

The rights of the data subject are, of course, also to be read as obligations of the controller.

The data subjects have rights to be informed actively by the controller; they have access rights; they can demand rectification, erasure or blocking of data, and notification of third parties; and they have a right to object to the processing of their data.

2.2.3.1 the right to be informed

Except where the data subjects are already in the possession of such information they have to be provided by the controller with the following information:

<<the identity of the controller and of his representative, if any; the purposes of the processing for which the data are intended; any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him >> (Art.10.a. to c.)

However - and this is an important restriction of this obligation - such information needs only to be given in as 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 of the data subject.>> (Art.10, last paragraph).

Additional obligations for the controller to inform exist if the personal data have not been obtained from the data subjects. In these cases , <<at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed>> the following information has to be provided:

<< the identity of the controller and of his representative, if any; the purposes of the processing; any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him >> (Art.11.a.- c.).

Again, however, the same restriction as above applies: such information needs only to be given in as 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 of the data subject.>> (Art.11.1, last paragraph). Even more so, no such information needs to be given 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 or if recording or disclosure is expressly laid down by law.>> (Art.11.2.)

At least in these cases Member States <<shall provide appropriate safeguards.>>

2.2.3.2 right of access

Upon request, without excessive delay or expense, without constraints and at reasonable intervals the data subjects must be able to obtain from the controller:

<<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, communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions>> (Art.12.a.)

2.2.3.3 rights of rectification, erasure or blocking

The data subject may demand - as appropriate - <<the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data>> (Art.12.b.)

2.2.3.4 right to have third parties notified by the controller

The data subject may demand that third parties <<to whom the data have been disclosed of any rectification, erasure or blocking>> with the restriction, however that this right may only be demanded <<unless this proves impossible or involves a disproportionate effort.>> (Art.12.c.)

2.2.3.5 general exemptions to these rights

In addition to the exemptions already mentioned Member States may adopt additional legislative exemptions to these rights - as already stated above - in as far as such a restriction is a necessary measure to safeguard <<national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions, an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters, a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority>> Further restrictions again are possible to safeguard <<the protection of the data subject or of the rights and freedoms of others>> (Art.13.1.).

2.2.3.6 the right to object

specific cases of legitimacy

Data subjects have a right to object to the processing of their data at any time on compelling legitimate grounds if the processing was only based on the legitimate reasons like being <<necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed >> (legitimacy as prescribed by Art.7.e.) or being <<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 overridden by the interests for fundamental rights and freedoms of the data subject which require protection>> (legitimacy as prescribed by Art.7.f.) However, such objection is not possible <<where otherwise provided by national legislation.>>

direct marketing

The right to object can also be used by the data subject against

<<processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.>> (Art.14.b.)

automated decisions

Finally the data subject can object to being subjected to a decision <<which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.>> (Art.15.1.). Again, however, there are exemptions to this possibility, if such a decision <<is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or [if such a procedure] is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.>> (Art.15.2.a. and b.)

2.2.4 Institutions

The Directive addresses institutions to be set up on the national level via national legislation and installs two institutions on the Community level.

2.2.4.1 national level

On the national level each Member State shall provide <<that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.>> These authorities are independent (Art.28.1.).

They - and this is perhaps one of the most important proactive requirements of the Directive - have to be consulted <<when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.>> (Art.28.2)

The supervisory authorities have to have

- investigative powers,

- effective powers of intervention,

- powers to engage in legal proceedings (Art.28.3.).

They shall deal with claims by the data subjects or associations representing the data subjects concerning the protection of their rights and freedoms in regard to the processing of personal data. The claimants have to be informed about the outcome of their claim. The supervisory authorities shall, in particular, hear claims of any person for checks on the lawfulness of such data processing that is based on national regulations which build on the general exemptions provided by the Directive in Art.13 (derogations in the public interest etc.). The person shall be informed that a check has taken place. (Art.28.4)

The supervisory authorities will publish at regular intervals reports on their activities. These reports shall be made public.(Art.28.5.)

The authorities co-operate with each other and may request each other to help in the exercise of their duties and powers (Art.28.6.)

In the context of the notification procedure the authorities shall be requested via national law to check such processing that is <<likely to present specific risks to the rights and freedoms of data subjects>> prior to the start thereof (Art.20.1.). Such prior checking may also take place <<in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.>> (Art.20.3.). The supervisory authorities shall keep a publicly accessible register on notifications (Art.21.2.).

For further regulations on which information has to be made public in particular when no notification is required cf. Art.21.

Finally the supervisory authorities are to provide opinions on draft national codes of conduct (Art.27.2. first paragraph).

role of the national supervisory authorities with regard to Codes of Conduct

Such codes of conduct <<intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors>> shall be encouraged by the Member States and the Commission (Art. 27.1). Trade associations and other bodies representing types of controllers can then submit drafts of such codes to the opinion of the supervisory authority which will then <<ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.>> (Art.27.2.).

Members and staff of these authorities are subject professional secrecy (Art.28.7.)

2.2.4.2 Community level

On the Community level the Directive establishes the <<Working Party on the Protection of Individuals with regard to the Processing of Personal Data>> (Working Party) and the <<Committee>>.

2.2.4.2.1 Working Party

The Working Party <<shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.>> (Art.29.2.) It has advisory status and acts independently (Art.29.1.). It decides by simple majority of the representatives of the supervisory authorities (thus excluding the representatives of the Commission and the supervisory authority or authorities for the Community institutions and bodies) (Art.29.3).

It tasks are

- to examine any question covering the application of the national measures in order to contribute to the uniform application of such measures (Art.30.1.a.);

- to give the Commission an opinion on the level of protection in the Community and in third countries (Art.30.1.b.);

- to advise the Commission on amendments, additional or specific measures in the context of the Directive (Art.30.1.c.)

- to give an opinion on the codes of conduct on the Community level (Art.30.1.d.).

Furthermore it informs the Commission, if it observes divergence within the Community that might affect the *equivalency* of data protection to be ensured within the Community (Art.30.2.)

It can make recommendations upon its own initiative (Art.30.3.)

All opinions and recommendations of the Working Party are to be forwarded to the Commission and the Committee, and the Working Party has to be informed by the Commission <<of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.>> (Art.30.5.)

The Working Party itself shall make <<an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.>> (Art.30.6.)

2.2.4.2.2 Committee

The Committee consists of the representatives of the Member States (governments). It gives its opinion on measures the Commission proposes in reaction to the observations of the Working Party and in the context of transborder data flows into third countries (cf. the following section). (Art.31.1.)

2.2.5 Regulations concerning transnational data flows into Third Countries

Regulations on the transfer of personal data to third countries are highly complex.

2.2.5.1 The principle

Provided that there are no other special national regulations (that stay within the requirements of the Directive) Member States have to set down in their national laws that transfers may only take place if the third country ensures an *adequate* level of protection.(Art.25.1.)

The qualification <<without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive>> in that paragraph is not without practical relevance: In some countries, Germany and Austria, e.g. labour law requires that the appropriate bodies representing the employees have to give their consent for the transfer of employee data. This requirement cannot simply be overridden by pointing to the adequacy of the data protection regulations in the recipient third country. This rational is

explicitly acknowledged in recital 9 as a <<margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners>>.

Adequacy will be determined <<in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall 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, 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.>> (Art.25.2.)

2.2.5.2 Derogations

Member States shall lay down in their national laws that transfers can take place nevertheless under certain circumstances.

These following derogations, however, only apply <<save where otherwise provided by domestic law governing particular cases >>(Art.26.1). So here too, as with the general principle, the Member States are left with a margin of manoeuvre.

Conditions for derogations are:

- unambiguous consent to the proposed transfer by the data subject (Art.26.1.a.),

- the necessity of such a transfer for the performance of a contract or within a pre-contractual relationship in response to the data subject's request(Art.26.1.b.),

- the necessity of such a transfer <<for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party>> (Art.26.1.c.);

- public interest grounds, or necessity for the establishment, exercise or defence of legal claims (Art.26.1.d.)

- vital interests of the data subject (Art.26.1.e.) or

- that <<the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.>> (Art.26.1.f.)

Finally transfers may (but need not) to be authorised by national legislation <<where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.>> (Art.26.2.) In this case the Commission and the other member States have to be informed. (Art.26.3.)

This leads to questions of procedure:

2.2.5.3 Procedure

There are three types of procedures explicitly envisaged by the Directive:

- the procedure relating to the situation just described as to what extent contractual clauses are acceptable in derogation of the adequacy principle (the case of Art.26.2.)

- the procedure for cases where either the Commission or Member States regard the level of protection inadequate (Art.25.3. and 25.4.),

- the procedure to positively declare the level of protection of a particular country as adequate (Art.25.6.).

There are (no longer) any provisions in the Directive that would provide for the establishment of (politically damaging) <<black lists>>.

2.2.5.3.1 measures in the context of Art.26.2.

If an exemption according to Art.26.2. has been granted by a Member State and if - upon being informed by that Member State another Member State or the Commission object <<on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals>> the Commission will bring the issue before the Committee proposing adequate measures. The Committee votes on this proposal by a qualified majority vote, the Commission representative who is ex officio chair of the Committee abstaining.

If the proposal of the Commission coincides with the vote of the Committee the measures shall be taken immediately.

If the proposal of the Commission does not coincide with the vote, the Commission refers the issue to the Council of Ministers. For three months the application of the measure will be deferred. The Council can overrule the proposal of the Commission with a qualified majority within this time limit. (Art.31.2.)

In the case of Art.26.2. such a proposal may contain the acceptance by the Commission of certain standard contractual clauses. In accordance with the procedure described such contractual clauses would then have to be accepted by the Member States.

2.2.5.3.2 procedure in the context of Art.25.3. and 25.4.

In cases where either the Commission or Member States regard the level of protection that a particular country provides as inadequate the Commission will refer the issue to the Committee where the same procedure will take place as described above with the aim to prevent any transfers of data of the same type as in question to that third country (Art.25.4.)

In this case, however, the Commission is expressly required by the Directive to enter, at the appropriate time, into negotiations with that country to remedy the situation. (Art.25.5.)

2.2.5.3.3 Positive finding

As a result of such negotiation but also independently of such cases the Commission may find <<that a third country ensures an adequate level of protection [...] , by reason of its domestic law or of the international

commitments it has entered into>>. This decision has to go through the same procedure in the Committee as the other measures described. (Art.25.6.)

Countries that have that have ratified the Convention of the Council Europe on data protection and transformed the Convention into national law but which are not members of the European are the most likely candidates for such a positive certificate.

2.2.6 Accompanying regulations

The Directive requires that national legislations contain provisions for legal remedies (Art.22), liability (the Member States may provide that the controller can exculpate himself; but regulations setting down strict liability are also possible - Art.23) and sanctions (Art.24).

3. Political analysis of two selected issues

The Directive is not only a legal instrument, it is a political instrument born out of a series of heavily fought compromises.

As stated at the beginning most of the countries already had data protection regulations or got such regulations while the Directive was in the making. These countries wanted to make sure that as much as possible of their own regulations was reflected in the Directive without getting other regulations into the Directive -via the proposals by other countries - which they had successfully avoided on the national level. It should be remembered that the crucial debate took place in the Council, with the representation of the Member States governments and not of the national data protection agencies. As far as I know it was only the German government that had left the chair of its national delegation to their supervisory authorities. (The debates in the Council would make an excellent object for an access request according to the Council's decision on access to Council documents.).

Furthermore the drafting process and its result reflects the constructional problem of the Union being primarily concerned with economic policies (and regulations) yet also being an - albeit insufficient - political Union based on the obligation to Human and Political Rights as expressed in the European Convention of Human Rights.

Among the many interpretative and political problems posed in this context I want to address two issues which are of interest to a non-European readership. One problem relates to external relations, the other one to internal relations, both dealing with the issue of <<Third Countries>>, i.e. countries that are not members of the European Union and are recipients of personal information coming from a Member State.

3.1 Adequacy

The first issue is how to define <<adequacy>>. This problem, however, has to be seen in perspective: As shown above Art.26.1. provides a whole range of types of data flows where <<adequacy>> has no role to play. Only a brief look at this article reveals that a significant portion of international flows of personal data is covered by these derogations. Furthermore Art. 26.2. provides for derogation in individual cases or types of cases. As shown the Directive provides for two types of <<adequacy>> analysis. There is the analysis for individual cases. This decision is first of all in the hands of the relevant national authority (Art. 25.1.) and

eventually - if there is conflict about adequacy - in the hands of the Commission and the Committee (Art. 25.3., 31.2.).

For the remaining cases <<adequacy>> demands first of all a holistic view on the individual transfer in question, the specific regulations (whether privacy regulations or other regulations) covering that type of transfer and the general regulatory situation in the country in question.

In all, we are faced with a broad range of possible criteria which will give the Commission and the Committee its own political <<margin of manoeuvre>>. This margin may provide flexibility but also creates a problem of predictability. It also poses a long range political problem: If the interpretation becomes too flexible there will be less incentives for third countries to bring their national legislation up to the level of the Directive or to continue with such activities. Such an interpretation policy might then endanger the aim to create in the long range some sort of universal high level of data protection necessary to the Global Information Infrastructure. It is to be feared that countries that play an important economic role in international data communications may be granted <<privileges>>.

As to the criteria themselves the most important question will be to what extent it will be regarded as necessary to have an independent supervisory authority in order to be admitted among the third countries with an adequate level of protection. Another issue will be the question to what extent contractual solutions will be accepted to overcome lacking adequacy. In spite of the constant referral to such contractual solutions in the Directive, their feasibility, in my view, remains dubious. Contractual solutions in order to be effective need a legal environment that ensures that they can be adequately enforced. Since contractual solutions come into play when inadequacy is already stated and thus a negative judgement on the legal environment for data protection has already been passed it remains questionable where such effective enforcement should then come from. Furthermore, as we remember from the discussion of this issue in the Council of Europe, direct enforceability of such contractual solutions by data subjects is not guaranteed in all legal systems. Finally, even if this is the case, enforcing the contractual solution, in absence of the existence of a supervisory authority, places a considerable burden on the data subjects that casts a strong doubt on the adequacy of such a solution.

On the other hand, the holistic approach taken by the Directive at least ensures that third countries cannot simply achieve an adequate level of protection by merely passing <<symbolic>> legislation.

3.2 A procedural problem

The internal political problem is one of procedure in the case of the adequacy decision making: The Directive emphasises the independence of national supervisory authorities (Art.28.1.: <<These authorities shall act with complete independence in exercising the functions entrusted to them.>>). And yet it is the Commission in co-operation with the Committee that restrict this very independence in deciding itself upon adequacy. And the Committee, we remember, represents the Member States governments. It will also be the Member States, through the Council of Ministers, that will eventually decide if there is disagreement between the Commission and the Committee. The supervisory authorities are represented in the Working Party (Art.29) , but the Working Party can only give opinions on that issue (Art.30.1.b.). The reason for this inconsequent construction is, of course, Community law: Setting up an independent authority - like e.g. the European Central Bank - on the level of the Union would have required a change of the Treaties and it was already difficult enough to see through the Directive. However, it is predictable that the current construction will be a source of internal conflict with regard to the future of European Union data protection practices and

policies. The national supervisory authorities and their Working Party will have to keep a close watch on Commission activities as to how much concern for economic policy and how much concern for privacy these activities will reflect.

4. Evaluation - A preliminary comment

This is not yet the time for a comprehensive evaluation of the Directive. One has to watch first the national transformation processes to see what actually will be achieved by the Directive. In particular one has to see to what extent national legislators will make use of the extensive exemptions that national legislators may impose on the observation of the data quality principles (Art.6), the rights of the data subjects (Art.10,11,12) and on the publication duties (Art.21) and of the exemptions which are contained in these respective articles and in the general article on exemptions and restrictions to which we have referred at various instances (Art.13).

At least these general exemptions and restrictions are bound to the condition that they constitute <<necessary measures>>. One should hope that the interpretation of necessity will turn out to be interpreted as restrictively as similar exemptions in the European Convention on Human Rights are interpreted by the Strasbourg Court. Furthermore particularly with regard to these exemptions there is an explicit right of the data subject to lodge a request with the national supervisory authority to check on the lawfulness of such processing claiming such exemptions (Art.28.4. 2nd paragraph).

At the same time one cannot overlook that the Directive has tried to achieve a balance between what the German Constitutional Court in his landmark decision on the National Census Law had described as the need to balance the right to informational self-determination with the conditions imposed on the individual as a social being. May third countries find this balance attractive enough to continue in their efforts to provide comparable safeguards in their own national legislations not just for economic reasons but to continue to contribute to make the right to informational privacy an inherent element of a universal concept of civil, political, economic, social and cultural rights./--

Cybernews Volume 2, numéro 3 (automne 1996)

The article reflects the personal view of the author.

(*) The text of the Directive is available in various languages at
http://www2.echo.lu/legal/en/dataprot/dataprot.html

(**)Senior Policy Adviser, GMD German National Research Centre for Information Technology, St. Augustin, Germany;
Assistant Professor for Public Law, Information and Communication Law, University of St.Gallen (HSG), Switzerland;
Chairman, Legal Advisory Board for the Information Market, European Commission DG XIII,

Luxembourg.
Personal Web-Page: http://www.gmd.de/People/Herbert.Burkert/Welcome.html

 ISSN 1201-7302

I. Le courrier électronique: un outil de communication séduisant

Les qualités et les avantages du courrier électronique sont constamment vantés. Rapide, peu couteux et synonyme d'informations facile à traiter avec un ordinateur le courrier électronique a de plus en plus d'adeptes. Certains voient même sa croissante popularité coïncider avec la mort du télécopieur.

La thèse est séduisante. Quels sont les avantages du fax, une technologie lente, coûteuse et messagère de documents difficiles à traiter par rapport à ceux du courrier électronique? Un confrère vous fait parvenir un projet de contrat par courrier électronique et vous voulez y apporter des modifications... Rien de plus facile, votre traitement de texte vous permettra très certainement de travailler directement sur le document transmis. Au contraire, s'il s'agissait d'une télécopie, il faudrait resaisir, c'est-à-dire redactylographier, l'ensemble des informations transmises pour arriver au même résultat. Sans compter la lenteur des télécopies et les coûts y associés.

Pourtant, l'emploi du courrier électronique comme outil de communication par les avocats soulève des interrogations. Prophètes de malheur ou non, bien des spécialistes remettent en question la sécurité du réseau Internet, sentier emprunté par le courrier électronique, et son utilité dans le transport d'informations à caractère confidentiel.

Si la transmission par télécopieur a déjà été qualifiée de courrier décacheté [1] puisqu'à chaque extrémité de la transmission, plusieurs personnes peuvent prendre connaissance du message, que penser du courrier électronique. À la différence du fax qui utilise habituellement une ligne de transmission privée, le courrier électronique, circule "à ciel ouvert", au vu et au su de quiconque parmi les millions de branchés voudra bien se donner la peine de capter au passage n'importe quel message lancé sur cette autoroute électronique. En ce sens, ne peut-on pas qualifier ces messages de cartes postales électroniques que tout un chacun peut lire n'importe où sur le réseau et n'importe quand entre le moment de leur expédition et celui de leur réception?

Pour les juristes, avocats ou notaires, ces caractéristiques du courrier électroniques sont lourdes de conséquences. Soumis à de strictes et lourdes obligations en matière de protection des confidences données par le client - identifié comme le sacro-saint "secret professionnel" - le professionnel du droit peut-il se permettre l'utilisation d'un outil de communication qui, en apparence, offre aussi peu de garanties de confidentialité?

II. Le secret professionnel et les professionnels du droit?

Notaires et avocats sont tenus au secret professionnel par le Code des professions, par leur codes de déontologies respectifs et, pour les avocats, par la Loi sur le Barreau. Le respect de la confidence donnée fait aussi partie des obligations implicites d'un contrat passé entre un client et son conseiller juridique, fût-il avocat ou notaire.

Lorsqu'il est question du secret professionnel la doctrine réfère à deux notions: une "obligation de se taire" et un "droit de ne rien dire"[2]. La première expression réfère à l'obligation du professionnel du droit de ne pas révéler les confidences qui lui sont faites par son client sous peine de sanctions civiles ou disciplinaires. La seconde expression réfère au droit du juriste de ne pas révéler devant un tribunal des renseignements couverts par le secret profesionnel, malgré les règles générales au sujet du témoignage.

La question de la reponsabilité civile de l'avocat ou du notaire qui manque à son devoir de confidentialité et cause un préjudice à son client a été peu étudiée au Québec. L'analyse doctrinale et jurisprudentielle a plutôt porté sur le caractère confidentiel d'informations ou de documents dans le cadre de procédures judiciaires et sur le droit du juriste de refuser de témoigner à leur sujet, invoquant l'exception du secret professionnel.

Cela dit, face aux développements des moyens électroniques de communication et à leur utilisation sans cesse grandissante les juristes sont chaque jour davantage exposés à des fuites provoquées par une utilisation insouciante ou peu éclairée d'outils comme le télécopieur [3] ou le courrier électronique. Ces risques rendent nécessaire qu'on s'attarde de façon spécifique à la responsabilité de l'avocat en matière de divulgation fautive du secret professionnel.

De plus, l'utilisation généralisée de systèmes informatiques en réseau, accessibles par modem ou par l'Internet comporte également des risques pour les informations contenues dans de tels systèmes [4]. Ces risques, s'ils se matérialisent, sont susceptibles d'engendrer des poursuites contre les avocats ou les notaires. Aussi, à l'heure des outils électroniques de gestion de l'information, ce n'est pas que la transmission des confidences d'un client par les voies électroniques qui doit être examinée, mais aussi les moyens utilisés pour leur conservation. Ce dernier aspect dépasse malheureusement le cadre du présent exposé.

L'obligation de préserver indemne le secret de son client est sans aucun doute l'une des obligations les plus importantes et les plus enveloppantes reposant sur les épaules du juriste. Elle s'étend à tous les mandats visant la fourniture de services juridiques: que le juriste agisse comme avocat-conseil [5], conseiller juridique, officier public ou comme procureur]ad litem, il sera toujours tenu au secret professionnel. Cette obligation s'étend même aux communications confidentielles qui ont lieu avant l'octroi du mandat.

Face à son obligation de conserver secrètes les confidences faites par son client, le juriste a-t-il une obligation de moyen ou de résultat? L'importance de l'obligation de la protection du secret professionnel milite pour sa qualification d'obligation de résultat. Le libellé de l'article 131 de la Loi sur le Barreau qui impose à l'avocat de "...conserver le secret absolu des confidences qu'il reçoit..." et de l'article 15 a) de la Loi sur le Notariat à l'effet que les devoirs du Notaire comprennent celui de "...ne pas divulguer les faits confidentiels dont il a eu connaissance" semblent aller dans ce sens.

Pourtant, conserver le secret professionnel fait partie de l'essence même de la relation client-avocat, relation que l'on qualifie de mandat. Or, l'article 2838 C.c.Q. est à l'effet que le mandataire doit, dans l'exécution de son mandat, "...agir avec prudence et diligence".

De plus, le texte de l'article 3.06.01 du Code de déontologie des avocats impose simplement à l'avocat l'obligation "...[d']exercer une prudence raisonnable afin d'empêcher..." que ne soient divulguées les confidences de son client par ses employés. Cette disposition trouve son corollaire à l'article 2141 C.c.Q. qui prévoit que c'est en fonction du soin avec lequel le mandataire choisit son substitut et de la qualité des instructions qu'il lui donne que l'on évalue sa responsabilité. Ces facteurs militent à notre avis pour la reconnaissance de l'obligation de conserver indemne le secret professionnel comme une obligation de moyen.

Cela dit, la qualification de l'obligation du juriste de conserver le secret professionnel nécessiterait une étude approfondie que le présent texte ne vise pas. De plus, d'aucuns prétendront que la distinction entre obligation de résultat et de moyen peut paraître artificielle. Pour les fins de la présente discussion nous allons considérer que le juriste a une obligation de moyen quant au secret professionnel de son client.

Aussi, pour évaluer si la conduite du juriste est fautive ou non, l'on devra se demander s'il s'est acquitté de son devoir de protéger le secret professionnel comme l'aurait fait, dans les mêmes circonstances, un juriste semblable [6]. Mais étant donné que les communications électroniques sont en plein essor et que les problèmes qui y sont reliés ne semblent pas encore avoir commencé à provoquer des poursuites, la prudence est de mise pour le praticien. Trop de précautions valent mieux qu'une violation fautive du secret profesionnel.

III. Le courrier électronique est-il par définition une communication publique?

L'utilisation du courrier électronique pour communiquer des informations confidentielles offre-t-elle suffisamment de garanties pour que l'on puisse considérer qu'il y a une assurance qu'elle ne sera pas divulguée? En effet, parmi les critères que doit remplir une communication afin de bénéficier de la protection du secret professionel, celle-ci doit être faite dans des circonstances où le juriste et son client ont une expectative raisonnable de ne pas voir leur communication interceptée. Le traitement accordé aux communications par téléphone cellulaire illustre bien cette condition.

Cela dit, des auteurs ont déjà prétendu que l'utilisation du courrier électronique offre suffisamment de garantie de secret pour ne pas être une communication publique, arguant comme suit:

"In the ordinary course of events, given the variability of routing over the Internet, it may be only a remote possibility that a transmission would ever fall into the hands of a party capable of using the information against a client. Arguably, given the low probability of interception, the commmercial usefulness of the mode of communication, and the impropriety or illegality involved in the interception, the choice of the communication medium does not necessarily imply an absence of an intention to communicate confidentially or a lack of reasonable steps to keep the communication confidential.[7]

Mais il est encore trop tôt pour conclure de façon définitive à ce sujet. Selon Jones:

"no case in any jurisdiction has addressed the specific question of whether transmission of unencrypted messages over the Internet is an intentional divulgence of that information so as to form a waiver of any claim to a privilege.[8]

Nous n'avons pas non plus recensé de décision à ce sujet.

Cela dit, une communication ou un document couvert par le secret peut perdre le bénéfice de cette protection. Règle générale la doctrine et la jurisprudence considèrent qu'une communication ou un document perd la protection du secret professionel s'il est divulguée à des tiers ou s'il est transmis sans expectative raisonable de confidentialité.

Les types de divulgation susceptibles de faire perdre le bénéfice de la protetion du secret professionnel sont nombreux [9]. Tout comme nous l'avons écrit plus haut, il est encore trop tôt pour dire si l'utilisaton du courrier électronique sera considéré comme une renonciation au caractère confidentielle d'une communication entre le juriste et son client.

IV. Quels moyens utiliser pour éviter que les confidences faites par un client ne perdent leur caractère confidentiel ou ne soient divulguées par inadvertance?

A. Une règle d'or

La règle d'or de l'utilisation du courrier électronique avec un client est simple: il est impératif de l'avertir des risques inhérents, réels ou appréhendés, à l'utilisation du courrier électronique comme moyen de communication.

En fait, l'on peut s'interroger à savoir si le devoir de conseil du juriste n'est pas générateur d'une obligation d'éveiller son client aux risques inhérents à l'utilisation de moyens de communication comme le télécopieur ou le courrier électronique? Surtout quand on sait que bien des entreprises, contrairement aux cabinets d'avocats n'ont pas l'habitude d'utiliser une page de garde avertissant le récipiendaire accidentel du caractère confidentiel de la communciation.

Aussi, nous croyons qu'il est souhaitable pour le juriste de conseiller ses clients quant à certaines procédures ou pratiques à adopter dans l'utilisation d'outils de communication comme le fax ou le courrier électronique. Bien entendu, charité bien ordonnée commence par soi-même: des procédures d'utilisations bien définies devraient être suivies dans les cabinets de notaires et d'avocats.

B. L'utilisation d'une page de garde informant de la nature confidentielle de l'information

Les auteurs Dodd et Bennett dans leur article "Waiver of privilege and the Internet", à la page 370, concluent que:

"In the result it is the authors' view that the courts should favour upholding a claim of privilege where there has benn a disclosure, even where documents have been sent over the Internet, assuming the appropriate covering notice has been included with the e-mail."

Leur conclusion repose notamment sur les prémisses qu'il est peu probable que la communication soit interceptée par des personnes susceptibles d'en faire usage et que l'interception, s'il y en a une, sera illégale. Par conséquent, ils croient que même la nature peu fiable du réseau au niveau de la sécurité ne suffit pas à faire perdre aux parties leur droit de l'utiliser tout en ayant une expectative de confidentialité dans leur transmission.

Pour eux, l'utilisation d'une page de garde sur un message électronique devrait être aussi efficace que dans le cas d'une télécopie. Ils appuient leur raisonnement sur le Professional Conduct Handbook du Law Society de Colombie-Britannique interdisant à un avocat de prendre connaissance d'un document lorsqu'il a des motifs raisonnables de croire qu'ils sont couverts par le secret professionnel. Selon eux, la page de garde suffit pour indiquer que les parties désirent que leur communication soit confidentielle et indique clairement à l'avocat de Colombie-Britannique qu'il s'agit d'une information couverte par le secret profesionnel. Il est intéressant de noter que le jeu combiné des article 36 (2) C.c.Q. et 2858 C.c.Q. pourrait permettre de justifier une conclusion semblable au Québec.

Malheureusement, la seule page de garde ne suffit pas à éviter que la divulgation ait des effets dommageables, même si pour les fins d'un tribunal, une telle divulgation serait présumée ne pas avoir été faite. Le secret de commerce qui est révélé ne sera plus jamais secret...

C. La cryptographie: une protection intéressante

Par conséquent, l'utilisation du courrier électronique par les juristes dans le cadre de leurs prestations de services professionnels ne devrait-elle pas toujours se faire par le biais de message cryptés?

D'une part, contrairement à Dodd et Bennett, nous ne sommes pas nécessairement prêts à affirmer que la probabilité que le message tombe entre les mauvaises mains et faibles. La nature même du réseau fait en sorte qu'il est difficile d'évaluer les risques qui s'y rattachent adéquatement. De plus, la cryptographie protègera non seulement contre la perte du caractère confidentiel devant un tribunal, mais aussi contre les dommages pouvant découler d'une divulgation accidentelle d'informations protégées.

Bien entendu, lorsqu'il est question de cryptographie, le degré de sécurité associé à une méthode plutôt qu'une autre devra aussi être considéré. Pour l'instant, il semble que les principaux obstacles à l'utilisation répandue de la cryptographie sont au nombre de deux. En premier lieu, les logiciels de cryptographie sont parfois difficiles à utiliser et relativement lents. Ensuite, tant qu'une norme ne sera pas répandue, le juriste risque de devoir faire l'acquisition de bien des logiciels pour avoir un système compatible avec celui de ses clients. Quoiqu'il en soit, un minimum de protection pour le contenu du message semble approprié et sage.

D. Banaliser les documents: un compromis acceptable?

Enfin, certains préconisent la banalisation des documents transmis par le biais du courrier électronique. De cette façon, celui qui intercepte un message se trouvera peut-être en possession d'un contrat bien rédigé, mais il ne pourra pas identifier les parties liées. Malheureusement, dans bien des cas il est difficile de banaliser les transmissions d'informations entre avocats et clients, dans la mesure où les messages électroniques portent en général l'adresse du récipiendaire et de l'expéditeur. De plus, les renseignements techniques, de par leur nature, sont difficiles à banaliser.

V. Conclusion

L'emploi du courrier électronique chez les professionnels du droit en est à ses débuts. Et tout porte à croire que son usage ira en grandissant. Dans un tel contexte, le juriste averti devra tenir compte des obligations qui lui sont imposées par les lois, les règlements et le contrat qu'il a avec son client avant d'embrasser de façon trop enthousiaste une technologie dont les garanties de confidentialité ne sont pas encore certaines.

Dans tous les cas, la règle d'or consiste à aviser les clients des risques associés à l'utilisation du courrier électronique et à les aider à adopter des pratiques sécuritaires.

Cybernews Volume 2, numéro 3 (automne 1996)

Notes

1 J. LAMBERT, Le télécopieur, un merveilleux cauchemar juridique? ou... (1992)2 CP du N 453.

2 J.L. Baudouin, "Le secret profesionnel du conseiller juridique", (1963) 65R. du N. 483-511, p. 484; J.C. Royer, La preuve civile, 2e éd., Éd. Y. Blais, Cowansville, 1995, no. 1155, p. 705; depuis l'arrêt Descôteaux c. Mierzwinski, [1982] 1 R.C.S. 860, l'existence d'un droit au secret professionnel susceptible d'engendrer une obligation de réparation en cas de violation est reconnue de façon expresse par la Cour suprême.

3 Ejan Mackay rapporte que le télécopieur, peu connu en 1987, était utilisé par 95% des avocats de la province en 1991 (E. Mackaay, Les avocats du Québec, Barreau du Québec, 1991, p.52; les modifications apportées au Code de procécédure civile permettant la signification par télécopieur est un symptôme évocateur de cet engouement. Voir arts 140.1, 142, 146.01 et 146.02. À quand la signification par courrier électronique? À quand la dématérialisation des actes de procédure?

4 Voir par exemple W. R. Cheswick et S. M. Bellovin, Firewall and Internet Security, Addision-Wesler, Reading, 1994

5 Expression utilisée par Gérald Tremblay, dans "La responsabilité professionnelle de l'avocat-conseil",Conférences Commémoratives Meredith 1983-84, De Boo, Toronto, 1983, 177-226, p. 178, pour désigner les praticiens dont la pratique n'est pas contentieuse au même titre que celle des plaideurs - on pense tout de suite aux juristes spécialistes des fusions et acquisitions - et ceux qui, peu importe s'ils sont des plaideurs ou non, rendent des services juridiques "hors cour": rédaction d'opinions dans le cadre d'un litige éventuel, etc.

6 J.L. Baudouin, La responsabilité civile, 4e éd., Éd. Y. Blais, Cowansville, 1994, nos130- 134, pp 93-96

7 P. Dodd et D.R. Bennett "Waiver of Privilege and the Internet", (1995) 53The Advocate, 365-370, p.369

8 R.L. Jones, "A lawyer's Duties with regard to Internet E-Mail", p.16 (travail étudiant, 6 août 1995, Georgia State University College of Law in Atlanta. Pour une copie: bobjones @ mindspring.com.

9 Ibid.; R.D. Manes et M.P, Silver, Solicitor-Client Privilege in Canadian Law, Butterworths, Toronto, 1992, pp.187 et suiv.

 ISSN 1201-7302
