The Law and New Information Technology

Poullet, Yves

Published in:
Essays on computer law

Publication date:
1990

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

37 The Law and New Information Technology: A Comparative Approach to the Laws of Continental Europe

Prof. Yves Poullet, Director, Centre of Research for Computer Science and Law, Facultés Universitaires Notre-Dame de la Paix

This subject is vast, and the reader should appreciate the difficulty I experienced in proposing to cover in a few pages a synthesis of the law, or rather the laws, of continental Europe (hereafter, Europe) in relation to new information technology.

The difficulty arises first of all from the very diversity of the subjects to be examined. The law relating to new information technology encompasses aspects of civil law, such as the law of evidence *vis-à-vis* electronic data, the law relating to telecommunications contracts, aspects of penal law, intellectual property rights, administrative and public law, constitutional rights such as privacy, to say nothing of fiscal and accounting laws.

This chapter seeks to highlight several aspects of European law, under five headings:

- The protection of computer programs
- Computer crime
- The protection of individual rights and liberties
- Telecommunications
- Public IT services

Under none of these headings—and this is a second difficulty—can a law common to all countries of Europe be discussed. It is not a question of comparing the Latin approach—encompassing the laws of Belgium, Spain, Italy and France—with the Scandinavian approach, and then with the Germanic approach—encompassing the laws of Germany, Austria and the Netherlands. On the contrary, it must be emphasised that each country, in its own way, has tried to develop a legal response to the questions arising from the emergence of new information technology, choosing in some cases to give a rigorous interpretation of classical law in the face of the new reality, and in other cases electing to concentrate on the protection of the individual.

The reader will not find in this chapter an exhaustive review of the laws and solutions posed to the problem. I will, however, under each of the chosen headings, try to touch on the principal themes in the laws of the European countries, examining one or two solutions to the problems, and for the remainder, referring the reader to a selected bibliography.

Computer Programs as Intellectual Property

A computer program is defined by the Commission of European Communities' 'Green Paper on Copyright and the Challenge of Technology' (COM (88) 172 final, Brussels, 7 June 1988) as 'a set of instructions the purpose of which is to cause an information processing device, a computer, to perform its functions'.

Legal protection of computer programs is demanded by the software industry in Europe, just as it is in Anglo-Saxon countries. Similarly, our countries have adopted the same approach as the Anglo-Saxons, that is, they have largely preferred to apply, and in some cases adapt, the existing laws of intellectual property to the protection of software, rather than to conceptualise new legislative solutions. Thus, the protection given by patent, and above all by copyright, is extended to computer programs.

The protection of computer programs by patent was rejected initially on the basis that programs *per se* were the application of mathematical methods and the representation of information, and therefore non-patentable. Article 52 of the European Convention on Copyright specifically excludes computer programs. (The convention exclusion is echoed by the laws of Belgium, Denmark, Germany, France, Italy, Luxembourg and Spain). Notwithstanding this, certain jurisdictions have progressively begun to allow the patenting of inventions which have a technical and inventive character, and have included computer programs in this category: see M. Flamme, *Octrooierbaarheid van Software*, Brugge, Die Keure, 1985.

For example, a decision of the Paris Court of Appeals (*Schlumber* case, Propriété Intellectuelle Bull. Documentaire, 1981, III, 175), affirmed that the classification of 'patentable invention' could not be refused to an invention which involved the analysis of soil and potential exploitation of petrol, just because certain steps of the procedure were carried out by a computer program. It seems, then, that under French law, patenting of programs will not be refused in all circumstances.

In Germany, on the other hand, at least for the Bundesgerichtshof (*Rolled Bar Cutting Case*, GRUR, 1981, 39–42), patents for inventions which include programs are still refused. H.W. Hanneman has summarised the position of the German court as follows:

> An invention the gist of which lies in a program is non-technical. A computer with which the program can be executed is of technical nature, it is true, but if the program can be executed on any general purpose computer—which usually is the case—the technical means lack novelty.

It should be noted that in spite of its reticence, the European Patent Office in 1985 decided to re-examine its policies and to adopt new examination guidelines under which an invention which, taken as a whole, had a

technical character and met all the conditions of patenting, would be patented even if it included a computer program.

The protection of computer programs by copyright was more heavily debated in the countries of Europe than in the Anglo-Saxon countries. The law had been previously interpreted as being a means of protecting literary and artistic works at the time of their publication, and not as protection for inventions having an essentially industrial and commercial character. This conclusion was reached in several German and French decisions. It was, however, queried by a majority of commentators, given that international conventions and national legislation were seeking to simultaneously protect scientific and technical works of a commercial and industrial nature: see, for example, A. Dietz, 'A Common European Copyright—is it an Illusion?' (1985) 8 EIPR 215; E. Ulmer and G. Kolle, 'Copyright Protection for Computer Programs' (1974) 14 IIC 172. A German case (Bundesarbeitsgericht, 13 Sept. 1983, BB, 1984, 871) summarised the majority position:

> Computer programs can be classified as literary works within the meaning of s.2(1)(1) of the Copyright Act and/or as representations of a scientific or technical nature within the meaning of s.2(1)(7) of the Copyright Act. A computer program also constitutes a creation arising from personal intellectual activity. The fact that it may serve scientific, technical or commercial purposes is irrelevant in this respect.

Legislative amendments have supported this majority position. In Germany, legislation introduced on 24 June 1985 equated computer programs with literary works. In France, an amendment enacted on 3 July 1985 extended the protection of copyright to computer programs, but subject to specific conditions (for example, limiting the duration of copyright to twenty five, rather than fifty, years). Spain has specifically extended copyright protection to programs, and similar amendments will be introduced in Belgium, Holland, Denmark and Italy.

The virtual unanimity of the countries of Europe in accepting the protection of computer programs by copyright does not prevent profoundly divergent interpretations of the extent of this protection. Thus, the concept of the 'originality' of the program, a necessary characteristic for the protection of the work by copyright, is interpreted differently by the various national legal systems. The divergence between German and French decisions adequately illustrates this. On 7 March 1986, the French Court of Appeals confirmed a decision of the Paris Court of Appeals, stating:

> The development of a computer program is an original work of the mind in its composition and expression, and goes beyond automatic and imposed logic since a programmer, like a translator, must *choose between various alternatives and expressions*. His choice reflects his personality and he is therefore entitled to invoke the rights granted to the author by the copyright law.

Thus, only programs created by other programs—a rare case—are not eligible for protection.

On the other hand, the well-known German case *Inkasso* (OKG Karlsruhe, 9 February 1983, BB, 1983, 986) was more restrictive in its appreciation of originality. It was held that the program must represent an individual work, original and creative. It required that the nature of the new program, resulting from use, compilation and dissemination of relevant information and theories, exceed the utility of an average program.

The question of the attribution to the employer or to the employee of the intellectual property rights of a program is another source of divergence between the countries of Europe: see B. Hubo, 'La titularité des droits d'auteur sur les logiciels civils par un salarie', *Droit de l'Informatique*, 1986, No. 3, p. 151.

In Germany (OLG Koblenz, 13 August 1981, BB, 1983, 992), the employer is automatically the owner of intellectual property rights in concepts developed by an employee during the carrying out of his professional tasks. The right to a payment of an 'equitable remuneration' to the employee as compensation, in circumstances where he leaves the firm, has been mooted, although the Bundesarbeitsgericht decision of 13 September 1983 (BB 1984, 871) would not seem to support it.

In Belgium, on the other hand, only a specific clause in the employment contract relinquishing the intellectual property rights of the employee for the benefit of his employer will entitle the employer to those rights.

More divergence has arisen in the case of the merger of parts of one person's programs into another's software: to what extent does this reproduction constitute a breach of copyright? Bertrand and Couste ('Copyright Protection for Computer Software in Civil Law Countries' in *Distribution, Access and Communications*, 1–3 June 1988, Amsterdam, p. 84) cite the solutions given by various national legal systems:

- There *is* a breach, according to a decision in the Netherlands, if at least 16 per cent of the functions of the two programs are identical.
- A German decision maintains that a reproduction of 70 per cent of a source program constitutes a breach.
- The Paris Court of Appeals has condemned the reproduction, with minor adaptations, of more than twelve sub-programs.

Further Reading

G.P. Vandenberghe, *Bescherming van Software, Een rechtsvergelykend onderzoek*, Kluwer, Antwerpen, 1984; G. Bertin and I. de Lamberterie, *La protection du logiciel—Enjeux juridiques et economiques*, Paris, Litec, 1985; G. Alpa, *La tutela giuridica del Software*, Milano, Giuffre, 1984; S. Denis, Y. Poullet, and X. Thunis, *Banques de donnees, Quelle protection juridique?*, Cahiers de Recherches du CRID, Bruxelles, 1988; Commission of the European Communities, 'Green Paper on Copyright and the Challenge of New Technologies', Communication from the Commission, COM (88) 172 final, Brussels 7 June 1988; A. Bertrand and M. Couste, *Copyright Protection for Computer Software in Civil Law Countries*, 1988, Amsterdam, 73–93.

Computer Crime

A group of experts in the OECD defined 'computer crime' as 'any illegal, unethical, or unauthorised behaviour involving automatic processing and/or transmission of data': OECD, ICCP, 'Computer-related Crime: Analysis of Legal Policy in the OECD', Report DSTI/ICCP 84.22, 18 April 1986. Such a definition embraces the crimes of fraud by computer manipulation,

computer spying, pirating of programs, copying of semiconductors, electronic sabotage, non-authorised use of a computer, non-authorised access to a data base, and breaches of privacy laws.

This section is not concerned with privacy or copyright breaches, which are discussed elsewhere. It analyses, however, the response given to each of the other types of breach by judicial interpretation of the law and occasionally by new legislation.

Computer Fraud

Computer-assisted fraud involves the manipulation of data in pursuit of gain. An example is the siphoning of funds in electronic funds transfers. Regulation of this classical criminal activity has certain legislative limitations in the countries of Europe. For example, 'theft' involves the 'taking of some actual thing belonging to someone else' according to definitions in such countries as Germany, Belgium, Greece and Luxembourg. Can one speak of the taking of an actual thing when it is a simple manipulation of information? Similarly, breach of trust, or fraud, involves, particularly in Belgium, France, Italy and Germany, a person being cheated. Can one speak of a 'person' being cheated in the case of computer fraud?

Certain countries of Europe have established, in the fashion of some Australian and United States jurisdictions, new offences specifically directed at computer-assisted fraud. For example, chapter nine, section 1 of a Swedish amendment of 1985 seeks to penalise 'any person who, by presenting incorrect or incomplete information, or by altering a program or a recording without permission, affects the result of an automatic process in a way which involves gain for the offender and loss for someone else'.

An alternative approach, followed particularly by Germany and Denmark, is the broadening of traditional definitions by the addition of an appropriate paragraph dealing specifically with computer fraud. Thus, for example, article 263 of the German Penal Code, which deals with fraud, was amended in 1986 to make reference to computer fraud in the following way:

> Any person who, with the intention of procuring an unlawful gain for himself or for a third party, causes loss to another by influencing the result of data processing by improper programming, by the use of incorrect or incomplete data, by the unauthorised use of data, or by otherwise interfering without authorisation with the processing, shall be liable . . .: *Second Law for the Prevention of Economic Crimes*, 1986.

The latter approach is clearly predominant in the countries of Europe. Our legislatures are loathe to define new offences and prefer to extend the existing offences already dealing with 'fraud' or 'forgery'.

Computer Sabotage—Malicious Damage

Computer sabotage or mischief poses the same conceptual problems with respect to the extension of criminal laws. In order for 'malicious damage' to exist, the traditional legislation in our countries usually demands physical destruction. However, this arguably does not occur in the context of interference with software unless, perhaps, there is an erasure of programs or, more commonly, of data.

Courts in a number of countries, for example Italy, Belgium, Norway and Austria, have held that the wilful alteration of data or programs is embraced by the traditional criminal offences. It has not been necessary, therefore, to await legislative direction. Other countries, such as Germany and France, have amended their legislation to specifically extend the legal concept of malicious damage to include such erasures. This extension may be quite wide; section 193 of the Danish Penal Code, revised in 1985, declares: 'Any person who, in an unlawful manner, causes major disruptions in the operation of public means of communications, of the public mail service, or of telegraph or telephone systems . . . shall be liable . . .' This Danish provision, likely to be emulated by the Finnish and Norwegians, is rationalised by the vulnerability of an 'informational society' to the sabotaging of telephone lines, the jamming of airwaves, the erasure of programs, and so on (see Sieber, p. 80).

Unauthorised Computer Use

The issue of whether unauthorised use of computers is a criminal offence is not contentious in certain countries, like Belgium, Denmark and Finland, where illegitimate use of someone else's property is punishable as theft and where the law specifically refers to the use of computer hardware (as opposed to programs) belonging to another in this context.

Some countries retain the classical notion of 'usage theft' (*furtrum uses*) and will not adapt it, except in very specific cases. In this category, Sieber cites the Netherlands, Germany and Austria. In contrast with other countries like Switzerland, Portugal and Norway, they have refused to criminalise the actual use of someone else's computer (as opposed to the unauthorised access to a data base). These countries consider that to penalise the intrusion itself, the simple theft of machine time, without there being either malicious damage or illegitimate access to or manipulation of data, would constitute over-criminalisation (see Sieber, p. 85).

Unauthorised Access

Finally, unauthorised access to an information system has caused a broadening of traditional offences in most countries, through prohibitions on the interception of telephone messages (for example, article 17 of the Belgian *Telephone and Telegraph Act* 1930; section 201 of the German Penal Code; paragraphs 139a and 139c of the Netherlands' *Penal Code*; article 617 of the Italian *Penal Code*). In most cases it is a question of protecting the integrity of an information storing system and/or of transmission, independently of the private nature of the information contained within it or transmitted by it.

An extension of criminal liability previously reserved for public transmission systems to all information systems causes difficulties. Some countries, like Sweden, have not hesitated to penalise the activities of a person who illegitimately procures access to data stored on computer. Most countries, however, refuse to condemn mere access. Thus, German law, and Norwegian and Finnish proposals, require that a person who seeks to benefit from criminal law protection must as a prerequisite take practical preventive measures (section 203 of the *German Penal Code*, revised in 1986, punishes 'any person who obtains without authorisation, for himself

or for another, data which are not meant for him and *which are specially protected* against unauthorised access'). Others, such as France, demand proof of an intent to harm before penalising the person responsible (article 462–2 of the *Penal Code*, amended on 5 January 1988, speaks of fraudulent access, that is to say it demands *dol special*).

Further Reading

U.Sieber, *The International Handbook on Computer Crime—Computer-related Economic Crime and the Impingement of Privacy*, Chichester, New York, 1986; R. Kaspersen (ed.), *Strafrecht in de Informatiemastschappij*, Amsterdam, 1986; OECD, ICCP, 'Computer-related Crime: Analysis of Legal Policy', Paris, 1986; U. Sieber, R. Kaspersen, G. Vandenberghe, K. Stuurman, 'The Legal Aspects of Computer Crime and Security: A Comparative Analysis with Suggestions for Future International Action', doc. prepared for the Commission of the European Communities—Legal Advisory Board, 10 December 1987; IBI, *Le droit penal de l'informatique: Problèmes et Perspectives*, January 1983.

The Protection of Data and Privacy

The need for the protection of data and personal privacy in both the public and private sectors resulted in all the countries of Europe progressively implementing, each in its own way, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. The convention was approved by the Council of Ministers on 17 September 1980 and was opened for signature on 28 January 1981. It has so far been ratified by France, Sweden, Spain, Germany, Austria, Luxembourg and Norway, as well as the United Kingdom.

The principles of the convention have, however, met with a diversity of interpretation among different countries. The convention aims to protect only *data relating to individuals*, and not data relating to corporations. Certain legislation (Norwegian, Austrian, Luxembourgois) has, however, suggested that the general objects of data protection, coupled with the recurring difficulty in distinguishing between data relating to groups and data relating to individuals, justifies an extension of the principles of data protection to corporations.

Only *automatic data-processing* is embraced by the convention. French law (article 45), however, extends to certain manual files. Similarly, recent legislation in the Netherlands extends the application of the law to all 'coherent data storage systems . . . automated or manual, designed to provide efficient access to data'.

The *setting up* of a data base is subjected, in certain countries, to a preliminary procedure. The procedure often takes the form of a simple declaration, to the control authority, as to the existence of the file along with a few other details. This is the case in Austria, France, Holland and Sweden. Denmark, Germany and Norway require a declaration only for public sector files or files held by enterprises which are not involved directly with the individual about whom the file contains information (commercial intelligence agencies, headhunters, etc).

The *data quality* principle is espoused by article 8 of the convention, according to which the processed information must be:

(a) . . .
(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
(d) . . .
(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

This principle is taken up by the legislation of all Germanic countries: Austria, Denmark, Germany, Holland, Norway. There is, however, a distinction between *public files*, *files held for private use*, and *those containing information on a third person*. Public files can only hold data in the manner prescribed by law and only if it is necessary for the performance or maintenance of lawful and public functions. Files held for private use (such as those operated by banks, insurance companies, etc.) may contain data necessary for any professional service provided to the person on file. Finally, private files held by companies whose business involves supplying personal information to third persons (such as credit insurance companies) are subject to stricter control.

A recent law in the Netherlands diverges, and proposes a *sectoral* approach. It allows professional bodies to make codes of conduct consistent with the law, and to seek endorsement or ratification by the control authority. (Similarly, a simplified declaration system established by French law enables the control authority to authorise certain organisations to establish their own privacy procedures if these are consistent with the rules laid down by the authority).

The 'data quality' principle permits the legislatures of the abovementioned countries to distinguish between internal data-processing and external communications, subjecting the latter to stricter provisions. (For example, article 24 of the German law permits 'the transmission of nominal data as authorised within the limits of the legal relationship—whether contractual or quasi-contractual or based on trust with the data subject—or to the extent necessary for the protection of a legitimate interest of the transmitting institution or of a third person, or as a matter of general interest provided that the transmission does not endanger the data subject's right to privacy'.)

All legislation in Europe institutes a control authority: the French Commission Nationale Informatique et Libertés, the German Bundesbeauftragte, the Danish, Norwegian and Swedish Commissioners for Data Protection, the Registration Chamber in the Netherlands, and so on. These authorities have a role for 'ombudsmen': inspection of data-processing operations, maintaining public registers, assisting data subjects, advising on government legislation and, finally, publication of reports. The members are appointed by the governments of the day. (The composition of the French CNIL is more complex, however, The parliament, the judiciary and the public service are involved in the nomination of the members. The intention is to guarantee the independence of the commission from the government.)

With respect to a right of access to files by data subjects, as required by the Council of Europe Convention, some legislation provides that a person who keeps a file on another is obliged to inform that other person about the processing of the file. This is the case in Denmark, France, Sweden and Germany. This right can generally be exercised upon payment of an amount fixed by the government. (On the right of access and its different methods of application in the countries of Europe, see C. Debrulle, 'Le droit d'acces', in *Problèmes legislatifs de la protection des données*, Conf. Intern. Madrid, 13 June 1987, Council of Europe, p. 33.)

A number of countries regulate transborder data flow, notwithstanding the principle of article 12 of the convention which purports to abolish all restriction between member countries. For example, article 32 of the Austrian law subjects to the control authority's authorisation all transborder flows; article 21 of the Danish law is similar. Articles 19 and 24 permit the French government to restrain transborder flow. Commentators in the European Community have expressed concern that the application of these restrictions does not permit states to establish tariff-free services, as required by article 59 of the *Treaty of Rome*, and plead for the adoption by all countries in the Common Market of common principles that can be written into a directive. (In this respect, note the reflections of H. Burkert, *International Information Flows between Freedom and Protection*, the Report of the Second World Conference on Policies Concerning Transfrontier Data Flows, Rome, 26–29 June 1984, IBI, TDF 260.)

Further Reading

Banque de données, *Entreprises et vie Privee, Actes du colloque de Namur*, CIEAU, Bruxelles, 1981; R. Pagano, *Panorama of Personal Data Protection Laws*, Camera dei deputati, Roma, 1983; B. Catania, *Privacy Dossier*, Ed. Sarin, Torino, 1984; and J. de Houwer, *Privacy and Transborder Data Flows*, VUB, Brussels, 1984.

Telecommunications

Traditionally, the regulation of telecommunications in Europe has been characterised by public monopolies to which are entrusted both a regulatory power and an entrepreneurial or profit-making responsibility. Whether one looks at the German Deutsche Bundespost, the French Direction Générale des Télécommunications or Belgium or Holland's Régie des Télégraphes et Téléphone, the pattern is similar. Only the Italian SIP and the Spanish Telefonica, those being public enterprises or enterprises where the State has a strong interest, stray slightly from the pattern.

This confusion of the regulatory and exploitative roles has been denounced on several occasions by the European Commission (Green Paper, 65) and national tribunals: note, for example, in Belgium, the questions posed to the Court of Justice of the European Communities in the case *RTT* v. *GB Inno BM*, Trib. comm Brux 11/1/88.

American and British deregulation, as well as the recent Green Paper of the Commission (CCE, 'Project for a Dynamic Economy: Green Paper on

the Development of a Common Market of Services and Equipment by Telecommunications', Communication of the Commission in Council, Brussels, 26 May 1987) has caused most of the countries above progressively to modify, little by little, their positions. The regulatory landscape of telecommunications in Europe is clearly undergoing change: everywhere laws or law reform commissions are looking to reconcile the existence of strong and autonomous public service with the principles of a sane and efficient management. This has been affirmed by the commission and already consolidated by a first directive (Directive 88/JO//CEE, 16 May 1988, O. J. no. L131/73, 27 May 1988) on the matter of liberalising the terminal equipment market.

This brings us to an analysis of the evolution of laws in two countries, France and the Netherlands. It is worth noting how these countries have interpreted the most important principles of the Green Paper:

- the necessity to clearly separate the activities of governmental regulation and commercial exploitation; and
- the possible maintenance of a monopoly on the supply and exploitation of the telephone service infrastructure with all others open to private enterprise.

The French enactment of 30 September 1986 (law no. 86–1067) relating to the freedom of communication stipulates in article 1 that 'the establishment and use of telecommunications installations shall be free'. If the actual wording seems to allow for a total deregulation, it must be recognised that other provisions impose certain major restrictions on the principle. Thus, article L33 of the Post and Telegraph Code which enshrines the monopoly on telecommunications to France Telecom, is not abolished. It follows that the 'freedom of communication' is not complete and is subject, according to article 10 of the 1986 law, to an *authorisation system*:

> The National Commission of Communications and Rights will provide the authorisation required by Articles L33 and L34 of the Post and Telegraph Code for the establishment and use of all telecommunication installations with the exception of those of the State.

The reader's attention is drawn to two points:

- the authorisating body is an *independent administrative authority*: the CNCL. Thus the separation of the activities of exploitation and use is ensured. The CNCL is composed of experts along the lines of the American FCC or the Canadian CRTVC; and
- authorisation is not given for all services.

A provisional decree of 24 September 1987 (Decree of 24 September 1987 Relating to Special Links and to Telematic Networks Open to Third Persons, O. J. 25/9/87) limits what can be offered publicly and what stays within the monopoly of France Telecom. Without going into a technical examination of the ordinances, note only that criteria are established to ensure a stable, competitive service.

> The organisation [says the decree] offering a public system . . . must specify, for each service offered on the network, the annual management charges related to

the movement of data, and the annual total revenue related to the management of the telematic service, with a ratio at the most equal to a fixed percentage. This percentage, that can not be less than 15%, is fixed by decree of the Minister . . .

A recent enactment in the Netherlands is the 'Op telecommunicatievoorzieningen'. At the time of writing, it is still in the preliminary stages, approved by the second chamber of parliament. Its text will probably not be further modified. The proposed date of inception was 1 January 1989. This governs the infrastructure of telecommunications services and terminals; the 'Op PTT Nederland NV' determines the status of the future manager. The two laws are linked: it was necessary, before freeing up the telecommunications market, to define precisely the rules governing the public body responsible for the regulation of the competitive market (for an analysis on the above-mentioned laws, see R. van den Hoven van Genderen, 'De wet op de telecommunicatievoorzieningen, afsluiting van een tijdperk of handhaving van de status quo?', *Computerrecht*, 1988, No. 1, 51).

Care is taken to separate strictly the activities of regulation and commercial exploitation and this led the Netherlands' authorities to create a number of organisations, for example, the regulatory Directie Regelgeving en Vergeening Post en Telecommunicatie created within the Ministry for Telecommunications, and the consultative Raad voor Advies voor Post en Telecommunicatiebeleid, composed of experts and 'overlegorgaan', being a discussion forum for the public operator and the people concerned. The same care led to the transforming of the old State enterprise into a new organisation: the PTT Nederland NV, not only set up, for a limited period, to govern the management of the activities under State monopoly, but also capable of offering other services or products in competition with the private sector.

As for the right granted to the private sector supplier, the law excepts particular types of telecommunications equipment (telecommunications cables) and activities (emission appliances or radio electric reception). All services, according to the same law, which may be supplied by the private sector dealer must be defined by ordinance. The reason for recourse to ordinances is clear: the government wishes to retain the option, bearing in mind the evolution of technology and the nature of the market, to modify quickly the list of services offered to the private sector. However, telephone services, telex services and pure data exchange are the only ones currently under State monopoly.

Further Reading

R. Bruce, J. Cunard, M. D. Director, *From Telecommunications to Electronic Services*, Butterworth, 1986; CRID, *Les Reseaux de Service à valeur ajouteé: quelle reglementation?*, Cahiers de Recherche du CRID, No. 4, 1989 (to be published); E. J. Mestmaeker (ed.), *The Law and Economics of Transborder Telecommunications*, Nomos Verlag, Baden-Baden, 1987; OECD, *Changing Market Structures in Telecommunications*, North-Holland, 1984; and R. L. White, H. M. White, *The Law and Regulation of International Space Communication*, Artech House, Norwood, 1988.

Telematic Services

The marriage of data-processing and telecommunications has permitted the birth of numerous services called 'telematics' (electronic messaging), after the expression coined in the French Nora-Minc report. Following in the footsteps of telematic services designed for the professional world are those developed for public use. Following the public acceptance of automatic teller machines in banks and point-of-sale terminals, governments have started to permit a number of public services for voluntary subscribers: electronic mail, electronic press, home shopping. One immediately thinks of the French Teletel experiment (more than 3 million terminals in circulation), but Holland's VIDITEL, Germany's Bildschirmtext and Italy's VIDEOTEL are equally remarkable. It seems in any case that in France and the Netherlands these experiments have created a real private market.

The aim of this section is to analyse succinctly the effect of laws that apply to these services (e.g. France: decision of the CNCL of 4 February 1988 relating to home shopping and Circular of 17 February 1988 read in conjunction with article 43 of the law No. 86–1067 of 30 September 1986 relating to freedom of communication applicable to certain audiovisual communication services; Italy: Decreto Ministerialle 17 May 1985/Istituzione del servizio pubblico 'VIDEOTEL'; Germany: Bildschirmtext-Staatsvertrag, 18 March 1983; Netherlands: Viditelcode inzake reclame en interactief gebruik, 1 January 1984), looking at the specific regulations enacted at the time of the introduction of these new services, and pre-existing laws concerning electronic fund transfers.

The offering of telematic services to the general public is not subject to any preliminary authorisation except in Italy where 'all VIDEOTEL service must be the subject of previous authorisation by the Minister and conducted in accordance with the relevant conditions of subscription' (Ministerial Decree, 30 October 1982). Therefore, while the old French law of 1982 on audiovisual communication established a provisional authorisation system, article 43 of the amendment of 30 September 1986 set up a declaration system exempting electronic messaging services which were considered a private correspondence service. The German Bildschirmtextstaatsvertrag of 1983 gave the same right to all persons participating in BTZ, subject to the sole qualification of having a permanent base in Germany. (This distinction is considered by some as a breach of article 59 of the *Treaty of Rome* concerning free services.)

Though the offering of services is not subject to any authorisation, the contents of the services *can* be regulated, in particular for reasons of consumer protection. Again, the examples of French and German rules serve as a reference.

Articles 37, 43 and 76 of the French law referred to above oblige the producer to identify himself, to indicate the price per page and to clearly distinguish between advertising and information. With respect to electronic

press, the traditional values relating to the press apply: independence of journalists, financial openness, naming of an editor, and respect for the freedom of the press (article 37 of the law of 1986). The German Bildschirmtextstaatsvertrag obliges the producers to give exact, accurate, up-to-date information, and to identify all advertising by a 'W' (Werbung).

With regard to relations with the users, in particular the supply of the card or of the code necessary to use the services, a recently proposed European directive (XI/267/88, April 1988) relating to payment cards is inspired by the Danish law on electronic fund transfers and the American *Fund Transfers Act*. These Acts oblige those who offer services to inform the users at the same time as to who bears overall responsibility for the system, the cost of the service, the frequency of the periodic statements, procedures to be followed in case of error, and finally, the uses made of collected information.

Putting this into practice may result in other difficulties. Some laws, especially Belgian, French and Luxembourgois (see B. Amory, Y. Poullet, 'Le droit de la preuve face a l'informatique et a la telematique, *Droit de l'Informatique*, 1985, No. 5, 14) demand a signed statement as proof that an individual has used a service. The validity of clauses to the effect that 'registration of automatic apparatus or its reproduction on computer data carriers is sufficient proof that the transaction took place by means of the card or the electronic key operated by the subscriber' may be legally questioned under some consumer protection laws. For example, article 180 of the Code of Civil Procedure in the Netherlands stipulates that 'standard clauses which ignore the laws of evidence are not admissible as proof of facts'. La Corte di cassazione italienne decided on 29 January 1982 that parties may not contract out of responsibility for providing such proof when one of the parties is disadvantaged by the clause.

As a consequence, it seems that in Europe, even if a judge accepts *a priori* an electronic signature, he still reserves the right, notwithstanding any exclusion clause, to examine the validity of the electronic document according to technical and organisational criteria.

On the question of the *responsibility of the supplier* of the card or secret code, in case of loss or theft of the means of access, a finding of the Belgian Court of Appeals concerning electronic fund transfers EFT is often cited as reference. The responsibility of the user ceases from when he reports the loss or theft. The responsibility then rests with the supplier (the bank in this instance) to take all necessary measures to avoid financial loss that may result from the illegitimate use of the card. The Danish law of 1978 affirms the same principle in its article 21. It adds, following the example of American legislation, that in case of a delay in reporting the loss or theft, the responsibility of the user is still largely limited.

Further Reading

Y. Poullet and G. Vandenberghe (eds), *Telebanking, Teleshopping and the Law*, Computer Law Series, Kluwer, 1988; T. Bourgoignie, M. Goyens, J. Laffineur, *Questions juridiques liées a l'introduction de la télématique grand public*, UCL, Centre de Droit de la Consommation, 1985; F. Van Ryn, R. Williams (eds), *Concerning Home Telematics*, Proceedings of the IFIP TC9

Conference on Social Implications of HIT, North Holland, Amsterdam, 1987; W. Ring, R. Harstein, *Bildschirmtext heute: Neues Recht und Praxis*, Fraunzs Rehm, Munchen, 1983; and *La télématique: Aspects techniques, juridiques et socio-politiques, Actes du colloque de Namur*, 1984, Story Scientia, Bruxelles, 2 volumes.