

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

The Law and New Information Technology

Poullet, Yves

Publication date:
1988

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

[Link to publication](#)

Citation for pulished version (HARVARD):
Poullet, Y 1988, *The Law and New Information Technology: a Comparative Approach to the Laws of Continental Europe..*

General rights

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

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

Take down policy

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

THE LAW AND NEW INFORMATION TECHNOLOGY

A Comparative Approach to the Laws
of Continental Europe

Yves POULLET

Professor of Law and

Director of the Center
of Research for Computer
Science and Law

Facultés Universitaires
Notre-Dame de la Paix
Namur

The chosen subject is vast, and the reader ought well to understand the embarrassment of the author in proposing to cover, in twenty-odd pages, that which would be a synthesis of the law, or rather the laws, of Continental Europe in relation to 'new information technology'.

The embarrassment comes first of all from the very diversity of the subjects to be examined (1). The law of new information technology encompasses aspects of civil law, such as the law of evidence vis-a-vis electronic data, the law concerning telecommunications contracts, aspects of penal law, intellectual property rights, administrative and public law, constitutional rights such as individual liberty, to say nothing of fiscal and accounting laws.

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

- the protection of computer programs;
- computer crimes;
- the protection of the rights and liberties of the individual;
- telecommunications;
- public IT services.

Under none of these headings - and this is a second embarrassment - can a law common to all countries of Continental Europe be discussed. It is not a question of comparing the latin approach - characterizing the laws of Belgium, Spain, Italy and France - with the Scandinavian approach, and then with the Germanic approach - characterizing the laws of Germany, Austria, and the Netherlands. On the contrary, it must be stated that each country, in a unique way, has tried to give a judicial answer to the questions arising from the development of new information technology, choosing in some cases to give a rigorous interpretation of classical law texts in the face of the new reality, and in other cases electing to concentrate on the protection of the individual.

(1) On the whole of these subjects, Y. POULLET - X. THUNIS, Droit et Informatique, un mariage difficile, Droit de l'Informatique et des Télécommunications, no. 2, p.11

The reader thus will not find in this essay an exhaustive review of the laws and solutions posed to the problem. The essay will, however, using a different approach to study each of the chosen headings, try to touch on the larger themes in the laws of the European countries, examining one or two solutions to the problem, and for the remainder, referring the reader to the footnotes and selected bibliography.

CHAPTER ONE: Computer Programs as Intellectual Property

A computer program is defined by the Green Paper of the Commission (1) as 'a set of instructions the purpose of which is to cause an information processing device, a computer, to perform its function'.

Under this definition, covering a range from application programs to operating systems, from programs coded by object to those coded by source, even the smallest distinctions appear useful in a discussion of the extension of protection accorded by different judicial systems.

Legal protection of computer programs is demanded by the software industry in Continental Europe, just as it is in Anglo-Saxon countries. Similarly, our countries have adopted the same point of view as the Anglo-Saxons; that is to say, they have preferred to apply, in some cases adapting them, the existing laws of intellectual property to the protection of software, rather than legally defining new legislative solutions (2). Thus, the protection given by the patent, and above all, by copyright of the author, are extended to computer programs.

The protection of computer programs by the patent had been rejected formerly because computer programs, in so far as such, were the application of mathematical methods and the representation of information, non-patentable, and Article 52 of the European Convention on the subject of copyright excludes computer programs by name (3). Notwithstanding this principle, certain jurisprudences, encouraged by the doctrine (4), have progressively allowed the patenting of inventions which have a technical and inventive character, and have incorporated in this, computer programs.

For example, the decision of the Paris Court of Appeals (5), affirmed that the classification of 'patentable invention' could not be refused to an invention which allowed analysis of the soil and potential exploitation of petrol, for the single reason that certain steps of the procedure were carried out by a computer program. It seems, then, that patenting, according to French jurisprudence, would not be refused except in the case of programs by themselves.

In Germany, on the contrary, at least for the Bundesgerichtshof (6), patents for inventions that include programs are refused. HANNAMAN (7) summarizes the position of the German court as follows: 'An invention whose gist lies in a program is non technical. A computer with which said program can be carried out is of technical nature, it is true but if said program can be carried out on any general purpose computer - which usually is the case - the technical means lack novelty.'

It is noted that in spite of its reticence, in 1985 the European Patent Office (8) decided to reexamine its politics and to adopt new examination guidelines according to which an invention that, taken as a whole, has a technical character and meets all the conditions of patenting, can be patented even if the invention in question includes a computer program.

The protection of computer programs by the copyrights of the author was more harshly discussed in the countries of Continental Europe than in the Anglo-Saxon countries. The principle reason for this is certainly that such a protection, in legal systems of civil law, has been previously understood to be a means of assuring the protection of literary and artistic works, at the time of their communication to the public, and not as a given for inventions having a character frequently industrial and commercial (9). This objection is reiterated by several German and French decisions (10). It is, however, rejected by the majority of authors and the jurisprudence, given the fact that international conventions and national legislation protect equally the scientific and technical works having a commercial and industrial character (11). A German decision (12) summarizes this majority position: 'Computer programs can be classified as linguistic works within the meaning of sec. 2 (1) (1) of the Copyright Act and/or as representations of scientific or technical nature within the meaning of sec. 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 proven this majority position. In Germany, the law of 24 June 1985 (13) identifies computer programs with literary works. In France (14), the law of 3 July 1985 extends the protection of the author's copyright to computer programs, but subjects them to specific conditions (for example, limiting the duration of copyright to 25, rather than 50, years). Spain (15) explicitly plans protection of programs by author's copyright. Law projects of similar content exist in Belgium, Holland, Denmark and Italy (16).

The virtual unanimity of the countries of Continental Europe in accepting the protection of computer programs by author's copyright does not prevent profoundly divergent interpretations of the extension of this protection (17). Thus, the concept of the 'originality' of the program, a necessary characteristic for the protection of the work by copyright, is understood differently by the national jurisprudences. The opposition between German and French decisions adequately illustrates this. On March 7, 1986, the French Court of 'Cassation' confirmed the decision of the Paris Court of Appeals (18) according to which 'The elaboration 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 the image of his personality and he is therefore entitled to invoke the rights granted to the author by the Copyright law'. Thus, only the programs for which the instructions are dictated by the function of the programming - a rare case - are not eligible for protection.

Inversely, the famous German case 'Inkasso' (19) is more restrictive in its appreciation of originality. The program must represent an individual work, original and creative. It requires that the structure of the program resulting from choice, assembly, and distribution of relevant information and propositions, exceeds the competence 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 a second source of divergence (20). In Germany (21), the employer is automatically holder of intellectual property rights on the logic developed by his employee during the carrying out of professional tasks. The payment of an 'equitable remuneration' to the employee as compensation, in the case where he leaves the firm, has been discussed (22).

In Belgium, on the other hand, it seems necessary to insert a clause in the work contract relinquishing the intellectual property rights of the employee for the benefit of his employer (23). In France, the amendment to the law of 1985 deviates from the general rule by attributing to the employer the property of software developed in the framework of working.

Different decisions are concerned with the partial duplication of programming developed by one person, in another's software: to what extent does this reproduction constitute an infraction? BERTRAND and COUSTE cite the solutions given by national jurisprudences (24):

- there is an infraction, according to a decision in the Netherlands, if at least 16% of the instructions of the two programs are identical;
- a German decision maintains that a reproduction of 70% of a source program constitutes an infraction;
- finally, the Paris Court of Appeals condemns the reproduction, in exchange for minor adaptations, of more than twelve sub-programs.

SELECTED BIBLIOGRAPHY

G.P. VANDENBERHE, Bescherming van Software, Een rechtsvergelykend onderzoek, Kluwer, Antwerpen, 1984.

G. BERIN and I. de LAMBERTERIE, La protection du logiciel - Enjeux juridique et économiques, Paris, Litec, 1985.

G. ALPA, La tutela giuridica del Software, Milano, Giuffré, 1984.

S. DENIS - Y. POULLET - X. THUNIS, Banques de données, 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 - M. COUSTE, Copyright Protection for Computer Software in Civil Law Countries, June 1-3, 1988, Amsterdam, 73-93

INTELLECTUAL PROPERTY: Notes

- (1) Green Copyright on Copyright and the challenge of technology - Copyright issues requiring immediate Action - Communication from the Commission COM (88) 172 final, Brussels 7 June 1988.
- (2) ... Except for semiconductors (chips), about which following the American invitation, the European countries had to adopt new legislation, conforming to the Council of the European Community's Directive of 16.12.86 (87/54/EEC), OJ L24 of 27.01.87, p. 36. In the restraining framework of the article we could not develop the specific problem of protection of microconductors could not be developed.
- (3) The exclusion planned by Article 52 of the Convention is echoed by the laws of Belgium, Denmark, Germany, France, Italy, Luxembourg and Spain.
- (4) In relation to this, see M. FLAMEE, Octrooierbaarheid van Software, Brugge, Die Keure, 1985.
- (5) Schlumberger case, Propriété Intellectuelle Bull. Documentaire, 1981, III, 175.
- (6) Rolled Bar Cutting case, GRUR, 1981, 39-42, note Pietzker.
- (7) H.W. HANNEMAN, op.cit., 252.
- (8) Decision given by the President of the European Patent Office; 6 March 1985.
- (9) For a complete list of critics on the extension of author's copyright protection to computer programs, see G.P.V. VANDENGERGHE, op.cit. et M. VIVANT, Informatique et propriété intellectuelle, J.C.P. éd. C.I., 1985, II, 14382.

- (10) In Paris, France, 20 February 1985, note J.R. BONNEAU, Paris, 4 June 1984, JCP, éd. C.I., 1985, II, 14.409, note M. VIVANT.

In Germany, L.G. Mannheim 12 June 1981, B.B., 1981, 1543 (rejected in Appeal by OCG Karlsruhe, 9 February 1983 GRUR, 1983, 300). 'Computer programs are not eligible for copyright protection since they lack intellectual aesthetic substance.' Another objection is the lack of 'communicability' of the work to the public: see BERTRAND-COUSTE, p.76. In addition, DIETZ demonstrates very well that notwithstanding the different fundamental approaches to common law on one hand, and civil law, on the other, the jurisprudences and recent legislative modifications have progressively abolished the oppositions. (A. DIETZ, a common European copyright, is it an illusion?, 8 EIPR, 215 (1985))

- (11) For an excellent synthesis of the different arguments, E. ULMER and G. KOLLE, Copyright protection for computer programs, 14 IIC, 172 (1974).
- (12) Bundesarbeitsgericht 13 Sept. 1983, B.B., 1984, 871.
- (13) Law of 24 June 1985 on the Amendment of legal provisions in the copyright field, Bundesgesetzblatt, no. 33, 27 June 1985.
- (14) Law no. 85-660 of 3 July 1985 on the rights of authors, performers, record and videogram producers and communication enterprises, J.O. 4 July 1985, 7495 and s.
- (15) Art. 91-100 of Ley de Propriedad Intelectual, no. 22/87 of 11 May 1987, Boletín Oficial del Estado, no. 275 of 17 November 1987.
- (16) In this respect,
Denmark, Bill no. L 153 of 14 January 1988 on the amendment of the Copyright Act.
Italy, Draft Law no. 1746, Senate, 25 March 1986.
Belgium, Prop. de Loi Lallemand, Sénat, 329-1, 1988.

- (17) This divergence is highlighted as a source of problems for commerce among Member States in the Green Paper of the Commission.
- (18) Paris, 2 November 1982 G.P., 1983, 1, 1/7 note J.R. BONNEAU, more recently, Paris, 5 March 1987, GRUR Int., 1983, 669; in the same vein, a German case of Landsgericht de Kassel, 21 May 1981, B.B., 1983, 992.
- (19) OKG Karlsruhe, 9 February 1983, B.B., 1983, 986. In the same vein, the decision of the Bundesgerichtshof of 9 May 1985, BGH2, 1985, 1747 which states that only the proof that two programmers haven't chosen the same programming to resolve a problem, is not sufficient to satisfy the condition of originality.
- (20) On this subject, B. HUBO, La titularité des droits d'auteur sur les logiciels civils par un salarié, Droit de l'Informatique, 1986, no. 3, p. 151.
- (21) OLG Koblenz 13 August 1981, B.B., 1983, 992 (same solution in Holland)
- (22) The decision of the Bundesarbeitsgericht of 13 September 1983 (B.B. 1984, 871) seems to exclude it.
- (23) Cf. B. HUBO, op.cit., 151. The project of law presently studied by the Senate plans the software copyright be automatically attributed to the employer.
- (24) A. BERTRAND - M. COUSTE, Copyright protection for computer software in civil law countries, in Distribution, Access and Communications, June 1-3 1988, Amsterdam, p. 84.

CHAPTER TWO: Computer Crime

A group of experts in the OECD (1) area defined 'computer crime' as 'any illegal, unethical, or unauthorized behaviour involving automatic processing and/or transmission of data'. Such a definition includes such crime as fraud by computer manipulation, computer spying, the pirating of programs, the copying of semiconductors, electronic sabotage, non-authorized use of a computer or non-authorized access to a data base, and infractions of the privacy rules (2).

This chapter does not concern itself with privacy infractions, nor those of copyright, discussed elsewhere (Chapters One and Three). It analyzes, however, through judicial systems and occasionally through new legislation, the response given to each of the other types of infraction.

Computer-assisted fraud consists of the manipulation of data in pursuit of gain, for example the siphoning off of funds in the case of EFT. This incrimination by classical crimes comes up against legal exigencies set by the legislation of the countries of Continental Europe to repress such crimes. Thus, the theft supposes the 'subtraction of some actual thing belonging to someone else' according to the definition given particularly in Germany, Belgium, Greece, Luxembourg, etc; can one speak of the subtraction of an actual thing when it is a simple modification of information? Thus the breach of trust, or fraud, supposes, particularly in Belgium, France, Italy and Germany, that a person - and can one speak of a person with regard to a computer? - would be cheated.

Certain countries of Continental Europe have established, in the manner of Australia (3) or the U.S.(4), new provisions allowing them to incriminate for computer-assisted fraud. Sieber distinguishes different types among these new provisions; for instance, it is question of actually attacking the problem of computer crime and targetting as well the manipulation of data whose distinction, substitution, access or use is not authorized. Chapter Nine, Section 1 of the Swedish law of 1985 (5) proposes to repress 'any person who, by presenting incorrect or incomplete information, by altering a program or a recording or otherwise without permission affects the result of an automatic process in a way which involves gain for the offender and loss for someone else, shall likewise be guilty of fraud.'

Inversely, another tendency developed particularly by Germany and Denmark, is characterized by the broadening of traditional dispositions by the addition of a relative paragraph on the specificity of the computer fraud.

Thus, for example, in Article 263 of the German Penal Code, on fraud, the law of 1986 (6) adds a disposition on computer fraud, in the following way (7): '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 unauthorized use of data, or by otherwise interfering without authorization with the processing, shall be liable...'

This latter tendency is clearly the majority in the countries of Continental Europe. Our laws are loath to define new infractions and prefer to extend the existing incriminations that are concerned with 'fraud' or 'forgery'.

Computer sabotage or mischief poses the same question of the extension of penal concepts. In order for sabotage to exist, the classical legislations of our countries demand most often physical destruction. However, this does not exist unless there is the effacement of programs, or, more simply, of data. Without waiting for legislative modifications, the doctrine and 'jurisprudence' of a number of countries, for example Italy, Belgium, Norway and Austria, consider that the voluntary altering of facts or programs falls under the classification of traditional incriminators. Other countries have modified their legislation, such as Germany and France, to enlarge the field of application of the legal concept of sabotage to include such effacements (9). 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 disturbances in the operation of public means of communications, of the public mail service, of telegraph or telephone systems, ... shall be liable ...' This Danish extension, hoped for equally by the Finnish and Norwegians, is justified by the wish to prevent, by the same incrimination, all criminal acts based on the larger vulnerability of a society said to be informational, whether the sabotaging of a telephone line, the jamming of waves, the effacement of a program, etc (10).

The questions over incrimination for non-authorized use of computers does not arise in certain countries, like Belgium, Denmark and Finland, where illegitimate use of someone else's property is punishable as theft in the instance where the user necessarily uses the hardware that is the material property of someone else, and not simply the programs.

Some countries either refer to the classical notion of 'usage theft' (furtum usus) or do not allow it except in very specific cases. For this, Sieber cites the Netherlands, Germany and Austria. As concerns these countries (11), one notes that in contrast with other countries like Switzerland, Portugal and Norway, they have refused to make criminal the actual use of someone else's computer (cf. as opposed to the non-authorized access to a data base). These countries consider that, to penalize the intrusion itself, the simple theft of machine time, without there being either an act of sabotage or illegitimate access to certain data, or manipulation of another's data, would constitute an excess of severity (overcriminalization) (12).

Finally, the question of non-authorized access to an information system has often been treated as a broadening of the traditional incriminations prohibiting, in most countries, the interception of oral telephone messages (13); in both cases it is a question of protecting the integrity of an information storing system and/or of transmission, independently of the secret of the information contained within it or transmitted by it.

Such an extension of the penal protection that was previously reserved for a public system of transmission to all information systems causes difficulties. Some countries, like Sweden (14), would not hesitate to punish any person who illegitimately procures access to data stored on computer. Most countries, however, refuse to condemn mere access. German law, and Norwegian and Finnish projects, demand of he who seeks to benefit from of penal protection that he has taken technical measures of protection (15). Others, for example France, demand the proof of intent to harm, to punish the author of the infraction (16).

SELECTED BIBLIOGRAPHY

U. SIEBER, The International Handbook on Computer Crime - Computer related Economic Crime and the Impingement of Privacy, Chichester, New York, Brisbane, Toronto, 1986.

R. KASPERSEN (ed.), Strafrecht in de Informatiemaatschappij, 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 pénal de l'informatique, Problèmes et Perspectives, January 1983.

COMPUTER FRAUD: Notes

- (1) OECD, ICCP, Computer related criminality: Analysis of Legal Policy in the OECD area, Report DSTI/ICCP 84.22, 18 April 1986 (final version)
- (2) This is the typology proposed by the OECD and taken up by SIEBER, The International Handbook on Computer Crime, op.cit. 2 and 3. You are referred to this work for a succinct presentation of the following ideas.
- (3) Cf. the 'Northern Territory Criminal Code Act' (No. 47) of 1983 and the 'Crimes ordinance (No. 4)' no. 44, 1985, amending the New South Wales Crimes Act of 1900.
- (4) Cf. the Federal Credit Card Fraud Act of 1984 and the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 and 1986.
- (5) Under this provision, U. SIEBER, R. KASPERSEN, G. VANDENBERGHE, K. STUURMAN, op.cit.
- (6) Second Law for the prevention of economic crimes, 1986. SIEBER also puts into this second group the Austrian and Norwegian projects, in addition to the Danish law.
- (7) Cf. Similarly, the proposed modification by section 269, on the subject of forgery, permitting the inclusion of false electronic signals.
- (8) Cf. For example, the wording of Article 528 of the Belgian Penal Code, that penalizes the voluntary damage to material possessions.
- (9) Cf. Along the same lines the Swiss law project, and those of Portugal and the Netherlands.
- (10) On this extension of the notion of data sabotage and the arguments in favor of the extension, U. SIEBER, The International Handbook, op.cit., p.80 and s.

- (11) The debate in front of the German parliament is particularly instructive in this regard. A first project repressed 'any person who makes unauthorized use of data processing equipment and by so doing causes damage to another party, entitled to use it.' This first project was abandoned. On this topic, HARTMANN, *La criminalité informatique et sa répression par les réformes pénales en R.F.A., Droit de l'informatique*, 1986, no. 6, 11 and s.
- (12) For a more thorough discussion, SIEBER, *op.cit*, 85 and s.
- (13) For example, article 17 of the Belgian law of 13 October 1930 relating to telephone and telegraph; section 201 of the German Penal Code; paragraphs 139a and 139c of Holland's Penal Code; article 617 of the Italian Penal Code, etc.
- (14) In the case of the general disposition already cited on the topic of computer-assisted fraud.
- (15) Cf. For example, section 203 of the German Penal Code revised in 1986 which punishes 'any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access.'
- (16) Article 462-2 of the Penal Code revised by the law of 5 January 1988 speaks of fraudulent access, that is to say it demands 'dol spécial'. In this respect, M.P. LUCAS de LEYSSAC, *Fraude informatique - protection des systèmes de traitement automatisé de données - loi du 5 janv. 1988, Droit de l'Informatique et des Télécoms*, 1988, no. 2, p. 20 and 21.

CHAPTER THREE: The Protection of Data or of Individual Liberties

The protection of data or of individual liberties in relation to computer use in both public and private (1) sectors brings all the countries of Continental Europe (2) progressively towards implementing, each in its own way, the principles of the Council of Europe Convention (3) which have henceforth a direct legal value in the countries which have ratified it (4).

The examination of the principles of the Convention lead us to take account of the diversity of their interpretation in different countries (5).

The Council of Europe intends to protect only data on individuals, and not those relative to groups of legally-recognized existence. Certain legislation (Norwegian, Austrian, Luxembourgish) has, however, estimated that one of the objects of the legislation of protection of data, namely the struggle between discrimination among people and the difficulty, sometimes, in distinguishing between data relative to groups and that relative to individuals, members of these groups, justifies the extension of the principles of protection of data to groups.

Only the automatic data processings are concerned by the convention of the Council of Europe, but all of these without exception are concerned. French law (article 45), however, permits the control authority to extend to certain manual files, the principles of data protection (6). Recently, in 1982, Swedish law, and even more recently Holland's law of 1987, have set up special treatment for automatic data processings held in the scope of private activities, such as the agenda or the file of addresses held on a microcomputer by one private person for his own use.

The setting up of a data base is required to undergo, in certain countries, a preliminary procedure. The procedure takes the form often of a simple declaration, to the control authority, of the existence of a file and of certain of its characteristics. This is the case in Austria, France, Holland and Sweden. Denmark, Germany and Norway require a declaration only for the files belonging to the public sector, or held by enterprises which do not work directly in relation with the individual about whom the file contains information (commercial intelligence agencies, headhunters, etc).

The **principle of pertinence**, stated in Article 8 of the Convention of the Council of Europe, according to which the object of data processing must be:

- a)
- b) stored for determined and legitimate ends and must not be used in a manner incompatible with these ends;
- c) adequate, pertinent and not excessive in relation to the ends for which they are registered;
- d)
- e) conserved in a form that permits the identification by the interested person, for a period not more than is necessary to the ends for which they are registered.

is taken up by all the legislations of all Germanic countries: Austria, Denmark, Germany, Holland, Norway. It is based on a distinction between public files, files held for private use, and those containing information on a third person. The first may not register data except in the way prescribed by the law and only if the data is necessary for the execution of legal tasks. A recent case of the constitutional court of Germany on the subject of the statistic law applies these principles; it condemns the government for having insufficiently specified in this law the goals followed by the public processing.

Files held for private use, that is to say in relation to the person on file (such as banks, insurance companies, etc) can process data necessary for the service provided to the person on file. Finally, private files in the third category are held by companies whose profession it is to transmit to a third person personal information (such as credit insurance companies). These are subject to a more severe control.

The recent law in Holland goes farther still in this differentiated approach between the treatments and proposes a sectoral approach since it allows the organisations of a determined professional sector to make codes of good conduct whose object is the application of the law, and to demand the control authority for their ratification (7).

The interpretation of this principle of pertinence allows the legislations of the above-mentioned countries to distinguish between internal processing of data and its external communication, submitting the latter to the more strict laws (8).

All the legislations of Continental Europe institute a control authority: the French Commission Nationale Informatique et Libertés, the German Bundesbeauftragte, the Danish, Norwegian and Swedish Commissioner for Data Protection, the Registration Chamber in Holland, etc. These authorities have a role 'ombudsman': inspection of data processing, possibly holding hold a public register of these processings, assistance of people who are on file, above all advice on the intention of the governments and the legislation, finally, publication of a report. The members are named by the government (9).

Regarding **right of access** to files by the person whose information it contains, according to the Council of Europe, it is guaranteed in certain countries by the fact that the people who put someone on file are obliged to inform him about the processing of the file. This is the case in Denmark, France, Sweden and Germany, with several important exceptions. This right can be acted upon, given a payment whose amount is fixed by the government (10).

A number of countries regulate **transborder data flow** (11), notwithstanding the principle of article 12 of the Convention of the Council of Europe, announcing the suppression of all restriction between two countries adhering to the Convention and disposing the principles, granting to the people on file a similar protection. For example, article 32 of the Austrian law submits to the control authority's authorisation all transborder flow, article 21 of the Danish law similarly demands the authorisation or the consent of the person whose information a file contains, for the most sensitive data. Articles 19 and 24 permit the French government to restrain transborder flow. People in the European Community who consider these problems fear that the application of these dispositions do not permit the States to put in place non-tariff barriers for free services, affirmed by Article 59 of the Treaty of Rome (12) and plead for the adoption by all countries in the Common Market of similar principles that can be written into a directive.

SELECTED BIBLIOGRAPHY

Banque de données. Entreprises et vie Privée, Actes du colloque de Namur, CIEAU, Bruxelles, 1981.

R. PAGANO, Panorama of Personal Data Protection Laws, Camera dei deputati, Roma, 1983.

B. CATANIA, Dossier Privacy, Ed. Sarin, Torino, 1984.

J. de HOUWER, Privacy and Transborder Data Flows, VUB, Brussels, 1984.

PRIVACY: Notes

- (1) One notes that in the North American countries (Canada, the United States) the Privacy legislations are not valid except in terms of processing in the public sector.
- (2) Germany: law of 27 January 1977 (Bundesdatenschutzgesetz)
 Austria: law of 18 October 1978 (Datenschutzgesetz)
 Belgium: law project
 Denmark: law of 8 June 1978 on private registers;
 law of 8 June 1978 on public registers
 France: law no. 78-17 of 16 January 1978 relating to
 data processing, to files, and to liberties
 Greece: law project under discussion
 Holland: law of 17 September 1987
 Italie: law project under discussion
 Luxembourg: law of 31 March 1979
 Norway: Personal Data Registers Act, 9 June 1978
 Portugal: Article 35 of the Constitution;
 law project under discussion
 Spain: Articles 18 and 105 of the Constitution
- (3) The convention approved by the Council of Ministers, 17 September 1980, was opened to signature 28 June 1981.
- (4) At the actual moment, France, Sweden, Spain, Germany, Norway and the United Kingdom.
- (5) ... understanding that we choose each time the most original solutions.
- (6) Similarly, the recent law in Holland that extends the application of the law to all 'coherent assemblies of data...automatically managed or set up by systematic means with a view to efficient consultation of the data.'
- (7) Similarly, the system of the simplified declaration put in place by the French law that permits the authority to control and to permit the enterprises of a sector not to follow certain procedures if these respect the rules of processing set down by this authority.

- (8) For example, article 24 of the German law 'The transmission of nominative data is authorised in the limits of the relation - whether contractual or quasi-contractual or based on trust with the interested person - or as far as the protection of legitimate interest of the transmitting institution or of a third person, or general interest demanded and that this transmission does not endanger the interested person's right to protection.'
- (9) The composition of the French C.N.I.L. is more complex. The parliament, the magistrature and the government intervene in the nomination of the members. The point is to guarantee the independence of the commission as concerns the government.
- (10) On the right of access and its different methods of application in the countries of Continental Europe, read C. DEBRULLE, *Le droit d'accès*, in *Problèmes législatifs de la protection des données*, Conf. Intern. Madrid, 13 June 1987, Council of Europe, p. 33 and s.
- (11) On this question, our analysis, *Transborder Data Flows and Privacy*, in *Information Market - Legal Aspects*, G. VANDENBERGHE (ed.), Kluwer, Amsterdam, 1988, to be published, and the very complete study by J. de HOUWER, *op.cit.*
- (12) In this respect, the reflections of M. BRIAT, *Flux de données transfrontières et barrières non tarifaires*, in *Actes du colloque of the ABDI*, December 1987, to be published, and 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.

CHAPTER FOUR: Telecommunications

Traditionally, the regulation of telecommunications in Continental Europe was characterized by the existence of an extended legal monopoly, entrusted to a public enterprise, to which moreover was entrusted on one hand the regulatory power to decree the norms for the terminals, and on the other, the 'police d'éther'. Whether a question of the German 'Deutsche Bundespost,' the French 'Direction Générale des Telecommunications' or Belgium or Holland's 'Régie des Télégraphes et Téléphone', the pattern is similar. Only the Italian case of the S.I.P. and the Spanish one of Telefonica, those being public enterprises, or enterprises where the state has a strong majority, stray slightly from the pattern.

Such a confusion of the regulatory roles and exploitation has been denounced on several occasions by the European Commission (1) or in front of national tribunals (2), in the name of free enterprise.

The American and British deregulations, as well as the recent Green Paper of the Commission (3) had to bring most of the countries cited to progressively modify, little by little, their positions. The regulatory landscape of telecoms in Occidental Europe is clearly undergoing change: everywhere laws or law projects are looking to reconcile the existence of strong public service that one doesn't need to dismantle but whose autonomy is reinforced, with the principles of a sane and efficient management, affirmed by the Commission and already consolidated by a first directive (4) on the matter of liberalising terminal equipment.

Our subject brings us to an analysis of the evolution of two countries: France and the Netherlands. It is a question particularly for those two countries, of studying how they have understood the most important principles of the Green Paper:

- the necessity to clearly separate the activities of regulation and exploitation
- the possible maintenance of a monopoly on the supply and the exploitation at the time, of the infrastructure of the network and the services qualified as reserves, among which the Commission places only the vocal telephone; all others to be offered in a concurrent manner.

The French law of 30 September 1986 in relation to the freedom of communication (5) stipulates in Article One: 'The establishment and use of telecommunication installations are free'. If the actual wording seems to allow for a total deregulation, it must be recognized that other texts and the following to this text itself, presents certain major restrictions to the principle. Thus, Article L33 of the Post and Telegraph Code that consecrates the monopoly of telecommunication to the profit of a public enterprise, henceforth called France Télécom, is not abolished. It must be deduced that the freedom of communication is not total and is summarized according to Article 10 of the law of 1986 as an authorization system to which are submitted the establishment and use of telecommunications installations: 'The National Commission of Communication and Rights delivers the authorisations set up by Articles L33 and L34 of the Post and Telegraph Code for the establishment and use of all the liaisons and installations of telecommunication, with the exception of those of the state.'

The reader's attention is drawn to two points:

- the author of the authorisation is an independent administrative authority: the CNCL. Thus, not only is the separation of the activities of exploitation and use consecrated, but, further, participates in the regulatory function of the state, an independent institution of the government, and composed by experts on the model of the American FCC or the Canadian CRTC. The comparison with the Canadian precedent is extended when one considers that the CNCL covers the whole of the sector of telecoms and of audiovisuals.
- the authorisation is not given for all services.

A provisional decree of 24 September 1987 (6) thus limits what can be offered concurrently and what stays entrusted to the monopoly of France Telecom. Without going into the technical detail of the ordinances, note only the use of a criteria of originality (7) to delimit the notion of an added-value service, competitive service 'the legally existent group, says the decree, exploiting a system open to a third person... must respect, for each service offered on the network, between the amount of annual management charges corresponding to the activity of transporting the data, and the annual total revenue corresponding to the management of the telematic service, a ratio at the most equal to a determined percentage. This percentage, that can not be inferior to 1520, is fixed by decree by the Minister...'

With such legislation, the Netherlands intends at the same time to permit a rapid amelioration of their infrastructure by giving the public operator the financial means, and to become the place of privileged implantation of value-added service enterprises submitted to no restraints and having the right to demand of the operator the part of the infrastructure necessary to the development of their competitive activities.

SELECTED BIBLIOGRAPHY

R. BRUCE, J. CUNARD, M.D. DIRECTOR, From Telecommunications to electronic services, Butterworths, 1986.

C.R.I.D., Les Réseaux de Service à valeur ajoutée: quelle réglementation?, Cahiers de Recherche du CRID, no.4, 1989 (to be published).

E.J. MESTMAKER (éd), The Law and Economics of Transborder Telecommunications, Nomos Verlag, Baden-Baden, 1987.

OECD, Changing Market Structures in Telecommunications, North-Holland, 1984.

R.L. WHITE, H.M. WHITE, The Law and Regulation of International Space Communication, Artch House, Norwood, 1988.

TELECOMMUNICATIONS: Notes

- (1) Green Paper, op.cit., 65 et s.
- (2) For example, that which concerns Belgium, the prejudicial 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.
- (3) CCE, Project for a dynamic economy: Green Paper on the development of a common market of services and equipment of telecommunications, communication of the Commission in Council, Brussels, 26 May 1987.
- (4) Directive 88/JOI/CEE, 16 May 1988, O.J. no. L 131/73, 27 May 1988.
- (5) Law no. 86-1067 of 30 September 1986 relating to the freedom of communication, O.J. 1/10/86. The reader will find a commentary on this law in Juris PTT, no. 11, January 1988, 1 to 33.

It is not impossible that the new socialist government will modify the present law.

- (6) Decree of 24 September 1987 relating to special links and to telematic networks open to third persons, O.J. 25/9/87. This decree was made, given the impossibility of the government to accomplish the study on the law project on competition in telecoms. The text of this project would have led to more right-wing solutions.
- (7) The study on the law project cited in note 6 reserved for the public monopoly an elementary service of telecommunication, a service 'whose principal object is to transmit and direct the signals without submitting them to any processing not necessary for their transmission and direction.' (telephone service, service of data transmission by commutation of batches and circuits, telex service and rent of special links).

- (8) At the time at which this paper is being written, it still is now a law project, approved by the second Chamber of Parliament. Its text will probably not be further modified. The proposed date of inception is 1 January 1989.

Other texts are also under discussion: such as a law regulating the status of all postal services, another of the status of personnel.

- (9) For a text on the above-mentioned laws, read 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 and s.

CHAPTER FIVE: Telematic services, in particular those offered to the general public

The marriage of data processing and telecommunications has permitted, in Continental Europe as elsewhere, the birth of numerous services called 'telematic', after the expression of coined in the French Nora-Minc report. Next to the telematic services intended for the professional world are those developed for public use. If one thinks of the automatic tellers in banks (A.T.M.) or the point-of-sale terminals, certain governments have permitted, in the framework of voluntarist policies, the birth of multiple services: electronic directory, pink messages, electronic press, home shopping. One automatically thinks of the experiment of French Télétel (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 for France and Holland, that these experiments have created a true private market.

The aim of this section is to analyse succinctly the legal system that applies to these services (1), looking at the specific rules often put in place at the time of the introduction of these new services, but equally at the doctrine and the jurisprudence sometimes already well-established concerning electronic fund transfers.

The offering of telematic services to the general public is not subject to any preliminary authorisation (2). For example, the old French law of 1982 on audiovisual communication set up a provisional authorisation system; article 43 of the law of 30 September 1986 set up a system of simple declaration not applicable moreover to services of electronic messaging, considered a service of private correspondence (3). The German Bildschirmtextstaatsvertrag of 1983 gave the same right to all persons participating in BTX, under the sole provision of having a permanent base in Germany (4).

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 already mentioned French law oblige the producer to identify himself, to indicate the price per page and to clearly distinguish between advertising and information. Concerning electronic press, the traditional dispositions relating to the press apply: independence of journalists, financial transparency, nomination of a director of contributors, and respect of the pluralism 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).

As concerns relations with the users, in particular the delivery of the card or of the code necessary to use the services, a recent European directive proposition (5) relating to payment cards is inspired by the Danish law on electronic fund transfers and the American Fund Transfers Act (6). These texts oblige those who offer services to inform the users at the same time: responsibility for the system, the cost of the service, the frequency of the periodic statements, the procedures in case of error, and finally, the uses made of collected information.

The realization of the operations may result in other difficulties. Certain legislation (7) demand a signed paper as proof of a civil operation. The validity of inserted clauses in the general conditions of contracts permitting access to the telematic services according to which 'The registration of the automatic apparatus or its reproduction on computer data carriers count for the issuing organization as proof of the effected operations, which took place by means of the card or the electronic key with whom the systems operate' may be legally questioned, for the reason of consumer protection. For example, article 180 of the code of civil procedure in Holland stipulates 'Agreements which sets aside law on evidence are not admissible when they concern the proof of facts, which have legal consequences, and are not free to parties'. La Corte di cassazione italiana decided 29 January 1982 that the parties are not free to contract concerning responsibility for providing the proof when the position of one of the parties is weakened by the fact.

As a consequence, it seems that in Continental Europe, if no judge rejects a priori either the proof or the electronic (9) signature (8), however he reserves the right, notwithstanding the clauses evoked and the exigencies of the legal system in existence to examine the value of such recordings according to the technical and organisational criteria (10).

Concerning the question of the responsibility of the supplier of the card or the secret code, in case of loss or theft of the means of access, the clauses of a Belgian decision of the Court of Appeals in Liège concerning EFT are often cited as reference (11). The responsibility of the user ceases from when he reports the loss or theft. The responsibility then belongs to the supplier (the bank in this instance) to take all the 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 the American EFT Act, that in case of a delay in reporting the loss or theft, the responsibility of the user is limited, except in the case of recurrence or intentional act.

SELECTED BIBLIOGRAPHY

Y. POULLET - G. VANDENBERGHE (eds.), Telebanking-Teleshopping and the Law, Computer Law Series, Kluwer, 1988.

C. MONVILLE - Y. POULLET, La demande finale en télématique, Aspects juridiques, La documentation française, 1988.

T. BOURGNOIGNIE, M. GOYENS, J. LAFFINEUR, Questions juridiques liées à l'introduction de la télématique grand public, UCL, Centre de Droit de la Consommation, 1985.

F. VAN RYN, R. WILLIAMS (ed), 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, München, 1983.

La télématique, Aspects techniques, juridiques et socio-politiques, Actes du colloque de Namur, 1984, Story Scientia, Bruxelles, 2 tomes.

TELEMATIC SERVICES: Notes

- (1) **France:** Decision of the C.N.C.L. of 4 February 1988 relating to home shopping; Circular of 17 February 1988 taken in application with article 43 of the law no. 86-1067 of 30 September 1986 relating to freedom of communication applicable to certain services of audiovisual communication.

Italy: Decreto Ministeriale 17 May 1985/Istituzione del servizio pubblico 'VIDEOTEL'

Germany: Bildschirmtext-Staatsvertrag of 18 March 1983.

Netherlands: Viditelcode inzake reclame en interactief gebruik 1 January 1984.
- (2) Except that which concerns Italy where 'all VIDEOTEL service must be the object of the previous authorisation of the Minister subject to the obligation to respect the prescriptions of the conditions of subscription' (Ministerial decree, 30 October 1982)
- (3) Insofar as such services including pink messaging are considered correspondence services, they cannot be accused, at least according to the Paris Tribunal, of jeopardising public morals.
- (4) This disposition is considered by some as a breach of Article 59 of the Treaty of Rome concerning free service.
- (5) Draft Proposal for a Council Directive concerning the consumer and modern means of payment, The Commission of the European Community, XI/267/88, April 1988.
- (6) These are 'Law om betalingskat' danoise (1978) and the American EFT.
- (7) These are especially Belgian, French and Luxembourgish laws that legally demand a signed paper. Such legal dispositions are, however, legally considered as auxiliary. On this question of comparative law, B. AMORY, Y. POULLET, Le droit de la preuve face à l'informatique et à la télématique, Droit de l'Informatique, 1985, no. 5, 14.

- (8) An exception must be mentioned 'Le Tribunal de grande Instance de Sète' (9 May 1984) affirms that the so-called electronic signature is not equivalent to a legal signature.
- (9) On this conclusion, A. MEYBOOM, in Y. POULLET - G. VANDENBERGHE, *op.cit.*, 52 and s.
- (10) One notes that these are precisely the conclusion of the recommendation - in relation to the harmonisation of legislation concerning requirement of written proof and the admissibility of copy or of data processing
- (11) Liège, 22 February 1985, *Droit de l'Informatique*, 1985, no. 3, p.28, note B. AMORY, French jurisprudence is more hesitant. In favor of the responsibility of the cardcarrier, Douai, 26 October 1983, Pau 17 October 1983; Paris 29 March 1985, *Droit de l'Informatique*, 1986, 3, p. 120 and s; Against the responsibility of the carrier, Cass. 1 December 1980, *oed. loco*, p. 124.