# The Transborder Flow of Data - applicable Law and Settlement of Disputes, International Contracts for Sale of Information Services

Hanotiau, Bernard

*Published in:*
International contracts for sale of information services

*Publication date:*
1988

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

# THE TRANSBORDER FLOW OF DATA :

# APPLICABLE LAW AND SETTLEMENT OF DISPUTES

Bernard HANOTIAU
Professor at the Universities of Louvain and Namur,
Attorney-at-Law, Member of the Brussels and Paris Bar.

Translation from a French original.

CONTENTS

## I. GENERALITIES : OUTLINE OF THE SUBJECT WITH REFERENCE TO INTERNATIONAL CRIMINAL LAW AND PUBLIC INTERNATIONAL LAW - DISCUSSION OF PRINCIPLES

1. By its very nature, the international flow of data belongs to the domain of international law.

One is surprised that in the many studies that have been dedicated to the subject, the authors have spent so little time discussing the questions of applicable law and resolution of disputes. There is a double reason for such a silence : on the one hand the great difficulty, at the outset, of applying principles of private international law to a field that is quite technical and not very well understood by lawyers who specialize in that branch of law; on the other hand, the apparent absence of practical problems. Indeed, even the American case-law, which is always a bit avant-garde with respect to the new fields of law, does not seem, as of today, to contain one case on the subject that would have been decided by United States courts. There do not seem to be many decisions on the subject in other national case-laws either. A report of January 8, 1985, by the working group of O.E.C.D. on transborder data flow, underlined the absence of actual case law contributed by national delegations, and came to the conclusion that it was due to the non-existence of disputes (1).

Certainly, one can point to a certain number of criminal cases having an international dimension. Criminal law, nevertheless, is outside the scope of this study, which is dedicated to the law applicable to transborder data flow in civil and commercial matters. We will therefore focus on the problems raised by private international law as opposed to public international law and international criminal law.

2. At the criminal level, it appears that the development of data bank interconnections, made possible by the extension of international telematic networks, has developed computer fraud at the international level. It thus happens that one person, from a terminal located in A, can gain access to the CPU of a computer located in B, an act which can eventually produce effects on property belonging to a person domicilied in C. The question of which courts are competent and what law will be applicable has obviously to be raised.

It appears that the territorial criterium generally used to determine the applicable law is difficult to apply in the field of transborder data flow because the geographic

localization of the elements constituting fraud in a network of data transmission may be difficult to determine. Moreover, the elements constituting the offence may be localized within the territory of many states with the consequence that each of these states might very well assume jurisdiction, resulting in divergent incriminations or even an absence of a legal base for pursuing the offence. The problem arises in relation to those offences which require the existence of various material elements or when the offence is repeated in several jurisdictions.

3. If one takes again the example of one person situated in state A gaining access, by a non-authorized method, to the CPU of a computer located in state B, in order to manipulate the program so as to procure an illegal pecuniary advantage, are we in the presence of three separate offences or of a single one ? In the latter case, where is the offence localized ?

   If the legislation of state A qualifies an offence the fact to obtain directly or indirectly computer services without authorization, while state B requests that it be done with the intention of procuring for oneself or a third party an illicit pecuniary advantage, an action might be brought in the two states. This raises not only problem of court jurisdiction and application of the principle "non bis in idem", but also the general problem of international cooperation in criminal matters, most particularly the problem of the applicability and adequacy of existing treaties, notably those dealing with extradition, in the field of computer fraud. With respect to the issue of the competent court, many solutions have been proposed : the first jurisdiction in which suit is brought, the courts of the state where is gathered most of the evidence of the existence of the offence, or the courts of the state where the offence was perceived for the first time. The problem will not be solved until true uniformization of national laws is achieved or international conventions dealing with this problem are signed and ratified by the states concerned.

4. The problem in public international law appears much more simple. Indeed, there are several principles of public international law which define, to various extents, the rights and obligations of states with respect to the development of telecommunication networks and transborder data flows.

5. The basic principle is the free circulation of data. It is one of the foundations of the new international information order, such as discussed today at UNESCO, which desires to create a better distribution of information among nations. The principle of the free circulation of data is stated in

articles 18, 19 and 20 of the International Declaration of Human Rights and implies that states must act so as to aid access to information throughout the world, to guarantee the right to communication, the freedom of expression and the freedom of the press. However, because of the impact of this principle on matters of sovereignty, it has not received a uniform interpretation. Its most liberal interpretation postulates that governmental controls over the exchange of information should be reduced to a minimum except for those which confer protection upon certain informations considered confidential or secret or which prohibit false or misleading data to be divulged. The principle of the free flow of information, with its sanctions in case of non-respect, has not been unanimously accepted. Certain observers would prefer to have rules evolve concerning the free circulation of data which indicate clearly its borders and limits.

The principle of free circulation of data has received a blessing with respect to telematic matters in article 18 of the International Telecommunications Convention which affirms the right of the public to utilize the telecommunication systems and equipments. More precisely, article 18 affirms the right of those who furnish professional telematic services to supply their services within their country or abroad and the right of users to have access to them; at the same time, it affirms the obligation to assure equality of treatment between national and foreign suppliers, which notably implies that considerations other than those of a technical nature should be eliminated from consideration when deciding on rights to lines of telecommunication.

6. Two other principles recognized by numerous international conventions are equally applicable to the field of telematics : the principle of national treatment and the principle of most-favoured nation treatment.

The first principle implies that foreigners having commercial activities in a country should not be treated less favourably than nationals in the same circumstances. Although it has never become a principle of customary international law, it is included in a certain number of bilateral and multilateral treaties, such as G.A.T.T., the Bern Copyright Convention and the Paris Convention on the Protection of Industrial Property. This principle suggests, as a consequence, that foreign telematic services should benefit in a country of the same treatment as this country recognizes to its nationals. The principle is not, however, universally accepted with respect to transborder data flow, notably for reasons of national security and economic policy.

7. The principle of "most favoured nation treatment" forms the basis of G.A.T.T. Its first article states that foreigners and goods and services provided by foreigners should not be given less favourable treatment than that accorded to other foreigners or goods and services provided by foreigners to whom the state recognizes the most-favoured nation treatment. This implies that foreign providers of telematic services should all be submitted to the same conditions, but national providers might benefit from privileged treatment.

   It is equally doubtful that this principle will be universally accepted in the future, most notably by the states of the Eastern bloc.

8. Two other principles of international law are equally applicable to the field of transborder data flow : the principle of free transit and that of the confidentiality of communications. The principle of free transit is recognized by numerous international conventions, such as G.A.T.T., the Universal Postal Convention, the United Nations Convention on Law of the Sea, and the International Organization of Civil Aviation. According to the terms of this principle, when transportation from one nation to another involves transit through one or more other nations, this transit must be authorized without delay, whatever the mode of transportation which is used. The principle of free transit knows various exceptions, notably those which concern a transit which may be contrary to public order (article 19 of the International Telecommunication Convention). In other terms, the transit must be "innocent". Such is not the case with respect to the transit of informations which concern drug traffic, which threaten national security or which infringe upon intellectual property rights.

9. The principle of free transit is recognized today as a fact. One must remark, however, that access to information in transit is in principle impossible because of the principle of the confidentiality of correspondence, as stated in article 12 of the Universal Declaration of Human Rights and in the field of telematics, by article 22 of the International Telecommunication Convention under whose terms the member states agree to take all possible measures which are compatible with their systems of telecommunications to assure the confidentiality of international correspondence. The states must thus ensure that their networks will contain sufficient security and that they themselves will refrain from interferring with the communications which pass through their networks, exceptions being admissible only for reasons of national security or public order, in which case the procedure should be strictly controlled.

## II. POSITION AND COMPLEXITY OF THE PROBLEMS FROM THE VIEWPOINT OF PRIVATE INTERNATIONAL LAW

10. In the introduction I have outlined the problems from the viewpoint of international criminal law and public international law. The following developments exclusively concern private international law. In this regard, the development of information technology has opened new horizons and challenged the traditional concepts of law. The problem has so far been little analyzed. Apart from a study by Professor Rigaux on the law applicable to the protection of individuals with respect to personal data flows (2), one can find here and there only some very general statements on the subject, accompanied by regrets that the problem has not yet been the subject of a more intensive study, or that its evolution has not been such as to permit the presentation of clear and definite solutions.

11. Thus, the explanatory report of the O.E.C.D. guidelines exhorts the states to progress in the development of principles - at the national as well as the international level - to determine the law applicable to transborder flows of personal data.

According to the report : "As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed locations and rapid movement of data, and geographically dispersed data processing activity, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied".(3)

Concerning the protection to be given personal data, the suggestion has been made that preference should be given to the domestic law which gives greatest protection to such data, as long as this solution does not give rise to too much uncertainty.

12. If the problem of private international law has been mainly studied in the perspective of the transborder flow of personal data, it remains that the flows of commercial data are of such a nature as to give rise to even more disputes in

consideration of the greater multiplicity of connecting factors that may characterize commercial transactions which concern the transfer of information.

It is perhaps useful, in order to understand the complexity of the subject, to cite this paragraph by Mr William L. FISHMAN addressed to the Sub-Committee on Monetary Policy and International Finance of the U.S. Senate Banking Committee in November, 1981 :

"When an electronic message is generated in country A, switched in country B and C, transits country E, F, G and H, is processed in country I and J, stored in country K and involves entities residing in or operating in yet other countries, it is debatable whether existing choice of law and conflict of law doctrine are adequate. What law applies to data processing carried out by computer aboard a synchronous orbit satellite ? Do we need new forms of remedy for information theft, for information mishandling ? Do we need new rules on commercial entities' information rights and obligations ? New fora in which to prosecute these matters ? New law-making institutions ? If so, how do we get there ? Bilateral arrangements; multilateral arrangements; private contract law, world conference ? I do not know the answers; I know other countries are studying these questions and I know the United States is not, either in government or in the private sector." (4)

13. In terms of studying applicable solutions and without prejudice of the specific properties of each type of data, it does not seem necessary to make a distinction from the start between personal data and data of a commercial nature. Without prejudice of the qualification of the legal action, it does not seem necessary at the outset to make a distinction between the law applicable to a tort case initiated by an individual who complains of the communication of forbidden data which concern him and a case introduced by a company which is refused a bank loan and complains that the reasons for the refusal, possibly inaccurate, have been published by the international press.

14. Where can one find the solution to the question of the applicable law ? It is certain that the answer would be easier if the states concerned did adopt uniform rules on the subject or were parties to international conventions, the drafting of which is strongly suggested by prominent authors, some of whom propose their elaboration at the Hague Conference on Private International Law.

It remains that those suggestions made little impact when they were formulated with respect to other fields. Even if a working group has been formed at the Hague Conference, the degree of desirable harmonization will not be achieved tomorrow. Consequently, the problem must be examined at the outset with reference to the state systems of private international law.

From this point of view, to analyze the problem uniquely in terms of conflict of laws is insufficient. The technique of "rattachement" is only one of the methods of private international law. It is not sufficient by itself to resolve the various questions raised by transborder data flows.

It is equally necessary to approach the questions of the applicability of the rules of public law or administrative law, the application of public policy principles (lois de police), as well as that of the field of application of national rules of private international law.

15. Before proceeding to this study, two points must be first mentioned. The first one concerns methodology. The questions relating to intellectual property, that is to say the protection of software and data banks on the one hand and of works which are reproduced in data banks on the other, will not be dealt with in this report. The protection of intellectual property is governed at the international level by the Bern Convention of October 9th, 1986, and of the Geneva Convention of September 6th, 1952, as well as of numerous national laws. There is little doubt that the protection assured by these conventions and legislations also applies to matters involving professional telematic services.

The second observation concerns the determination of the international character of a telematic operation, a condition indispensable to the application of rules of private international law. In situations in which this question will be raised, the answer may not be always easy. One must therefore wonder whether it is not desirable to retain and to apply to the field of telematic flows a presumption that all data flows have in principle an international character, the opposite proof having to be made by those who plead the contrary.

## III. THE METHODS OF PRIVATE INTERNATIONAL LAW

16. The determination of the law which governs transborder flows requires, first of all, an understanding of the methods of international law, whose mastery is indispensable to the solution of the problems encountered.

### A. The technique of "rattachement"

17. The method most characteristic of private international law is that of "rattachement".

The forum court does not always apply its own law. It is a principle of private international law that legislative competence and court jurisdiction cannot necessarily be superimposed. In handling a dispute the judge will determine the applicable law through application of rules of conflit of laws. Those are in principle multilateral in the sense that they determine the applicability or non-applicability of the law of the forum as well as of the law of foreign countries. Rules of conflict will permit, by means of a connecting factor, the localization of the situation within one selected state, in principle the state with which it is more closely connected and whose laws should therefore govern the dispute.

The technique of "rattachement" is the principal method applied to matters of private law : contracts, torts, family law.

### B. The rules of public and administrative law

18. The applicability of a particular rule of public or administrative law to a particular case is not determined by recourse to a rule of conflict of laws. Public law has a strictly territorial character. With respect to public law, every state only applies its own rules of substantive law, to the exclusion of foreign law. The rules governing public law are thus territorial from the dual viewpoint of substance and form. The problem raised by the rules of public law and administrative law does not really belong to the conflict of laws in a strict sense but rather requires the territorial determination of situations to which they apply : thus one will try to determine to what facts located within its territory the forum will apply its own rules.

This method is important to the extent that a great number of rules which concern the treatment of data belong to administrative law : they provide for various declarations, authorizations, and controls by administrative authorities.

This second method of private international law is equally characterisic of public policy statutes (lois de police).

C. Public policy statutes (lois de police)

19. Certain legal provisions touch upon fundamental principles which are intimately linked with the organization, both political, economic and social, of a nation. Because of that fact they are qualified public policy statutes, with the consequence that a judge sitting in a state in which such public policy rules have been promulgated will have to apply them notwithstanding the law declared in principle to be applicable under the conflict of law rules of the forum. One must also admit that a court could just easily apply foreign public policy rules, even if today this hypothesis is only rarely verified.

The compulsory rules concerning the treatment of data are rules of public policy, e.a., the rules which define the categories of data whose collection and treatment are prohibited.

Public policy statutes are territorial in terms of substance in the sense that those who are addressed by such rules must respect them when a particular situation presents with the territory in which they are applicable those connecting factors which will give rise to its application.

The application of public policy statutes requires that one defines which situations connected with the territory will justify their application. They are therefore related to the second method of private international law.

D. The material rules of substantive private international law

20. Finally, particular attention must be given in the field of transborder data flows to national rules of substantive private international law.

If in the majority of cases, and outside the ambit of rules of public and administrative law, every international situation is ruled by a state law whose applicability is determined by the rules of conflict of laws of the forum, there may nevertheless be cases in which the state legislature, after having handled a typical international situation, decides to promulgate a rule of substantive law applicable to that situation. Instead of determining from the localization of the connecting factors which substantive rule is applicable, precepts of substantive private international law will determine directly the legal effects and status of

the situation. They include accordingly, an implicit solution to the problem of conflict of laws which consists of generally according competence to the lex fori.

## IV. LEGAL RELATIONS BETWEEN PARTIES TO A TELEMATIC CONTRACT

21. When it comes to legal relations between the producer or the supplier of services and the distributor, between the distributor and the user, or between the record keeper and the user, such relations are in principle contractual, whether or not a written contract exists.

Where a contractual relationship exists, the law applicable to the relationship is determined by the terms of the contract (law of autonomy). This principle, recognized by most national systems of private international law as well as by all international conventions means that in general, parties to an international contract are free to choose the law applicable to their contract, although they may not be able to avoid the application of public policy statutes.

Do parties make use of this prerogative ? An analysis of contracts reveals that in a certain number of them the parties have not determined the applicable law. In the others, the law chosen by the parties has generally been the law of the state in which the provider of the services sensu lato has its headquarters. Except in the case of arbitration, the tribunals of this state are also declared competent.

22. What law will be declared applicable in the absence of a choice by the parties ? That will normally depend on the court handling the dispute. One must mention again that given the rules of international jurisdiction, when there is an interpleader or a summons jointly against two defendants having their residences in different states, the state before whose courts such a dispute will be brought may not have been foreseeable when the contract was concluded. Each state applies its own rules of private international law, with the consequence that the ultimate solution of the dispute can vary from one state to the other.

Generally speaking, however, the majority of states today apply to contractual matters similar rules for determining the applicable law in the absence of a choice by the parties, even if the formulations may be different : research of the presumed intention of the parties, objective localization by simple enumeration of contacts or application of the theory of the characteristic performance. Whatever the method, the work of the court generally consists in determining which is the state whose relationship to the situation and the parties is the most significant. With respect to contracts for

telematic services it will normally be the state where the provider of the service, sensu lato, is domiciled or has its headquarters.

23. It is also the law of this state which is designated by application of the Hague Convention on the law applicable to the international sale of goods and the Rome Convention on the law applicable to contractual obligations. The former provides in its article 3 that when the parties have remained silent or have not clearly expressed their intent in the contract, the applicable law is the domestic law of the country where the seller had his usual residence at the moment when he received the order. As far as the latter Convention is concerned, its article 4 states that in the absence of a choice by the parties, the contract will be governed by the law of the country with which it has the most significant relationship. This law is presumed to be the law of the country where the party who must fulfil the characteristic performance has his ususal residence at the moment of the conclusion of the contract, or if it is a business entity, its principal place of business or, at least, the business place from which the services are supplied, if it is different from the former.

24. The best advice that one can give to parties to a telematic contract is to state to the extent possible the law which will govern their relations. Of course, this law will be applicable only to their contractual relations; it will not be applicable, for example, to an action brought by a third party. However, an interpleader by the party defendant to the other party to the contract should, arguably, be governed by the law stipulated in their agreement. Where it contains specific provisions concerning warranties for the services supplied, the liability of the contracting parties, and the limits of that liability, each of the parties can determine in advance with a maximum of security and previsibility the limits of his undertakings.

25. One will finally note that to avoid uncertainty with respect to the determination of the law applicable in absence of a choice by the parties, some authors have proposed the conclusion of an international convention which might also propose a certain number of standard clauses whose adoption would be suggested to parties negotiating an agreement.

26. What is the scope of application of the law chosen by the parties or declared applicable in the absence of such a choice ? It will govern, among other things, the validity of the contract, the contractual liability of the parties and the sanctions in the event of non performance of the agreement.

## V. NON CONTRACTUAL ACTIONS

27. It may happen that the parties to a dispute are not in a contractual relationship. With respect to data of a personal nature, one would think for example of a tort claim filed by an individual against the record keeper on the basis that the data contain informations that are inaccurate or prohibited concerning the plaintiff. With respect to data of a commercial nature, such situations can be extremely varied and one can cite as an example the following case reflecting an hypothesis proposed by C. OLMSTEAD. (5)

Assume that the German subsidiary of a multinational corporation X having its headquarters in New York requested a loan from the Hamburg branch of Telebank, an American bank, with its headquarters in New York. The request was for a loan of Euro-dollars in the amount of $ 200,000,000 which would be payable in Luxembourg and guaranteed by the financial subsidiary of X in that country. The German subsidiary furnished with its loan request detailed information concerning the financial condition of X, comprising its capital status, its projects ... and the justification for the loan. The German branch of Telebank, utilizing an international telecommunications service furnished by a corporation established in the Bahamas, sent the request with the accompanying documents to its headquarters in New York. The information was sent in digital form with an authentification code. The data were transmitted via the regional bureau of Telebank in London. As soon as they arrived in New York, the data were sent to Hong Kong to an organization of information services with which Telebank had an on-going contract for handling loan requests exceeding $ 100,000. This organization compiled a data bank concerning debt/equity ratios, both in general and by industry or type of activity of the borrower. Its services also made possible to verify the informations supplied by the borrower to the bank by comparison with other data in its possession. After these various verifications, the results were transmitted to Telebank in New York through the telecommunication network. In this particular case, Telebank received the information that X had furnished false data concerning its capital and its undertakings. Telebank therefore decided, at its office in New York, to reject the loan request of X and, passing a message through its telecommunication network via its regional office in London, let Hamburg know of its decision to reject the loan because of the erroneous information furnished by the applicant. The branch of X in Hamburg was informed of the rejection but not of the reason for it. That

same day an important financial magazine in London, the "Economic News", published an article containing a statement that the loan had been rejected because of a false declaration of X when making its loan application.

28. In a situation of this nature a certain number of actions can be considered. On the one hand, the subsidiary of X in Germany could institute an action against the German branch of Telebank. The relations between these two parties is contractual and in the absence of a provision in the agreement exonerating the bank from all liability, one will assume that the bank should be declared liable for not having taken the necessary steps to prevent the leakage of confidential information. The obligation of the bank might be qualified in this regard "result obligation" (obligation de résultat). At this stage, the subsidiary of Telebank might as well have an interest to bring its insurance company into the matter. And if it has reasons to think that the "leak" can be attributed to the Bahaman corporation which has supplied the telecommunication service or to the Hong Kong company, it might bring an action against one or the other of these corporations, likewise on a contractual basis.

If, on the other hand, the German subsidiary of X decided to bring a tort action against the English magazine "Economic News", because of the considerable injury it has incurred following the publication of the article, such an action would lie outside the sphere of contract law. It involves a tort claim. The same would be true of an action brought by an user against the owner of a data bank, in circumstances in which his contract with the provider contains an exculpation clause rendering illusory any recourse against the latter.

29. In such a case what is the applicable law ?

It seems to us that the rights and obligations flowing from the production and transmission of damaging data should be determined in conformity with the law applicable in the state of the residence of the injured party or of its principal place of business if it is a corporation. It is in this state, ultimately, that the individual or the corporation will suffer injury. The question is a bit more problematic in cases in which there was no transmission of data into the state of the residence or the principal place of business.

The solution should nevertheless remain the same to the extent that the injured individual or corporation concernedd will obviously suffer in that state the effects, even though indirect, of the damage caused in another state.

30. Prominent authors and various decisions of private international law may be cited in support of this solution.

Numerous national systems still apply to tort cases the lex loci delicti, the law of the place of the tort. To the extent that this law is not conceived as being the law of the state in which the act generating the tort was committed - which might be difficult to determine in situations involving telematic matters - but as being the law of the state where the damage took place, it necessarily leads to an application of the law of the residence or principal place of business of the injured party.

The same solution is reached in the United States by application of the rules of the Restatement (Second) on Conflicts of Laws, with respect to inter-state defamation or inter-state violations of privacy. Article 150 of the Restatement (Second) states that the rights and liabilities that arise from defamatory statements which are made public in more than one state are determined by the local law of the state which, with respect to the particular issue, has the most significant relationship to the occurrence and the parties. It is specified that this state will generally be the state of the domicile of the individual or the place of incorporation of the corporation which is the plaintiff, at least if the defamatory statements were also made public in that state. A similar rule is provided in article 153 of the Restatement (Second) in case of violation of a person's right of privacy by means of an oral or written communication which is published in more than one state.

The law which is applicable will determine the conditions of an eventual liability as well as its extent and effects.

31. One will note that with respect to data of a personal nature, Professor RIGAUX suggests the application of the law inforce at the principal place of business of the corporation which generates the file, but admits however, that there are very persuasive arguments to be made in favour of the application of the law of residence. The argument invoked by RIGAUX, i.e., the efficacity of the solution since it is unlikely that the courts of the country of residence will apply a law other than their own, is not decisive. If an action is brought against both the owner of the file or the producer and the user, it will generally be possible to introduce it in the state where the former is domiciled which will often be the state of plaintiff's residence.

One might equally conceive that the state of residence might subordinate the authorizations which it is required to deliver to the acceptance of the jurisdiction of its courts.

## VI. PROTECTIVE LEGISLATIONS : THE REGULATION OF PUBLIC INFORMATION

32. The regulation of public information, which includes a collection of rules considered by the states which have adopted them to be fundamental and, consequently, not to be interfered with, has involved the adoption of statutes on the protection of data and the privacy of individuals, of legislations protecting the confidentiality of informations held by companies, of statutes on computer crime, or concerning defamatory or misleading publicity. These statutes will be to some extent considered public policy statutes, in the same sense that these have been defined hereinabove.

33. From the point of view of private international law, the following problems are likely to arise (the list is not exhaustive) :

- what is the scope of application of legislations protecting or prohibiting the processing of certain data ? Does the prohibition only concern nationals ? Is it permitted to import into State Y, a state having passed such legislation, data which are prohibited but which concern only foreign individuals or corporations ? Can an individual residing in a foreign state X take advantage of the legislation of state Y to bring an action against the user of the data ?

- To which data does the control procedure set up by the state legislation apply ? Does the eventual obligation of prior authorization or of information of the individual or corporation concerned, only apply to the residents of the state having promulgated that obligation or is it also applicable to the corporations having an office in that state ? What individuals or corporations will be allowed to obtain the rectification of errors of fact or the radiation of illegal data ?

- To the extent that various statutes have an extra-territorial scope, is it not possible that their application will give rise to conflicting legal obligations ?

### A. The field of application of protective legislations

34. Among the statutes which regulate the automized treatment of data, some of them do not contain any indication as to their territorial scope of application. It is the case of the French statute; other statutes, on the other hand, contain at least some indications as to their territorial scope.

Thus, the Canadian statute provides that "individual" means every Canadian citizen and every person legally admitted in Canada with the status of permanent resident, in accordance with the law of Canada.

As was indicated by Professor RIGAUX, to make such restriction to the personal or territorial scope of the statute does not solve the conflict of laws problem.

"A l'intérieur d'une compétence législative donnée, ces dispositions subordonnent la mise en oeuvre des règles substantielles qu'elles accompagnent à une condition propre aux personnes protégées, en l'occurrence à une condition de nationalité ou de résidence, de la même manière que la protection aurait pu être restreinte aux militaires ou aux personnes exerçant une profession déterminée".(6)

Accordingly, one must determine, within these limits, what facts come into the competence of the state legislature.

35. On the other hand, if certain statutes include some self-limitation on their scope of application, other statutes contain rules of substantive private international law. These statutes submit a fact localized on their territory to the application of a specific rule of substantive law, adapted to the international character of the situation.

One can cite as an example article 21, 1 of the Danish statute N° 293, which prohibits the collection of data for the purpose of their recording outside the territory of Denmark; or article 3, 3 alinea 2 of the Luxembourg statute of April 11, 1979, which places under its control data imported in the Grand Duchy of Luxembourg. Such provisions contain an implicit rule of conflict of laws since they assume that the state which has adopted them has decided that it had competence to enact such regulation.

B. Territorial application of protective legislations

36. The statutes which have been adopted by different states concerning the automized processing of data prescribe in general measures of declaration, authorization or control, that is, measures of an administrative nature.

The narrow relationship between such measures and the administrative order will be reflected in the solution of the conflict of laws. Indeed, an administration never applies anything other than its own law. It will never follow foreign provisions. The administrative order will proceed to controls and will grant authorizations required by the lex fori in all the cases in which the latter is applicable to the situation concerned.

The problem from the viewpoint of private international law will not consist in determining which law will be applied by the authorities of the state concernedn but rather to which facts the lex fori may be applied. By reason of the very nature of such rules, their application will presuppose the localization of the processing elements within the territory of the forum.

The transmission of data in various states therefore presupposes, as the case may be, compliance with the provisions of an administrative nature contained in the rules in force in the different states, to the extent that the scope of spatial application of these rules makes them applicable to the particular situation, in consideration of the connection of the particular factors with the territory of the state concerned.

Actually, the rules of administrative law concerning the processing of data also have an important bearing in the sphere of private relations. Their spatial scope must be determined on the basis of the policy that the legislature had in view, i.e., the protection of the privacy of its people. Such provisions will therefore normally be applicable to all personal data involving people connected with the state which has enacted the rules.

C. Conflicting legal obligations

37. To the extent that some protective legislations have an extra-territorial application, they may give rise to conflicting legal obligations. One might cite the case, for example, where a corporation having its headquarters in state A organizes its internal structure in such a manner that its files are located in state B and accessible to state A by means of a data transmission network. In such a case if an investigation were to be brought in A, could the authorities of the latter state have access to the files situated in B by utilizing the telematic network of the corporation ? One might be tempted to answer in the affirmative but what should be the answer if according to a statute in force in B, it would be forbidden to communicate such informations to foreign authorities ? Or if the authorities of state A would conduct an investigation following a complaint lodged by citizens of A according to which the data bank located in B contains informations which concern them and whose storage, even outside the country, is forbidden by the legislation of state A ? (7)

Such situations can only be solved in the context of international conventions or if the states concerned agree to adapt their legislations to guidelines elaborated at the international level.

## VII. RECOURSE TO ORNIDARY COURTS OR TO ARBITRATION

Contracts for information services most often include an arbitration clause or a clause granting exclusive jurisdiction to the courts of a particular state. In a field as technical and difficult as transborder data flows, recourse to arbitration appears preferable. It, however, entails certain inconveniences, to the extent that the consolidation of several actions might be required.

In non-contractual matters the dispute will be brought before the court of the principal place of business of the defendant or of one of the defendants, or before the courts of the state where the tort ocurred.

FOOTNOTES

(1) O.E.C.D., Document DSTI/ICCP/Q85.4, Situtations juridiques contradictoires dans le domaine des flux transfrontières de données.

(2) Revue Critique de droit international privé, 1980, 445. See also HANOTIAU B., "Les flux transfrontières de données et la problématique du droit international privé", in La Télématique, Aspects techniques, juridiques et socio-politiques, T.II, Story-Scientia, 1985, 175 and the bibliography in footnote 1. See also OLMSTEAD C., "Transborder Data Flows; Legal issues including Conflicts of Laws", working paper presented at the seminar organized in London on October 16 and 17, 1985, by the International Law Association on the topic "Operational and Legal Aspects of Transborder Data Flows"; BING J., Transnational Data Flows, p. 108 and following; SCHAFF Sylvie, "La dimension internationale des services télématiques professionnels", working paper, Centre droit et informatique, Facultés Universitaires de Namur, 1986; H.P. LOWRY, "Transborder Data Flow : Public and Private International Law Aspects", 6 Houston J.Int.L., 159 (1984)

(3) O.E.C.D. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Explanatory Memorandum, 36, reproduced in International Legal Materials, 1981, 427

(4) Testimony of W.L. FISHMAN, United States Banking Committee, Sub. Committee on International Finance and Monetary Policy, 9th November 1981, pp.10-11, Mimeographed, cited by M.D. KIREY, "Legal Aspets of Information Technology", in An Exploration of Legal Issues in Information and Communication Technologies, ICCP Series, n° 8, OECD, 1983, 33

(5) Op.Cit., note 2

(6) Op.Cit., 459

(7) See for example OECD, International Investment and Multinational Enterprises, The 1984 Review of the 1976 Declaration and Decisions (July 1984)