# Privacy Protection and Transborder Data Flow. Recent Legal Issues

Poullet, Yves

*Published in:*
Advanced topics of law information technology

*Publication date:*
1989

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

# Privacy Protection and Transborder Data Flow; Recent Legal Issues*

*Y. Poullet***

## INTRODUCTION: TDF POLICY CHOICES AND LEGAL ISSUES

Transborder Data Flow ('TDF') is international Data communications defined as all kinds of electronic transmission of personal or non-personal informations across political and cultural boundaries for processing or storing in computer files. Today, the increasing uses of Telecommunications channels and the merger of previously disparate telecommunications and computer technologies have rendered the transfer of data from one country to another country commonplace and have created an emerging international information economy.

So, the legal environment of these international information flows is receiving more and more attention because of their significance for the economic growth and international trade. To quote the ICC declaration, 'there is a vital need for an unrestricted flow of business information. This position arises from four basic perceptions:

- the vital importance of the efficient exchange of information in the development and growth of modern international trade and production;
- the right of business to communicate freely within and outside its corporate structure;
- the right of business to access and utilize national and international communications facilities on a fair, competitive and non discriminatory basis;
- the necessity of recognizing the worldwide interdependence of modern business communications.' (ICC, Information flows, 1984)

If the legal framework can constitute a tool for developing international information flows, it can also create *potential barriers* thereto. Multinational enterprises and the US government have complained bitterly about what they call neo protectionist measures taken by several countries, including some

* This article has been written in June 1987. It does not take into account more recent publications in this field.

** Professor of Law, and director of the *Centre de Recherches Informatique et Droit* of the University of Namur.

developed nations like european western countries and Canada. These barriers have been erected for different reasons, some economic in nature, others founded both on their conception of the national sovereignty interests (problem of the cultural and industrial dependence on foreign data banks) and upon a genuine concern for the protection of individual privacy with respect to the sensitive data stored in foreign computer systems (Cf. The conclusions of the Canadian Clyne Report).

To summarize, 'the issues raised under TDF label relate to national sovereignty, national security, competitiveness and productivity regulation, employment, culture, privacy, protection and computer related crime' (Robinson) without forgetting taxation and intellectual property.

This article is focused only on one of these barriers: the *privacy protection.*

Historically, the debate 'Free flow of information' versus Privacy began in the early 70's with the development of various national regulations in European western countries. This debate encompasses different topics important to be distinguished.

Firstly, it is obvious that the diversity of regulations in this field create a barrier to international flows of information. The legal requirements for storing or disseminating sensitive information are deeply different and can constitute a source of economic and organisational problems for the companies which develop international business activities.

Furthermore, certain countries, before the increasing development of TDF, have explicitly regulated the transfer or the storage of sensitive data abroad with the avowed intent to protect their citizens from their improper use of personal data transferred extranationally. These legislations prohibit the export of such information under specified conditions.

More recently, the so-called freedom of information legislations enacted in certain countries (Cf. the analysis of these legislations provided by H. Burkert (1987)), permit to third parties to gain access to business information in one country, information which is unavailable in another nation. 'Therefore, an international company may seek to avoid the glare of disclosure by locating its particularly sensitive corporate records beyond the borders of that country unless secrecy can be guaranteed for the records it must submit to the governmental agencies there.' (Rankin)

Finally, one must underline the emergence in some European countries of the concept of a 'corporate privacy'. These regulations grant the right to corporations exactly like to individuals of inspecting other corporations' records in which they are identified. This new regulatory trend can affect very deeply the TDF

This overview of the various topics arisen in the context of the debate 'TDF and Privacy' leads to propose the following framework:

- first, the analysis of different national provisions contained in privacy regulations restricting or prohibiting international flows of informations and their practical application;
- next, the international efforts to reduce the national discrepancies in respect to privacy regulations (Council of Europe, OECD) and the problems expressed by the concept of 'equivalency';

– finally, the discussions arisen from the granting to corporates of a right of access by extending the privacy regulations to them.

## 1. National Privacy Regulations and TDF

As mentioned above, a major problem in enforcing Privacy regulations and securing the rights of the data subjects is the possibility of using a computer system outside the national territory and thus creates the fear of data Heavens. Before to comment the national provisions answering to this fear, it is important to point out that no more than ten percent of TDF are concerning individual data (OECD).

Against these situations, national regulations have developed two kinds of provisions. Firstly, they provide that certain transborder flows are considered as *submitted to the national provisions* because one major element of this flow is located inside the territory. Secondly, most of the regulations provide explicitly the possibility for the national Data Protection authority or directly for the government to *control the flows of personal data* to systems located in foreign countries.

### *Extraterritorial Application of the National Legislations*

The first kind of provisions create what one can call an extraterritorial application of the national regulations. These provisions clearly presume that the location abroad of the computerized system is not in itself sufficient to remove the system completely from the scope of the national regulations (Bing, 1986). One can distinguish different ways to regulate these situations (Olmstead).

So, the Danish act for the private sector provides that in case of exportation of individual data, the exporter should have to obtain from the foreign party warranties that the system abroad would be submitted to the substantial provisions mentioned in the Danish Act. At the other side, the Austrian, Luxemburgian and Swedish laws for example provide that a system located abroad and containing data on national citizens is submitted under their national laws if the foreign system is accessible from a terminal located from-their territory. The criterion of the application of the national regulation is thus the *location of the user and no more the location of the system(Rigaux)*.

The adoption of this criterion leads to an important extension of the scope of the regulation. With the development of the telecommunication services, it is obvious that most of the systems located abroad are accessible from another country and thus would be submitted to at least two national regulations, the regulation available in the country where the system is located and these available in the country where the system is used.

The imprecision of the criteria adopted is also to underline. If one can easily understand the major preoccupation of the national legislators to protect their citizens, although to avoid the multiplication of possible conflicts of law, it would be mandatory to distinguish occasional uses by remote terminal of systems located abroad, which do not create real dangers for the citizens and *intensive uses* by which an enterprise finally searches to avoid its national

regulation, location of its data bases in a foreign country. That's why one can suggest that an additional criterion would be employed like the criterion of the 'data controller', term used by the convention of the Council of Europe: the national regulation would be considered as applicable to systems abroad, only if the finality, content and uses of the data base even located abroad are decided from the national territory.

### *National Provisions Regulating the TDF*

Different ways are followed to regulate the TDF (Briat, Bing (1985) De Houwer): In Denmark, for example, a license of the Data Surveillance Authority is needed in two cases (Sect. 21 Private Sector Act):

'(1) if the data are collected in Denmark for inclusion in a system subject to license (Credit reporting Agencies, Black-listing), or sensitive data are collected for inclusion in a foreign register;

'(2) export of a register as such for processing abroad, if the register includes sensitive data'

Furthermore, article 6 prohibits collection of high sensitive data outside of Denmark, including notally sexual habits, criminal sanctions, etc..

In France, article 24 of the Privacy Act asserts:

'Sur proposition ou après avis de la commission informatique et Libertés, la transmission entre le territoire français et l'étranger, sous quelque forme que ce so it, d'informations nominatives faisant l'objet de traitements automatisés régis par l'article 1§ ci dessus peut être soumise à autorisation préalable ou réglementée selon les modalités fixées par décret en Conseil d'Etat en vue d'assurer le respect des principes posés par la présente loi.'

The same provision is provided by the recent Belgian Bill.

The German legislation lacks explicit clauses regulating TDF. Although, the practice of the German commissioner is to ask to the foreign computer bureaux located abroad, either to be submitted to a regulation available within the country of its location, equivalent to the German data protection legislation (regarding this concept, see infra), either to take an agreement ensuring to the data subjects the same protection then these available within federal Republic of Germany.

The Austrian case is still more interesting: the transfer of automatically processed data out of Austria shall be permitted on certain conditions:

- that the person affected has given his express consent, which consent may be revoked in writing; or
- that the disclosure of the data forms part of the legitimate purpose of the person responsible ; or
- that the disclosure is necessary for the protection of the overriding and legitimate interests of a third party; or
- when appropriate measures are taken to ensure that the person affected can no longer be identified by the recipient of the data.

The approval of the Austrian Data Protection Commission is needed and this approval shall only be given if different conditions are met:

- the transfer does not run counter to any public interests;
- it is established that the transfer will not damage interests of the affected persons warranting protection;
- the transfer abroad is made for the purpose of data processing as part of a service and adequate measures are agreed upon to ensure that the transfer shall return the data and any results obtained by processing them solely to the person responsible or shall disclose them solely in accordance with the instructions of such entity.

In Norway, TDF are regulated as follows: since 1981, the transfers must be notified to the Data Inspectorate (before a special permission of the King was needed) which may refuse to allow the transfer or set conditions to this export. Specific informations must be given to the Data Inspectorate, such the country to which the data will be exported, why they are exported and the method of transferring the data.

In certain countries, specific regulations prohibits the exportation of specific data (see already, the Danish Case) providing that certains computer records must be localized inside the country. For example, the 1980 Revision of the Canadian Bank Act (§157 (4)) explicitly provides a minimum set of records to be maintained in Canada and stipulates that all such bank records must be processed there. Furthermore, the inspector of banks may countermand any move outside Canada if he determines that such data processing undermines his oversight responsibilities (Rankin). It is obvious that such regulation encompasses not only the Privacy problems even if this preoccupation is explicitly mentioned but also the 'national sovereignty' questions (Yarn).

The concrete and effective application of these national principles is rarely discussed. It is right, as underlined by the British Lindop Committee, that data protection authorities have effectively imposed some restrictions on the export of data. To prove that, we will only refer to the conclusions of the Scandinavian experience as studied by J. Bing (1985).

In their first decisions (especially in Sweden), the data authorities merge often the Data Protection aspects and the national sovereignty or security interests; the necessity to insure the independence of the country from decisions taken outside the country is the major preoccupation in certain negative decisions towards registers of large fractions of the population, located abroad but containing no sensitive data and used for legitimate purposes (so the fabrication of magnetic cards). Progressively, the data protection authorities seem to distinguish better between these two topics and concentrate only their control on the privacy problems.

For giving a positive answer, the data authorities take especially into account the nature of the data exported, the purpose of the storage abroad, the adequate security measures taken and overall the remaining control of the national enterprise during the period the data reside abroad. Finally, they are considering the existence of an equal or at least equivalent Data Protection legislation in the country where the data will be exported. For instance, the Swedish Data Protection Authority has denied to Swedish enterprises to export certain individual data to Belgian enterprises with the argument no Data Protection regulation exists in Belgium.

Finally, one points out that Data Protection authorities are often giving their authorizations with conditions and after negotiating or suggesting some accommodations to be sure that no abuse will be committed (like transfer of data in anonymized form only for the production of statistics: Norwegian IBM Case).

## 2. The International Efforts to Harmonize the Privacy Regulations

We have underlined that in their application of the national Data Protection provisions, in regard to the TDF, the Data Protection authorities have laid great stress upon the existence in the foreign country of an *equal* or *equivalent* Data protection regulation than within their own countries.

In fact, it quickly became evident that the development of national laws could lead to a highly intricate and unsatisfactory situation for enterprises working at international level and having to satisfy to each national regulation. It is obvious that the discrepancies between national regulations can inhibit the growth of international data flows.

### *The International Instruments*

Accordingly, in 1980, the OECD and the Council of Europe both adopted an international instruments designed to harmonize the development and application of national laws and avoid restrictions on international information flows. These two international instruments are of different species.

The Council of Europe document adopted by the Committee of Ministers in Strasbourg, the 23 September of 1980, is entitled: "Convention for the protection of individuals with regard to automatic processing of personal data". Each country, member of the Council of Europe, is authorized to adhere to this convention only if its own regulation gives effect to the basic principles for data protection pointed out by the Convention.

The Convention is legally binding upon these countries under the condition that at least five countries ratify the convention. At present time, five countries have already ratified the convention (Sweden, France, Norway, Spain and Germany) and other ratifications are expected before the end of the year (Denmark, Austria, United Kingdom). Therefore, in these countries, the convention is become part of their national system directly invokable before their national jurisdictions. Since its entry into force, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to the Convention. One thinks particularly to the United States and to the Canada.

At the European Community level, it must be added that after the drafting of this Convention, on one side, the Commission of the European communities has recommended (29 July 1981) with partial success to the member states to sign the convention in 1981 and to ratify it before the end of 1982; on the other side,

the European parliament in its resolution 'on the protection of the rights of the individuals in the face of technical developments in data Protection' has required also the member States to ratify the convention of the Council of Europe.

So, it can be concluded that the European Community relies on the effectiveness of the Convention: recent document stress the urgent needs for Member States to ratify the Convention but at the same time leaves open the possibility of an original action if it is proved that the Convention of the Council of Europe is inadequate or insufficient to protect effectively the individuals.

The OECD Guidelines on 'Protection of Privacy and Transborder Flows of personal Data' intend to 'advance the Free Flow of informations between Member Countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member Countries'.

The implementation of the OECD Guidelines relies on a voluntary basis by private enterprises. For instance, Canadian and American governments, countries not members of the Council of Europe and where no privacy regulation exists for the private sector (except for Credit Reporting Agencies, . . .), have encouraged very actively this voluntary endorsement.

### *Content of these International Instruments*

The Council of Europe Convention and the OECD Guidelines adopt the same framework. Firstly, they are enumerating minimum standards, certain core principles to be found in all Data Protection private or public regulations. Secondly, they provide special rules directly available in case of TDF.

The minimum standards, already stressed out by the Canadian government HEW report in 1973 (Grossman), are the following:

- Personal data shall be collected, stored and communicated only for specified and legitimate purposes;
- Personal data shall be accurate, up to date, adequate relevant and not excessive;
- Any individual is entitled upon request
  - to be informed by any data controller whether he holds data related to that individual;
  - to receive a copy of such data;
  - to request correction or deletion of inaccurate obsolete or irrelevant data;
- Organizations should take appropriate technical and organizational measures to ensure the accuracy and security of personal data controlled by them.

It is important to denote that even in countries where the Council of Europe convention has not yet been adopted (Belgium, Netherlands (Verkade)), certain national jurisdictions have considered that the principles stressed so by the Council of Europe constitute a common standard directly available before them against enterprises which collect, store or disseminate personal data.

Another point to be pointed out is relating to the great flexibility let to the Member States by the Convention of the Council of Europe. Various provisions contained therein to permit to each country to enact stricter principles than those stressed by the Convention. For instance, countries can extend the protection to the legal persons, refuse the application of the Convention to certain types of data or at contrary, provide an extension of the list of the sensitive data provided by the Convention to cover additional data (Zimmerman). This last reflexion about the permissible exceptions leads to examine the exact significance of the leading concept stressed by these international instruments for regulating the TDF: the concept of the '*equivalent protection*'.

### *TDF and Equivalent Protection*

A first principle enacted by the OECD Guidelines concerns the necessary security safeguards to be implemented: 'Member States should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure'- . . . against unauthorized access, accidental modifications or loss. This principle is an application of the article 12 of the Convention of the International Telecommunication Union (1973) which imposes a duty to the member states to provide security requirements for the telecommunication networks.

Still in respect to the TDF, the OECD Guidelines admit some limited restrictions to the free flow of informations. The text of the Guidelines reads: 'Exceptions to the principles contained in Parts II and III of these Guidelines, including those relating to national sovereignty and public policy should be as few as possible and made known to the public.' These restrictions will not exceed the requirements of the protection of privacy (§ 18 of the Guidelines) and are available only in two cases.

The first case concerns the hypothesis when another Member State does not yet substantially observe the Guidelines or when data are reported in a such manner that this would circumvent the domestic privacy legislation of the Member State. So, the Council of Europe permits a ratifying nation to prohibit the export of data to a country which has not ratified the Council of Europe Convention. This principle would be the major explanation of the pressure exerted by the British industry on the British government because of their fears of interruption of data flows from other countries with the arguments that the British government doesn't provide adequate regulations to protect privacy.

A second restriction is included to help accommodate countries whose domestic legislation ban collection or export of certain types of personal data, except under limited conditions: 'A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection.'

So, according to the OECD Guidelines, the restrictions on TDF have to

concern specific data and are conditioned by the proof of the lack in the foreign country of an equivalent protection. The article 12 of the Council of Europe Convention authorizes broader restrictions on TDF, it stipulates:

'The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

'Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data undergoing to the territory of another party.

'Nevertheless, each party shall be enacted to derogate from the provision of paragraph 2

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
b. when the transfer is made from its territory of a non contracting State (e.g. USA) through the intermediary of the territory of another Party, in order to avoid such tranfers resulting in circumvention of the legislation of the party referred to at the beiginning of this paragraph.'

Reciprocity or equivalency of national laws is also the main enforcement mechanism of the convention according to the OECD Guidelines. Any differences between both international instruments exist however. The Council of Europe agrees with a priori national TDF restrictions limited to specific data or files beyond the cases where another party may prove that it has an equivalent protection for these files or data. Furthermore, the article potentially at least allow a party to prohibit TDF or to subject them to a special authorization insofar the restriction is not stipulated 'for the sole purpose of the protection of the privacy', for instance for national sovereignty purposes.

But the most important problem in enforcing the Convention will be the definition of what one may call an 'equivalent protection'. As seen above, the Convention permits a lot of derogations to the principles or minimum standards provided by the convention. In these case, is that admissible that a country which has adopted stricter regulations (e.g. by providing stronger criminal sanctions or by extending the number of prohibited data) or which has extended the right of access granted for individuals, provides restrictions on TDF with the argument that there is no equivalent protection in another country. One add that discrepancies can exist not only according to the content of the legislation but also in reference to the application made by the Data Protection Authorities of these legislations (for various examples, see Briat and Zimmermann).

So, it would be useful to know if the concept of 'equivalent protection' means 'identical protection' or 'similar protection'. If the first solution is adopted, it is sure that the requirement of an 'equivalent protection' may be more difficult to satisfy than the 'adequate protection' standard required up to now by the current national legislation or Data Protection Authorities, as seen above.

## 3. Business Secrets Across International Borders

Currently, certain national European legislations (Norway, Denmark, Austria, Luxemburg) have extended the protection afforded to individuals to legal persons, i.e. organizations and business corporations. The arguments for this extension seem to be of a double nature:

–*Firstly*, it was argued that the files about legal persons very often particularly in the case of small or medium sized companies, not only are containing also informations about the individuals working or leading, but also are permitting to deduce some indications about these individuals. The protection of the legal persons is thus a complementary way to protect effectively the individuals.

At my opinion, this argument is not founded. The definition of 'individual data' is very broad and in most of the countries covers data which permits directly or indirectly to identify the data subject and practically, the Data Protection Authorities are inspecting the files concerning legal persons, each time personal data are included therein.

–*Secondly* and especially for a small or a medium sized company, the extension of certain rights granted by European legislation to physical persons is needed. So, the right of access would permit to enterprises to correct or delete false or inaccurate informations kept in the files of the government, credit reporting agencies or Banks.

Against this second argument, a lot of authors opposed that a such extension to companies, that's to say essentially the granting of the right of access to informations about themselves will afford to them the opportunity to inspect whose files held by competitors, allowing them to deduce the strategies of the competitors in the market place and finally, will distort the competition.

In accordance with the American thesis of Bok, it is obvious, that the corporations have no right to privacy and that 'the attempt to personalize collective enterprises and stretch metaphors of personal space to embrace the realm of corporate activities is conceptually wrong.' (Rankin). Therefore, the granting to enterprises of certain rights must be founded upon pure economic reasons and not upon the protection of the civil liberties.

Thus, it seems to be difficult to restrict TDF concerning enterprises in the name of the protection of the civil liberties. By this fact, one can interpretate restrictively the article 3 (2) b of the Convention of the Council of Europe which authorizes ratifying States to extend the scope of application of the Convention to include 'informations relating to groups of persons, associations, companies, corporations and other bodies *consisting directly or indirectly of individuals*.' That's only in so far the data upon enterprises permit to deduce informations about individuals, that the member countries may restrict TDF. In summary, if national regulations can grant within their territory certain rights to the enterprises, in no case, in my opinion, it belongs to them to restrict transborder flows with the argument that another country doesn't protect by the same way its enterprises.

## 4. CONCLUSION

This overview of national and international instruments regulating TDF shows the difficulty to provide a clear set of standards in this field. The reason is obviously the necessity to balance two opposite or at least competing interests. From one part, it appears very clearly the need for the international business community to obtain the recognizance of the free flow of information principle. From the other part, in opposite to this interest, certain nations require to be enable to preserve the fundamental right of individuals to preserve their privacy.

It is clear that it would be necessary to take into account these two opposite needs without celling them beside ideological assertions. With the development of the techniques permitting the processing of a still more and more increasing number of informations, with particularly the development of the "telematic" services combining the use of telecommunications networks and computers, the problem of TDF is become the *key-topic of the privacy legislations* (Rigaux).

So, the national legislations of the second phasis (1978–1987) focused more and more upon this problem and since 1980, international regulations appear to harmonize the principles and secure compatible treatment and requirements in different countries so far as to promote international flows.

This harmonization requires that two remaining questions will be solved:

– *Firstly*, the question of the *law applicable*: notwithstanding the efforts of international regulations, the national regulations and jurisdictions may apply or interpretate each principle in an original way, depending from their national sensitivity or traditions. So in case of TDF, it would be necessary to determine which national regulation is available to solve the conflict. A lot of solutions have been proposed. The uncertainties created by these different ways to solve the conflict of laws generated some fears in the international business world. In this sense, certain authors require the adoption in the international conventions of provisions regulating this problem.

– *Secondly*, to prohibit or rather to decrease the risks of disparity between national regulations, the creation of *International Data Protection Authorities* is useful. To these authorities, must be granted competences like the interpretation of the international convention, the examination and analysis of the national development, the promotion of new international instruments focused on specific sectors (e.g. Bank or Insurance) or services (e.g. information data Bank Services or Videotex Services). Furthermore, must be added the action of international private associations, which can promote 'soft law' as guidelines, standards, codes of practice and common declaration. This 'soft law' will be developed as international usance or standards of good practice and received as such by the different national courts. The emergence of the 'soft law' constitutes an increasing phenomenon to regulate the New Technologies Information area. It permits a flexible and efficient autoregulation under the control a posteriori of the national courts and insofar may be approved.

These two preliminaries seem mandatory if we want a free trade of informa-

tion and information services avoiding 'the inefficiencies that would be imposed by the need to store every data in the home country and the legal wrangles of fighting through courts in two or more jurisdictions' (Frazee) and in the same time, to ensure the human rights guarantees, granting to individuals equivalent access and equivalent protection.

## *Bibliography*


G. ALPA et M. BESSONE, *Banche Dati Telematica e diritti della persona*, CEDAM, Ed. Cedam-Padova, 1984.

J. BECKER, *'Information Technology and a new international Order'*, student litteratur AB Lund (1984).

J. BING, P. FORSBERG and E. NYGAARD, 'Problèmes juridiques posés par les flux transfrontières de données' in: 'Une analyse préliminaire des problèmes juridiques dans l'informatique et les communications'. PIIC n°8, O.C.D.E. Paris (1983).

J. BING, 'Data Protection in Practice: International Service Bureaux and Transnational Data Flows', Complex 1185, Universitets-forlaget AS, Oslo (1985).

J. BING, Data Protection in Practice: International Service Bureaux and TDF; Teresa (17), Complex, NRCCL, 111985.

J. BING, Impact of Developing Information Technology on Data Protection Legislation, OECD, ICCP, 1986.

M. BRIAT, Données personnelles et libertés de flux de données, Conférence CELIM, 2–3 avril 1987, Bruxelles, à paraître.

H. BROWN, Economic and Trade related Aspects of TDF, Information and Society Series, Studentliterrature AB, Charwell-Bratt Ltd, Lund, 1986.

H. BURKERT, Freedom of Information and Data Protection, Data Security and Confidentiality, Item F, Research Programme, 1983.

CATALA, P., 'Flux de données nationaux et transationaux, problèmes communs et problèmes spécifique', IBI, Deuxième conférence mondiale sur les politiques en matière de flux transfrontières de données, Rome, 26–29 juin 1984.

Chambre de Commerce Internationale (C.C.I.), 'Flux d'informations. Analyse des problèmes qui se posent aux entreprises', Doc. n°373123, Rev. 3, Paris, December 1984.

J.P. CHAMOUX, L'enjeu des flux transfrontières de données, Data France, 15 June 1983, 25–30.

J.P. CHAMOUX, 'L'information sans frontière', La documentation française (1980).

Commission Consultative Internationale pour le Développement des Flux Transfrontières de Données, 'Etat de l'Art dans le Domaine des F.T.D.', I.B.I., Rome 1985.

Commission of the European Community, 'European Society faced with the challenge of New Information Technologies: A Community Response', Bruxelles, 1979.

J. DE HOUWER, 'Privacy en grensoverschrijdend dataverkeer: een vergelijkende studie van internationale en nationale reglementeringen' in 'Soft en hard, ware het niet om de fraude, bedenkingen over computercriminaliteit', I.U.S. n°7, Kluwer rechtswetenschappen, Antwerpen, 1985, p. 90 et seq.

J. DE HOUWER, 'Privacy and Transborder Data Flows', Computer and Law, V.U.B. Centrum voor International Strafrecht, Bruxelles, November 17 1984.

W. EGER, Emerging Restrictions on TDF: Privacy Protection or non Tariff Trade Barriers, 10 *Law and Policy Int'l Bus. 1055 (1978)*.

M.B. FELDMAN et D. R. GARCIA, 'National Regulation of Transborder Data Flows', *North Carolina Journal of International Law and Commercial Regulation*, vol. 7, Winter 1982, Number 1, pp. 1–25.

R. FRAZEE, 'Trade and Technology: It's Canada Move', address to Canadian Club of Toronto, 7 November 1983.

K.W. GREWLICH, 'Free Electronic Information and Data Flows', p. 55 et seq.

G.S. GROSSMAN, TDF: Separating the Privacy Interests of Individuals and Corporations, *Northwestern Journal of Int. Law and Business*, 1982, 4, 1–36.

G.S. GROSSMAN, 'Transborder Data Flows: Separating the Privacy Interests of Individuals and Corporations', *Northwestern Journal of International Law and Business*, Spring 82, volume 4, number 1, page 3 et seq.

G. GARZON, Le cadre juridique des flux transfrontières de données, Doc. IBI, TDF, 206, Polycopié, 53 pages.

C.J. HAMELINK, Transnational Data Flows in the Information Age, in information and Society Series, Amsterdam, 1984.

IBI, Enquête mondiale sur les politiques nationales et les pratiques des sociétés concernant les flux transfrontières de données, TDF 110.

IBI, Compte-rendu de la 2ème conférence mondiale sur les politiques en matière de flux transfrontières de données, Rome 26–29 June 1984, TDF 260.

International Institute of Communication (I.I.C.), 'Transborder flows of personal and non-personal data', London, 1983.

M.D. KIRBY, 'Aspects juridiques de la technologie de l'information', in P.I.I.C., n°8 (cf. supra).

H. LUDERS, Transnationales Wirtschaftsrecht und Grensüberschreitender Datenverkehr, RIWAWD, 1985, 85.

M. MASMOUDI, 'The New World Information Order', U.N.E.S.C.O., SC/IMD 163, 1979.

Note, Contracts for Transnational Information Services: Securing Equivalency of Data Protection, 22 Harv, Int'l L.J., 157 162 (1981).

O.C.D.E., 'Guidelines governing the protection of privacy and transborder flows of personal data', 23 September 1980.

'Transborder Data Flows: Proceedings of an O.E.C.D. Conference', North Holland, O.E.C.D., Amsterdam, 1985.

C. OLMSTEAD, 'Transborder Data Flows; legal issues including conflict of laws', paper presented at the Conference on 'Operational and Legal aspects of transborder data flows', organized in London on 16–17 October 1985 by the International Law Association, p. 4 et seq.

J.A. RANKIN, Business Secrets across international Borders: one aspect of the TDF Debate, 10, Can. Bus. Law Journal, (1985); 2, Computer L. and Pract., 1986, 106–119.

K.P. SAUVANT, 'Trade and Foreign Direct Investment in Data Services', Westview Press, Boulder and London, 1986.

'Telecommunications and Canada', Ottawa, Canadian Government Publishing Centre, 1979.

'Transborder Data Flows said to be impeded by trade restrictions in foreign countries', *International Trade Reporter*, 26–02–86, Vol. 3, pp. 280–281.

United Nations Centre on Transnational Corporations, 'Transborder Data Flows and Brazil', United Nations, ST/IC/TC/I40, New York, 1983.

United Nations Centre on Transnational Corporations, 'Transnational Corporations and Transborder Data Flows: a technical paper', United Nations, ST/IC/T//I23, New York, 1982.

D. YARN, The development of Canadian Law on TDF, 13, *Georgia Journal of Int. and Comp. Law*. 825–854, 1983.

J. A. ZIMMERMANN, TDF: Problems with the Council of Europe Convention, or Protecting States from Protectionism, 4, *Northwestern Journal of International Law and Business*, 1982, 601–625.