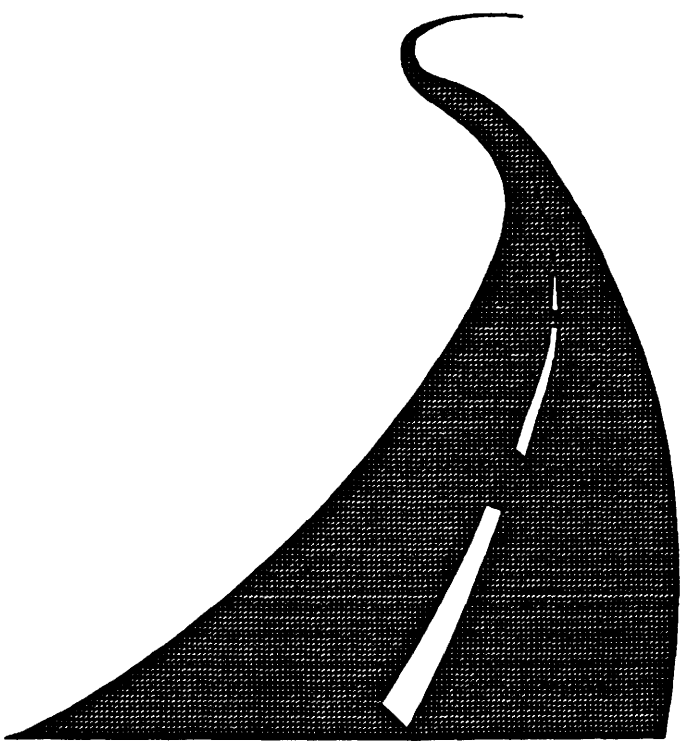
PARLEMENT EUROPEEN

Direction Générale des Etudes

DOCUMENT DE TRAVAIL

AUTOROUTES EUROPÉENNES DE L'INFORMATION

QUELLE SÉCURITÉ ?



Série Economique

W - 19

DA DE GR EN ES **FR** IT NL PT FI SV

La présente publication est disponible en français (original) avec résumé en anglais.

Cette étude n'engage pas le Parlement Européen en tant qu'institution.

Editeur: Parlement européen
Direction Générale des Etudes
Division Marché Intérieur
L-2929 Luxembourg

Date de fin de rédaction: 25 janvier 1995

Responsable: Anton LENSEN
avec la collaboration de Pascal VERGUCHT

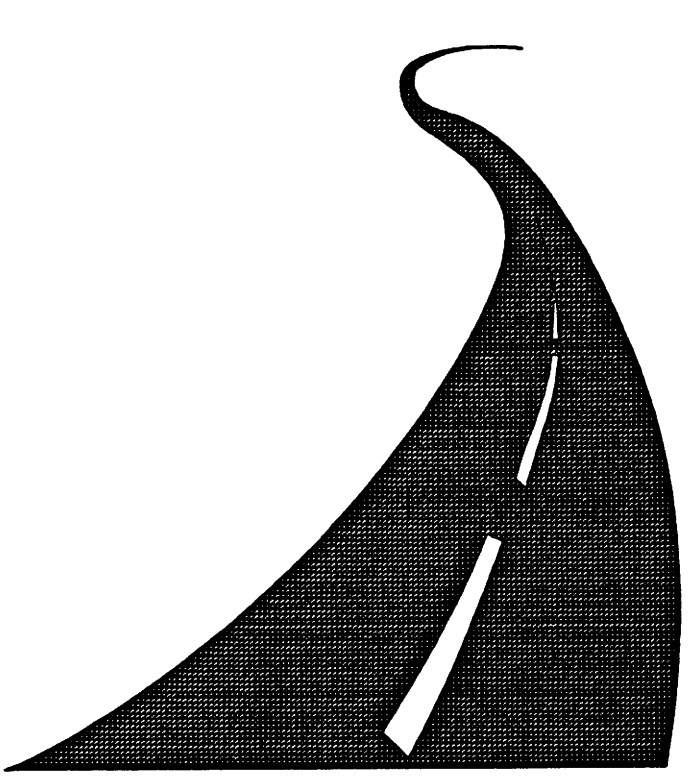
PARLEMENT EUROPEEN

Direction Générale des Etudes

DOCUMENT DE TRAVAIL

AUTOROUTES EUROPÉENNES DE L'INFORMATION

QUELLE SÉCURITÉ ?



Série Economique

W - 19

2 - 1995

Sommaire

Résumé ..... *iv*

Summary ..... *vii*

Index *18*

INTRODUCTION 1

- Quelle est la nature des problèmes liés à la sécurité des systèmes d'information? 1
- Comment peut-on cerner ces problèmes? 2

I. LA PROTECTION INFORMATIQUE 4

- Qu'est-ce que la sécurité informatique? 4
- Qu'est-ce que le cryptage? 4
- Quel est le problème en matière de cryptage? 4
- A quel niveau la question de la sécurité des systèmes d'information peut-elle être traitée? 5
- Quelles ont été les initiatives de la Commission et les textes adoptés en matière de sécurité de l'information? 6
- Quelle est la nature des contacts de la Communauté avec les pays tiers? 7
- Quelle est la position du Parlement? 8

II. LA PROTECTION JURIDIQUE 11

- Qu'est-ce que la protection juridique recouvre? 11
- Quel est l'enjeu de la protection des données personnelles? 11
- Quelle est l'action de la Communauté? 11
- Quelles ont été les initiatives communautaires? 12
- Quel est le contenu de la législation envisagée? 12
- Quelle est la position du Parlement européen? 13
- Quelle est la nature de la protection juridique des données et des bases de données en général? 13
- Quel est le contenu de la proposition de directive sur les bases de données? 14
- Quelle est la portée de la protection en matière de base de données? . . 15
- Quelle est la position du Parlement européen? 15
- Que peut faire la Communauté en matière de criminalité informatique? 16
- Quelle est la position du Parlement européen? 17

Résumé

Dans la perspective du développement de la société de l'information et des réseaux de télécommunication au sein d'un "Espace européen de l'Information", il est nécessaire de définir un cadre juridique qui permettra de maîtriser le développement des nouveaux services électroniques, et notamment d'assurer la fiabilité de ces services.

La sécurité de l'information touche aussi bien les moyens pratiques de protection que la réglementation de l'utilisation de certains procédés, la normalisation des techniques relatives aux télécommunications ou l'adoption d'un dispositif de sanctions pénales.

Les préoccupations dans ce domaine se concentrent sur quatre grandes questions:
- le droit d'auteur,
- la protection de la vie privée et des données personnelles,
- le codage des télécommunications et des échanges de données,
- la sécurité des réseaux.

On peut alors envisager la sécurité de l'information:
- sous un angle informatique, pour évoquer le cryptage;
- sous un angle juridique, pour évoquer le droit d'auteur, la protection des données personnelles et les délits informatiques.

Sous l'angle technique

La définition de la sécurité et du cryptage est un préalable à l'examen des problèmes existants. Le problème du cryptage est de concilier, d'un côté, la confidentialité du système de codage et, de l'autre, l'accès des autorités publiques au contenu des échanges codés, au nom de la sécurité publique ou de la sûreté nationale.

Certains Etats tentent, ou ont tenté, d'adopter une politique de cryptage, pour pouvoir contrôler étroitement et rapidement les télécommunications dans le cadre de leur politique de lutte contre la criminalité et l'espionnage, en procédant à des écoutes téléphoniques et à des interceptions d'échanges de données. En tout état de cause, le cryptage préoccupe les législateurs et les autorités publiques de tous les Etats membres qui attendent une prise de position au niveau communautaire. Par conséquent, la Commission a pris l'initiative de développer une politique communautaire en la matière.

La question de la sécurité des systèmes d'information peut être traitée à plusieurs niveaux. D'un point de vue individuel, l'adoption de moyens pratiques de protection et d'un comportement responsable par les constructeurs, les prestataires de services et les utilisateurs doit être encouragée. De manière plus générale, la réglementation ou la normalisation des procédés et du matériel de sécurité doit être opérée au niveau international, car les problèmes ont acquis une irrémédiable dimension transfrontière. Au niveau communautaire se pose une question politique et juridique plus pragmatique: il s'agit d'identifier les instances qui pourraient traiter la sécurité dans la société de l'information.

Après avoir commencé à aborder le sujet en 1992, la Commission a accéléré le rythme de ses travaux en 1994, alors que la sécurité informatique est devenue une préoccupation majeure.

Le Conseil a adopté en avril 1992 une décision en matière de sécurité des systèmes d'information sur une proposition de la Commission qui datait de 1990. Celle-ci a mis en place un premier plan d'action, et un Livre vert sur la sécurité des systèmes d'information a été édité par la Direction Générale XIII en avril 1994. Ce livre met l'accent sur la nécessité d'assurer des services de certification électroniques, de développer des solutions internationales et d'assurer une harmonisation technique. La Commission a en outre adopté un programme sur les mesures à adopter par la Communauté, dans une communication de juillet 1994 intitulée "Vers la société de l'information en Europe: un plan d'action". Ce plan reprend les conclusions du rapport Bangemann établi à la requête du Conseil européen de décembre 1993. Enfin, une proposition de décision, actuellement en cours d'examen, prévoit l'adoption d'une seconde action pluriannuelle concernant l'établissement d'un réseau européen de services électroniques fiables.

Le Parlement a, quant à lui, émis des avis et rendu plusieurs résolutions, notamment lors de l'examen de la proposition de décision du Conseil relative à la sécurité des systèmes d'information et de la proposition de directive du Conseil relative à la protection des données personnelles. Une importante résolution a été adoptée en novembre 1994 sur la société de l'information.

Sous l'angle juridique

Il est convenu de distinguer deux catégories de données: les données personnelles, qu'on peut rattacher à un individu, et qui font l'objet d'une protection juridique mise en place à partir des années 1970, et les autres données.

Quant à la protection juridique, elle recouvre différentes procédures:
- le recours au droit civil: responsabilité contractuelle et extra-contractuelle, protection de la vie privée et des données personnelles, etc.;

- le recours au droit pénal: incriminations relatives à certaines informations, incriminations relatives aux oeuvres protégées par les droits de propriété artistique et industrielle, incriminations spéciales en matière informatique.

Il est important de garantir la protection des données personnelles car le développement de la société de l'information, multiplie les possibilités d'atteinte à l'image, au mode de vie, aux habitudes, aux communications, à la vie privée à proprement parler. Seuls des services attirant la confiance des utilisateurs pourront assurer le succès de la société de l'information.

La Communauté essaie d'adopter une protection équivalente de haut niveau dans tous les Etats membres afin d'éliminer le risque de voir se créer des obstacles aux échanges de données, qui nuiraient au fonctionnement du marché intérieur. La Commission a présenté dans cette perspective deux propositions de directive du Conseil sur la protection des données.
Les données non spécifiquement personnelles, et leur collection (base de données) ou leur utilisation pour la création de programmes utilitaires (logiciels) peuvent sans aucun doute faire l'objet d'une propriété intellectuelle, dans la mesure où elles constituent une création informatique. La Commission a élaboré une proposition de directive du Conseil concernant la protection juridique des bases de données, dont la dernière version date d'octobre 1993.

En ce qui concerne la criminalité informatique, des législations pénales spéciales ont été adoptées par plusieurs Etats membres, que la Communauté devrait s'efforcer d'harmoniser. Il est devenu nécessaire de faciliter les procédures internationales permettant de retrouver et de sanctionner les auteurs de délits en insistant sur la nécessaire harmonisation des incriminations nationales, afin notamment d'assurer la possibilité de demander des extraditions, et en renforçant l'efficacité de la coopération judiciaire internationale. Ces actions devraient avoir une portée intra-communautaire mais aussi mondiale (Conseil de l'Europe, OCDE), la Communauté pouvant jouer un rôle aux côtés de certaines organisations internationales.

Finalement, aucune législation n'a encore vu le jour pour encadrer de manière globale la société de l'information ou les systèmes de sécurité des données qui la composeront. Mais l'Union européenne est bel et bien engagée dans un processus où elle devra examiner les problèmes qui en relèvent. Il reste à savoir si l'on aboutira à une harmonisation dans le cadre du marché intérieur ou si c'est un autre pilier du processus de décision communautaire qui sera choisi par les Etats membres.

Summary

With a view to the development of the information society and telecommunications networks within a 'European Information Area', we must define a legal framework that will enable us to control the development of the new electronic services and guarantee the reliability of such services.

Information security covers not only the practical means of protection but also the regulating of the use of certain procedures, the standardization of techniques relating to telecommunications or the adoption of a set of penal sanctions.

Concerns in this area focus on four major issues:
- copyright,
- the protection of privacy and personal data,
- coding of telecommunications and data exchange,
- network security.

Information security can therefore be viewed:
- from the data processing angle, involving the encryption;
- from the legal angle, involving copyright, personal data protection and computer crime.

The technical angle

Definition of security and encryption comes before consideration of existing problems. Encryption involves reconciling, on the one hand, the coding system's confidentiality and, on the other, access for public authorities to the substance of encoded exchanges on the grounds of public safety or national security.

Some countries are trying - or have tried - to adopt a policy on encryption so as to be able to control telecommunications closely and rapidly as part of their policy of combating crime and espionage, carrying out phone taps and intercepting data exchanges. At all events, encryption is of concern to legislators and public authorities in all the Member States who are waiting for a position to be taken at Community level. Accordingly, the Commission has set about developing a common policy on this issue.

The issue of security of information systems may be dealt with at several levels. From an individual point of view, the adoption of practical protection methods

and responsible behaviour by manufacturers, providers of services and users must be encouraged. More generally, the adoption of rules and standards for procedures and security equipment must be undertaken at international level since the problems have taken on an irreversible transfrontier dimension. At Community level we are faced by a more pragmatic political and legal question: we need to identify the bodies which might concern themselves with security in the information society.

Having made a start on this issue in 1992, the Commission stepped up its activities in 1994 since information security has become a major concern.

In April 1992, the Council adopted a decision on security of information systems on the basis of a Commission proposal drawn up in 1990. This introduced an initial action plan, and a Green Paper on security of information systems was published by Directorate-General XIII in April 1994. The Paper emphasized the need to ensure electronic certification services, to develop international solutions and to guarantee technical harmonization. The Commission also adopted a programme on the measures to be adopted by the Community in a July 1994 communication entitled 'Europe's Way to the Information Society - an Action Plan'. That plan reiterates the conclusions of the Bangemann report drawn up at the request of the December 1993 European Council. Finally, a proposal for a decision, currently under consideration, provides for the adoption of a second multiannual action programme concerning the establishment of a European network of reliable electronic services.

For its part, Parliament has delivered a number of opinions and adopted several resolutions, particularly when it considered the proposal for a Council decision concerning security of information systems and the proposal for a Council directive on the protection of personal data. A key resolution was adopted in November 1994 on the information society.

The legal angle

We must distinguish between two types of data: personal data which may be ascribed to an individual and which has been subject to legal protection since the 1970s, and other data.

Legal protection covers various procedures:
- recourse to civil law; contractual and extra-contractual liability, protection of privacy and personal data, etc.;
- recourse to criminal law: litigation in the field of certain types of information, litigation in the field of works protected by artistic and industrial property rights, special litigation in the field of data processing.

It is important to guarantee personal data protection since the development of the information society multiplies the opportunities for attacking a person's image, way of life, habits, communications and private life as such. Only services securing user confidence can ensure that the information society will be a success.

The Community is trying to adopt high-level equivalent protection in all the Member States with a view to reducing the risk of finding obstacles created to the exchange of information which would adversely affect the operation of the single market. With this in mind, the Commission has submitted two proposals for directives on data protection. Not specifically personal data and its compilation (databases) or its use for the creation of programmes (software) may doubtlessly be considered intellectual property to the extent that they constitute creative data processing. The Commission has drawn up a proposal for a Council directive on the legal protection of databases, the most recent version of which dates from October 1993.

As regards computer crime, special penal laws have been adopted by several Member States, and the Community must seek to harmonize them. It has become necessary to facilitate international procedures enabling authors of computer crime to be sought out and punished by insisting on the requisite harmonization of national penalties, with a particular view to ensuring the possibility of seeking extradition, and by enhancing the efficiency of international legal cooperation. Such measures should cover the Community but should also apply worldwide (Council of Europe, OECD), with the Community playing a role alongside certain international organizations.

Finally, no legislation has yet been enacted to cover comprehensively the information society or the data security systems constituting it. However, the European Union has made a real start on a process where it must consider the problems involved. It remains to be seen whether harmonization will come about within the context of the internal market or whether the Member States will opt for another pillar in the Community decision-making process.

INTRODUCTION

Quelle est la nature des problèmes liés à la sécurité des systèmes d'information ?

L'émergence des nouvelles technologies est prise en compte par l'Union européenne, dans la perspective du développement de la société de l'information et des réseaux de télécommunication. Le Parlement a été amené à donner son avis sur la réglementation des services et matériels de télécommunication, à la suite des propositions de la Commission, et cela lui a permis d'élaborer une politique et de prendre des initiatives pour l'essor des futurs services multimédias.

La définition d'un cadre juridique qui permettra de maîtriser le développement et d'assurer la fiabilité des nouveaux services électroniques est un aspect que les institutions communautaires n'ont pas esquivé, et sur lequel repose un épanouissement harmonieux de la société de l'informatique et des télécommunications. La croissance d'un réseau comme Internet interpelle les décideurs et les responsables du monde des affaires et du secteur public.

La fiabilité, la sécurité de l'information sont devenues une nécessité dans notre société informatisée, qui devient de plus en plus urgente au fur et à mesure que les réseaux informatiques se multiplient et s'entrecroisent à travers la planète. Par exemple, le développement des services de paiement électroniques nécessite l'assurance que celui qui paie est bien celui qui reçoit le service, que les échanges de données demeurent confidentiels, que l'intégrité des signatures, des textes et des dates est assurée, qu'une reconnaissance légale est éventuellement permise. La volonté politique des institutions communautaires et des Etats membres de créer un "Espace Européen de l'Information" donne tout son relief aux préoccupations qui entourent l'avenir des réseaux et de la société de l'information.

Une expansion anarchique de la société de l'information risquerait de remettre en cause cette société, les utilisateurs rejetant un instrument de communication et de gestion qui ne garantirait ni la confidentialité, ni l'intégrité, ni la disponibilité des données.

La Communauté et le Parlement européen ont un rôle à jouer à ce niveau tant le problème revêt une portée internationale, dépassant le strict cadre national. Les systèmes de sécurité informatiques, la transparence de l'information, la multiplication des services télématiques peuvent certes

mettre en jeu des compétences nationales réservées liées à la sécurité et à l'ordre public, mais il s'agit d'arriver à dépasser les réticences étatiques pour garantir le progrès au niveau européen de la qualité des services liés à l'information.

La Commission a proposé dès 1990 un plan d'action en matière de sécurité des systèmes d'information, qui a donné lieu à une décision du Conseil en 1992. Une nouvelle proposition de décision relative à un deuxième plan d'action multiannuel est en cours d'examen. Le Conseil européen a d'autre part demandé à un groupe de hautes personnalités présidé par M. Bangemann, lors de sa réunion en décembre 1993, d'établir un rapport sur l'Europe et la société de l'information, qui lui a été présenté en juin de l'année suivante. A la suite de ce rapport a été adoptée par la Commission une communication contenant un plan d'action général sur tous les aspects relatifs à la mise en place de cette société. C'est dans ce cadre qu'est intervenu le Parlement, en adoptant en novembre 1994 une importante résolution.

Aucune législation européenne contraignante n'a donc encore vu le jour pour encadrer de manière globale "l'espace européen de l'information" ou les systèmes de sécurité des données qui la composeront. Mais l'Union européenne est bel et bien engagée dans un processus où elle devra examiner les problèmes qui en relèvent. Il reste à savoir si l'on aboutira à une harmonisation ou si c'est un autre pilier du processus de décision communautaire qui sera choisi par les Etats membres.

Il est en tout les cas utile d'essayer d'éclaircir certains points ou tout du moins de synthétiser les réponses à quelques questions qui touchent à la sécurité des systèmes d'information.

Comment peut-on cerner ces problèmes ?

La sécurité de l'information touche aussi bien les moyens pratiques de protection (aménagement des sites informatiques, imposition de règles de sécurité, etc.), que la réglementation de l'utilisation de certains procédés, la normalisation des techniques relatives aux télécommunications ou l'adoption d'un dispositif de sanctions pénales.

En ce qui concerne l'Union européenne, c'est surtout la réglementation, la normalisation ou l'harmonisation du droit qui importe. Les préoccupations se centrent alors sur quatre problèmes:

- les questions liées au droit d'auteur,
- celles liées à la protection de la vie privée et des données personnelles,

- celles liées à la sécurité des réseaux, qui concernent, d'une part, les délits informatiques (connus généralement sous le terme américain "hacking") et, d'autre part, la normalisation des réseaux.

On peut ici envisager la sécurité de l'information:

- sous un angle informatique pour évoquer le cryptage,
- sous un angle juridique pour évoquer le droit d'auteur, la protection des données personnelles et les délits informatiques.

1. LA PROTECTION INFORMATIQUE

Qu'est-ce que la sécurité informatique ?

Il s'agit de tous les procédés appartenant à la technologie informatique, qui permettent de protéger les données et leur échange: logiciels traqueurs, systèmes de mots de passe dynamiques, chiffrement. Au niveau communautaire, on discute notamment des questions liées au cryptage des données.

Qu'est-ce que le cryptage ?

Les procédés de cryptage (ou codage) sont conçus pour transformer à l'aide de conventions secrètes des informations intelligibles en signaux inintelligibles, et vice et versa. Ils sont de plus en plus usités dans les flux transfrontières de données, surtout dans le domaine financier.

Quel est le problème en matière de cryptage ?

Le cryptage est considéré, sur un premier plan, comme le moyen de garantir la confidentialité des échanges de messages, le moyen d'accréditer la provenance et la qualité de ceux-ci, en bref, d'assurer aux utilisateurs la fiabilité et la discrétion des réseaux. Mais en même temps, le cryptage est considéré comme un obstacle aux investigations judiciaires qui exigent l'accès à des informations codées, lorsque la personne qui fait l'objet de l'investigation est celle qui détient les clés du codage. Dans la plupart des pays, la personne détentrice n'est pas tenue de fournir la clef.

La poursuite est alors réduite à un recours aux tiers, qui peuvent être tenus de fournir les clés, s'ils les connaissent, en qualité de témoins. Pour certains, la solution la plus pratique serait de permettre aux autorités publiques l'accès aux clés universelles des créateurs des codages, par le biais d'une obligation légale, ou grâce à une obligation pour les concepteurs de déposer les clés "passe-partout" des procédés de codage qu'ils veulent commercialiser ou éditer.

Le problème du cryptage est donc de concilier:
- la confidentialité du système de codage,
- l'accès des autorités publiques au contenu des échanges codés, au nom de la sécurité publique ou de la sûreté nationale.

En tout état de cause, le cryptage interpelle les législateurs et les autorités publiques de tous les Etats membres qui attendent une prise de position au niveau communautaire; cela d'autant plus que la Commission a décidé de prendre l'initiative de lancer une politique en matière de sécurité des systèmes d'information.

A quel niveau la question de la sécurité des systèmes d'information peut-elle être traitée ?

On doit ici envisager la réponse sous trois angles: individuel, général et communautaire.

- Au niveau individuel, la prise des moyens pratiques de protection par les constructeurs, les prestataires de services et les utilisateurs est encouragée dans le cadre de la lutte contre la criminalité informatique. C'est un moyen de sécuriser les échanges de données qui permettrait d'éviter un recours trop fréquent au droit pénal pour réprimer les accès aux systèmes informatiques et l'utilisation illicite des données qui y sont stockées. En effet, il serait insuffisant de se limiter à la mise en place d'un dispositif pénal, qui est destiné à n'intervenir qu'une fois le mal accompli. La prévention étant la meilleur des politiques envers la criminalité, la Commission a adopté une ligne de conduite globale en matière de sécurité des informations. Il s'agit donc à ce niveau d'encourager les individus comme les entreprises, à prendre conscience de l'existence des risques informatiques, et à agir en conséquence en adoptant un comportement responsable. La sécurité n'est pas seulement une affaire d'autorité publique, mais elle est aussi l'affaire de chacun des acteurs de la société de l'information.

- Au niveau général, la réglementation ou la normalisation des procédés et matériels de sécurité doit être opérée au niveau international, car les réseaux de télécommunications couvrent désormais le monde entier. Les problèmes ont acquis une irrémédiable dimension transfrontière, et ne sauraient être résolus dans l'avenir par l'adoption de règles nationales indépendantes. Seule une coopération entre Etats et entre Organisations Internationales peut dorénavant faire face à l'impact des décisions qui concernent les télécommunications et la télématique.

- Au niveau communautaire se pose une question politique et juridique plus pragmatique. Il s'agit de savoir quelles instances pourraient être compétentes pour traiter la sécurité dans la société de l'information. La Commission a commencé à prendre des initiatives, qui toutefois se cantonnent à des plans d'action et à l'adoption de programmes pluriannuels. A l'avenir, la prise de mesures concrètes pourrait atteindre les compétences réservées des Etats membres, et ceux-ci pourraient

exiger un règlement politique au niveau ministériel qui passerait au dessus de la Commission, pour des raisons touchant à leur sécurité nationale ou à leurs intérêts fondamentaux.

D'autre part, certains Etats membres peuvent décider à tout moment de prendre des mesures restrictives relatives, par exemple, au commerce des matériels informatiques, pour des raisons de sécurité publique et au nom de l'article 36 du Traité de la CE.

La Commission tentera peut-être de défendre comme base juridique à son action l'article 100A qui permet une procédure de codécision. Mais certains Etats ont déjà entamé un débat préliminaire sur ce sujet.

Quelles ont été les initiatives de la Commission et les textes adoptés en matière de sécurité de l'information ?

La Commission essaie d'éveiller l'attention des Etats membres sur la nécessité de régler au niveau communautaire les questions qui relèvent de la "sécurité des systèmes d'information". Après avoir commencé à aborder le sujet en 1992, la Commission a accéléré le rythme de ses travaux en 1994, alors que la sécurité informatique devient une préoccupation de plus en plus sensible.

Le Conseil a adopté en avril 1992 une décision en matière de sécurité des systèmes d'information[1] sur une proposition de la Commission qui datait de 1990[2]. Il s'agissait de mettre en place une stratégie communautaire pour faire face aux menaces accidentelles ou volontaires contre les systèmes informatiques. La décision adoptait un plan d'action de 24 mois et créait un groupe de hauts fonctionnaires sur la sécurité de l'information (SOG-IS) composé de deux représentants de chaque Etat membre et de la C6ommission, est chargés de conseiller cette dernière. La décision instituait également un comité consultatif et un comité de réglementation fonctionnant selon la procédure III variante (a) pour assister la Commission dans la mise en oeuvre de l'action. Un budget de 12 MECU était octroyé pour l'application de l'action, et la Commission devait présenter un rapport au Parlement et au Conseil sur les résultats du plan d'action dans les trois mois suivant son achèvement.

---

1 Décision 92/242/CEE, JO no L 123, 8.05.92, p.19.

2 Proposition de décision COM(90) 314, JO C 277, 5.11.90, p.18.

Un "Livre Vert sur la sécurité des systèmes d'information" a été édité par la Direction Générale XIII en avril 1994. Il met l'accent sur la nécessité d'assurer des services de certification électroniques, de développer des solutions internationales et d'assurer une harmonisation technique.

La Commission a établi un programme sur les mesures à adopter par la Communauté, dans une communication de juillet 1994 intitulée "Vers la société de l'information en Europe: un plan d'action"[1]. Ce plan reprend les conclusions du rapport Bangemann et prévoit dans le domaine de la sécurité des informations:

- une proposition sur les exigences de codage dans le monde des affaires et du commerce ainsi que sur l'intégrité des signatures (suivi du programme Infosec mis en place avec la décision 92/242/CEE),
- un large examen des questions de sécurité devant donner lieu à la présentation d'une communication sur la sécurité des informations et le rôle des Etats membres,
- une étude dans le cadre du livre vert cité au paragraphe précédent, sur l'harmonisation des dispositions nationales sur les accès non autorisés aux données informatiques pour 1995,
- une coopération avec des Etats tiers, notamment les Etats-Unis.

Une proposition de décision correspondant au premier point est actuellement en cours d'examen, et prévoit l'adoption d'une action pluriannuelle concernant l'établissement d'un réseau européen de services électroniques fiables (ETS)[2]. Elle devrait prendre la relève de la décision 92/242/CEE citée ci-dessus. Une action sur cinq ans serait envisagée pour favoriser l'établissement d'un réseau offrant au monde des affaires et aux particuliers des moyens de signature électronique, une confidentialité et un support de services électroniques et multimédias. La mise en place de cet ETS serait estimée à 65 MECU.

Le Conseil devrait prochainement examiner dans ce cadre une approche commune sur la législation des réseaux télématiques, l'interception légale des télécommunications dans le respect des droits de l'individu, le droit de la preuve, les lois sur les délits informatiques, ainsi qu'une solution internationale en ce qui concerne la sécurité des réseaux, un renforcement de la normalisation internationale et de la position de l'Europe dans le domaine des techniques de confidentialité et de signature électronique.

---

1 Document COM (94) 347 final, 19.07.94.

2 A multi-annual action concerning the establishment of Europe-wide Trust Services for non-classified information services (ETS): voir Peter Bauer et Heribert Peuckert, "Chipkarten mit Kryptographie erschliessen neue Anwendungsfelder", Datenschutz und Datensicherung, juillet 1994, p. 381-384.

Quelle est la nature des contacts de la Communauté avec les pays tiers ?

Le Plan d'action de la Commission prévoit des prises de contact avec des Etats tiers, ce qui est d'une évidente nécessité, la Communauté ne pouvant régler à elle seule la sécurité des échanges de données au niveau international. Pour le moment, les contacts américains avec la NSA (National Security Agency), le NIST (Nationale Institute of Standard and Technology) et le cabinet du vice-président Al Gore demeurent informels.

Quelle est la position du Parlement européen ?

Le Parlement a émis son avis et rendu trois résolutions lors de l'examen du panier de propositions de la Commission relatives à la protection des données personnelles, à cette protection dans le contexte des réseaux numériques à intégration de services, et à la sécurité des systèmes d'information[1]. Le rapporteur, M. Herman envisageait l'amendement, consistant à assurer la présence au sein du SOG-IS de représentants des fabricants, des prestataires de services, des consommateurs et des syndicats. Le Parlement adopta cependant la proposition de directive relative à la sécurité des systèmes sans amendement. La Commission économique, monétaire et de la politique industrielle du Parlement européen a examiné sur le fond un projet de rapport et de résolution rédigé par M. Herman, sur la recommandation au Conseil européen "L'Europe et la société de l'information planétaire" et sur le Plan d'action de la Commission. La résolution a été adoptée le 30 novembre 1994[2]. On peut y trouver formulé le souhait de définir à l'échelle communautaire des règles en matière, notamment, de cryptage et de signature électronique.

Quelle est la situation juridique du cryptage dans les Etats membres?

L'intérêt des Etats est de pouvoir contrôler étroitement et rapidement les télécommunications dans le cadre de leur politique de lutte contre la criminalité et l'espionnage, en procédant à des écoutes téléphoniques et à des interceptions d'échanges de données. Cet intérêt se heurte à celui des individus qui est de sauvegarder une sphère de liberté et de vie privée, que les services de police et de contre-espionnage pourraient avoir tendance à restreindre au nom de la sécurité publique. L'intérêt des groupes commerciaux est similaire, quant à lui, dans le domaine du secret des

---

1 JO no C 94, 13.04.1992, p.77, 198, 202 et rapport A3-10/92.

2 Document A4-73/94.

affaires. Mais en outre, il s'agit pour eux de défendre la possibilité de créer, produire et commercialiser des procédés de codage sans contrainte administrative, et sans être limité par la normalisation d'un procédé qui handicaperait les progrès en la matière.

La France est actuellement le seul pays de la Communauté à posséder une loi sur les procédés de cryptage[1]. Autrefois rattachés au sévère régime des matériels de guerre, les procédés sont aujourd'hui soumis:

- à une procédure de déclaration lorsqu'ils ont pour objet l'authentification d'une communication, ou la vérification de l'intégrité d'un message transmis,
- à une procédure plus contraignante de licence obligatoire lorsqu'ils ne rentrent pas dans la première catégorie, la demande d'autorisation étant déposée avec la clé du codage auprès du Service de la sécurité des informations rattaché au Premier Ministre. Des procédures simplifiées peuvent être adoptées.

Dans les autres Etats membres, les procédés de cryptage sont de libre usage et de libre commerce, sauf bien entendu si l'utilisateur est l'objet d'une obligation de secret d'Etat ou de défense nationale.

Mais plusieurs Etats sont préoccupés par la multiplication des télécommunications codées, aussi bien sur le réseau GSM utilisé par les radiotéléphones, que par les échanges de données informatiques. Les Pays-Bas illustrent cette attitude. Une loi sur les délits informatiques est entrée en vigueur le 1er mars 1993, qui donne une base légale spécifique aux interceptions d'échanges de données, aux perquisitions de systèmes informatiques et à l'obtention de données décryptées ou des clés de décodage. D'autre part, un projet de loi de mai 1994 entendait soumettre les utilisateurs de procédés de cryptage à une procédure de licence et de dépôt des clés des codes devant une agence spéciale tenue par une obligation de secret. L'agence devait fournir ces clés aux services de police et de sécurité qui seraient munis d'un mandat adéquat. A la suite d'une fuite dans la presse, de nombreuses protestations conduisirent le gouvernement à abandonner son projet.

---

1 Loi du 29.12.1990; voir Eric Meillan, "Le régime juridique de la cryptologie en France", Revue internationale de police criminelle, mars-avril 1992, p.18-20.

Il convient de signaler l'importance de la politique américaine dans le domaine du cryptage[1]. La NSA a mené en la matière une politique délibérée pour entraver l'exportation des procédés de codage sophistiqués, et pour promouvoir dans les communications avec les administrations un procédé standard nommé "Clipper chip", dont elle aurait possédé une clé universelle. La généralisation de l'emploi de ce procédé lui aurait en outre permis de pouvoir considérer comme suspect tout codage par un moyen différent, utilisant par exemple le logiciel "Pretty Good Privacy", appelé "PGP", et que son auteur, Philipp Zimmermann, a largement diffusé sur le réseau Internet pour lutter contre la politique du gouvernement américain[2]. Les efforts de celui-ci ont cependant échoué face aux réticences des entreprises américaines, préoccupées PAR leur compétitivité sur les marchés intérieurs, et des associations privées, inquiètes AU SUJET DEDE la question de la protection des libertés privées.

1 Voir "US reaffirms computer eavesdropping policy", Transnational data and communications report, mars-avril 1994, p.7-9; "Encryption technology, Clipped", The Economist, 6 août 1994, p. 76.

2 Voir "L'Epopée de Pretty Good Privacy", Sciences et Avenir, janvier 1995, p.30.

II. LA PROTECTION JURIDIQUE

Qu'est-ce que la protection juridique recouvre ?

Il est convenu de distinguer en droit deux catégories de données:
- les données personnelles, qu'on peut rattacher à un individu, et qui font l'objet d'une protection juridique mise en place à partir des années 1970;
- les autres données.

Quant à la protection juridique, elle recouvre différentes solutions:
- le recours au droit civil: responsabilité contractuelle et extra-contractuelle, protection de la vie privée et des données personnelles, etc.;
- le recours au droit pénal:
  - incriminations relatives à certaines informations: secret des affaires, de la vie privée, professionnel, des télécommunications, etc.,
  - incriminations relatives aux oeuvres protégées par les droits de propriété artistique et industrielle (surtout, contrefaçon de logiciels),
  - incriminations spéciales en matière informatique: "fraude informatique", protection des données personnelles, protection des topographies de semi-conducteur, etc.

C'est en matière pénale que la Communauté peut mener une action d'harmonisation, en particulier au niveau des incriminations spécifiques au domaine informatique.

Quel est l'enjeu de la protection des données personnelles ?

Le "rapport Bangemann"[1] rappelle qu'il est important de garantir la protection des données personnelles (textes, images, voix...) pour assurer le développement de la société de l'information, car celle-ci multiplie les possibilités d'atteinte à l'image, au mode de vie, aux habitudes, aux communications, à la vie privée à proprement parler. Seuls des services attirant la confiance des utilisateurs pourront assurer le succès de la société de l'information. Une action au niveau communautaire pour harmoniser les mesures nationales divergentes est très importante, car les échanges de données personnelles entre les Etats membres pourraient être restreints au titre de la différence de protection, fermant ainsi la porte à la croissance du flux transfrontière des données et des nouveaux services multimédias.

---

1 L'Europe et la société de l'information planétaire, recommandation au Conseil européen du 26 mai 1994

Quelle est l'action de la Communauté ?

La Communauté essaie d'adopter une protection équivalente de haut niveau dans tous les Etats membres afin d'éliminer le risque de voir se créer des obstacles aux échanges de données, qui nuiraient au fonctionnement du marché intérieur. Il faut donc qu'un texte détermine les moyens et méthodes pour rapprocher les législations des Etats membres, et pour pousser les Etats dépourvus de législation en matière de protection des données à en adopter une qui soit conforme aux critères communautaires. Ces critères devraient forcément être d'un niveau élevé, pour éviter l'uniformisation d'une protection minimale qui ne saurait satisfaire les exigences des consommateurs et assurer la confiance du public dans les services informatiques.

Quelles ont été les initiatives communautaires ?

La Commission a présenté une proposition de directive[1], modifiée en 1992[2]. La procédure est désormais de codécision entre le Conseil et le Parlement[3], et une nouvelle proposition de directive relative à la protection des personnes à l'égard du traitement des données à caractère personnel a été rendue en resaisine[4]. En tout état de cause, et si le texte finit par être adopté par le Conseil et le Parlement, l'application de la directive dans les Etats ne devrait pas avoir lieu avant l'été 1996. Il convient de noter que la Commission a proposé une autre directive sur la protection des données, spécialement attachée aux problèmes posés par les Réseaux Numériques à Intégration de Services[5]. La volonté de la Commission était de faire adopter ce texte au plus tôt.

Ces deux directives furent présentées en même temps que la proposition de décision concernant la sécurité des systèmes d'information; mais celle-ci fut adoptée, conformément à l'avis du Parlement, de manière indépendante, en 1992.

---

1 Proposition de directive COM(90) 314, JO C 277, 5.11.1990, p.3.

2 Proposition de directive COM(92) 422, JO no C 311, 27.11.1992, p.30.

3 Article 100A du Traité de Maastricht.

4 Document COM(93) 570, resaisine.

5 Proposition de directive COM(90) 314, JO no C 277, 5.11.1990, p.3., modifiée par la proposition de directive COM(94) 128, JO no C 200, 22.07.1994, p.4.

Quel est le contenu de la législation envisagée ?

Les règles prévues par la directive relative à la protection des données personnelles concernent:
- la légitimité du traitement informatique des données personnelles (procédures administratives de déclaration ou autorisation),
- des droits pour la personne concernée par les données,
- des interdictions ou limitations concernant certaines catégories de données sensibles,
- des obligations pour le responsable du fichier de données personnelles, notamment une obligation de sécurité et un devoir de confidentialité,
- une limitation aux transferts de données vers des pays dont le niveau de protection n'est pas équivalent.

Quelle est la position du Parlement européen ?

Le Parlement a amendé les propositions de la Commission pour élargir le champ d'application de la directive, renforcer les obligations des Etats membres relatives au respect de la vie privée et renforcer les droits des individus, les mesures de contrôle dans le traitement, la collecte et la diffusion des données à caractère personnel[1]. Une partie des amendements a été acceptée par la Commission et reprise dans ses dernières propositions. Dans sa résolution sur la recommandation au Conseil européen "L'Europe et la société de l'information planétaire" et sur le Plan d'action de la Commission adoptée le 30 novembre 1994, le Parlement considère que devront être définies au niveau communautaire des règles en matière de sauvegarde des informations privées et de protection de la personne[2]. Le Parlement estime en outre "que ce serait une profonde erreur que d'englober dans une même catégorie générale d'informations tous les produits ou toutes les oeuvres et insiste par conséquent sur la nécessité de garantir d'urgence, de manière efficace et moderne, la protection des bases de donnée ainsi que de la liberté des personnes, par le biais d'une directive cadre sur la protection des données personnelles et de la vie privée"[3].

---

1 Avis dans une résolution du 11.3.1992, JO no C 94, 13.04.1992, p.77, 198 et 202.

2 Point numéro 16.

3 Point numéro 40.

Quelle est la nature de la protection juridique des données et des bases de données en général ?

Les données non spécifiquement personnelles, et leur collection (base de données) ou leur utilisation pour créer des programmes utilitaires (logiciels) peuvent sans aucun doute faire l'objet d'une propriété intellectuelle, en tant qu'elles constituent une création informatique.

Il en va ainsi des logiciels, qui sont inclus dans la quasi-totalité des pays dans la liste des oeuvres protégées par le droit d'auteur ou le copyright, et qui bénéficient d'un régime légèrement adapté.

Pour ce qui est des bases de données, il existe peu de texte prévoyant un régime spécifique de propriété intellectuelle, comme cela existe pour les topographies de semi-conducteurs (chips), ou les logiciels[1]. Mais l'opinion générale, presque unanime, est que ces bases sont protégées au titre du droit d'auteur. Les bases de données sont comparées à une catégorie connue d'oeuvres protégées, les oeuvres composites, et plus particulièrement les anthologies et recueils.

Dans sa communication intitulée "Les suites à donner au livre vert, Programme de travail en matière de droit d'auteur et de droits voisins"[2], la Commission adopta les conclusions suivantes à la suite des auditions menées après la publication du livre vert: "Tous les intervenants ont estimé que les bases de données étaient protégées par le droit d'auteur"[3] et "il ne faut pas se limiter aux 'compilations' étant donné que certaines bases de données sont des 'oeuvres littéraires' par elles-mêmes"[4]. La Commission s'est ensuite lancée dans l'élaboration d'une proposition de directive du Conseil concernant la protection juridique des bases de données, dont la dernière mouture date du 4 octobre 1993[5].

---

1 L'article 56 de la loi britannique sur le copyright du 15/11/1988 concerne spécialement les bases de données.

2 Document COM(90) 584 final, 17/01/1991.

3 Page 21, numéro 3.

4 Page 21, numéro 6.

5 Proposition de directive COM(93) 464 final, 4.10.1993.

Quel est le contenu de la proposition de directive sur les bases de données ?

La proposition amendée actuelle vise à:
- réglementer l'incorporation d'oeuvres protégées dans les bases en les soumettant à l'autorisation du titulaire des droits,
- assurer un monopole de reproduction, représentation, transformation et distribution en ce qui concerne le choix ou la disposition du contenu, et les éléments permettant la construction et le fonctionnement de la base, limité par les exceptions traditionnelles,
- instituer un droit d'interdire l'extraction ou la réutilisation non-autorisée du contenu des bases, sauf exceptions de transparence spécifiquement prévues dans certaines conditions, ce droit s'appliquant indépendamment de la possibilité d'une protection par le droit d'auteur.

Quelle est la portée de la protection en matière de base de données ?

L'une des questions les plus intéressantes qui se pose concerne la latitude laissée aux créateurs de base dans leur création, et l'ampleur de la protection accordée au résultat de leur travail ou de leur investissement.

Les emprunts faits à des oeuvres protégées par le droit d'auteur, que cela soit des oeuvres "classiques" (livres, disques, photos, etc.) ou des oeuvres informatiques (dessins assistés par ordinateur, base de données, etc.) pour constituer des bases de données peuvent être de deux ordres:
- soit ils sont opérés avec l'accord du titulaire du droit d'auteur,
- soit ils sont faits sans son accord, et alors pour être licites, ils doivent entrer dans le cadre des régimes d'exception qui limitent l'exclusivité de reproduction (c'est la fixation matérielle d'une oeuvre, par exemple l'édition d'un livre) et de représentation (c'est la communication au public d'une oeuvre, par exemple sa lecture en publique, sa radiodiffusion) des oeuvres sources.

En ce qui concerne l'action communautaire dans le domaine des bases de données, la Commission propose actuellement dans le projet de directive du Conseil[1] un article 5 sur l'incorporation d'oeuvres ou matières dans une base de données:

1) L'incorporation dans une base de données de toute oeuvre ou matière reste soumise à l'autorisation du titulaire du droit d'auteur ou d'autres droits existants ou obligations à l'égard de cette oeuvre ou de cette matière.

---

1 Proposition de directive COM(93) 464 final.

2) L'incorporation dans une base de données, de références bibliographiques, d'extraits (à l'exclusion de tout exposé ou de tout résumé substantiel du contenu ou de la forme d'oeuvres existantes) ou de brèves citations, ne nécessitent pas l'autorisation des titulaires des droits sur ces oeuvres, à condition que soient clairement indiqués le nom de l'auteur et la source de la citation, conformément à l'article 10 paragraphe 3 de la Convention de Berne".

A l'origine, la Commission avait proposé l'article 4.1 suivant:
"L'incorporation dans une base de données de matières bibliographiques, ou de courts extraits, citations ou résumés d'une oeuvre qui ne se substitue pas à l'oeuvre elle-même ne nécessite pas l'autorisation du titulaire du droit dans cette oeuvre".

Que peut faire la Communauté en matière de criminalité informatique?

Ce qui est souvent connu en matière de criminalité informatique se réduit au "hacking", méthode qui consiste à pénétrer dans des systèmes pour en forcer simplement les mots de passe, ou pour prendre connaissance des secrets qui sont enregistrés dans le système. Les délits sont pourtant beaucoup plus divers et causent parfois des dégâts financiers sans commune mesure avec la plupart des crimes économiques classiques comme le vol ou l'escroquerie. Des législations pénales spéciales ont été adoptées par plusieurs Etats membres, que la Communauté devrait s'efforcer d'harmoniser.
Ces textes incriminent:
- l'accès illicite, sans intention ou avec intention de nuire, dans des systèmes informatiques,
- l'usage illicite des données ou des systèmes, ainsi que leur falsification.

La criminalité informatique a déjà acquis une dimension internationale, au rythme du développement des réseaux informatiques mondiaux. Il s'agit d'éviter l'instauration de "paradis de hackers", comparables à des paradis fiscaux.

Le laxisme des lois permet aux criminels de commettre des forfaits en toute impunité. Il est devenu nécessaire de faciliter les procédures internationales permettant de retrouver et de sanctionner les auteurs de délits:
- en insistant sur la nécessaire harmonisation des incriminations nationales, afin notamment d'assurer la possibilité de demander des extraditions,
- en renforçant l'efficacité de la coopération judiciaire internationale (commissions rogatoires, transmission d'actes de procédure, comparution de témoins, échanges de casiers judiciaires, etc.).

Ces actions devraient avoir une portée intra-communautaire, mais aussi internationale, la Communauté pouvant jouer un rôle aux côtés de certaines organisations. Le Conseil de l'Europe, dans le cadre de son mandat sur la protection des libertés publiques qui lui a permit d'aboutir à la création de la Convention sur la protection des données à caractère personnel, travaille actuellement sur les problèmes de procédure liés à la poursuite des infractions en matière informatique (droit de la preuve et valeur des documents informatiques, pratique des écoutes téléphoniques, des saisies et des perquisitions dans l'univers de l'informatique, problèmes relatifs à l'obligation de coopération active des témoins) avec l'aide notamment de l'OCDE, qui s'est préoccupé de savoir quelles étaient les exigences des milieux économiques, industriels et financiers en ce qui concerne la maîtrise de la délinquance informatique, et quels étaient les efforts à fournir afin d'obtenir une certaine homogénéité des législations pénales des principaux Etats industrialisés.

Quelle est la position du Parlement européen ?

Dans sa résolution sur la recommandation au Conseil européen "L'Europe et la société de l'information planétaire" et sur le Plan d'action de la Commission adoptée le 30 novembre 1994, le Parlement considère que devront être définies au niveau communautaire des règles en matière de protection et de rémunération de la propriété intellectuelle[1].
Le Parlement exprime aussi sa préoccupation au sujet du retard pris dans l'exécution du programme relatif à la protection de la propriété intellectuelle, dans l'adoption des dispositions prévues relatives au droit d'auteur, spécialement la directive concernant l'utilisation à des fins privées des copies de productions audiovisuelles[2]. Le Parlement déclare attendre avec intérêt le Livre vert de la Commission sur les droits de protection industrielle dans la société de l'information, et souligne la nécessité d'adopter une législation sur la protection des créateurs dans le cadre de la mise en oeuvre des nouveaux médias, qui risquent d'échapper au droit existant[3]. Enfin, il considère que le développement de la transmission numérique doit s'accompagner d'un renforcement de la protection des oeuvres couvertes par un droit d'auteur et de la lutte contre la piraterie, compte tenu des possibilités de manipulations et d'utilisations des oeuvres[4].

---

1 Point numéro 16.

2 Point numéro 35.

3 Point numéro 36.

4 Point numéro 37.

Le Parlement considère par ailleurs que devront être fixées des règles communautaires en matière de sécurité d'exploitation et de protection des réseaux contre les intrusions malveillantes ou accidentelles ("network integrity")[1].

1 Point numéro 16.

Index

chiffrement 4
codage ..... iv, 2, 4, 7-9
criminalité ..... iii, iv, vi, 5, 8, 16
criminels 16
cryptage ..... ii, iv, 3, 4, 8, 9
décision 92/242/CEE 6, 7
ETS 7
GSM 9
Internet 1, 10
NIST 8
NSA 7, 9
ordre public 1
"Pretty Good Privacy" 9, 10
propriété ..... vi, 11, 14, 17
protection des données ..... iii, iv, v, vi, 3, 8, 11-13, 16
protection juridique ..... v, vi, 11, 13, 14
sécurité de l'information, des données ..... iv, v, vi, 1-9, 12, 13, 17
sécurité publique, nationale ..... iv, 4
société de l'information ..... iv, v, vi, 1, 2, 5, 7, 8, 11, 13, 17
SOG-IS 6, 8
sûreté nationale ..... iv, 4