

MÉMOIRE DE D.E.S.S.



**ASPECTS JURIDIQUES DE L'ÉMERGENCE
D'UNE SÉCURITÉ EUROPÉENNE DES RÉSEAUX
ET DES SYSTÈMES D'INFORMATION**

Mme Anne BRISSET-GIUSTINIANI

Directeur de mémoire : M. Philippe WOLF

Président du jury : M. le Professeur Georges CHATILLON

Membres du jury : Mme CHAPERON et Mme ROGER-GRAUX

Année universitaire 2003 - 2004

REMERCIEMENTS

Mes remerciements s'adressent tout d'abord à mon mari, Joseph, pour la patience et la constance avec laquelle il m'a toujours soutenue dans mes démarches universitaires ainsi que dans mon désir insatiable d'apprendre et de persévérer.

Je voudrais remercier, Monsieur Philippe Wolf, responsable du Centre de Formation à la Sécurité des Systèmes d'Information du Secrétariat Général de la Défense Nationale (SGDN), pour les documents qu'il m'a procurés et pour la grande liberté qu'il m'a laissée dans le traitement du sujet de ce mémoire.

Je souhaite aussi remercier Madame Isabelle Valentini responsable des relations internationales à la Direction Centrale de la Sécurité des Systèmes d'information du SGDN, pour son aide précieuse et pour la disponibilité dont elle a fait preuve. Je regrette de n'avoir pas eu davantage de temps pour mieux exploiter les nombreux contacts qu'elle a mis à ma disposition.

J'adresse ma profonde gratitude à Monsieur le Professeur Georges Chatillon dont l'enthousiasme pour le DESS Droit de l'Internet – Administrations – Entreprises a aiguisé ma curiosité et mon intérêt pour ce domaine en constante évolution et qui a soutenu mon effort au long de cette année universitaire.

Je remercie aussi Messieurs Wilkinson et Delmas, grâce à qui j'ai pu, lors d'un stage à la DG INFSO de la Commission européenne sous leurs responsabilités, explorer de l'intérieur les rouages communautaires et acquérir une connaissance pratique des politiques européennes de la société de l'information.

SOMMAIRE

Remerciements.....	3
Sommaire	4
Introduction.....	5
Titre Premier - Sécurité des Réseaux, Fraude Informatique et Cybercriminalité	8
De l'insuffisance des approches nationales à la nécessité d'une coopération internationale.....	8
Section 1: Les limites du cadre juridique national	9
Chapitre 1: Le cadre juridique français de la lutte contre la fraude informatique	9
Chapitre 2 : Le cadre juridique français de la lutte contre la cybercriminalité	16
Section 2 : La coopération internationale pour la lutte contre la cybercriminalité	25
Chapitre 1 : De la nécessité d'une coopération internationale	25
Chapitre 2 : Les outils de la coopération judiciaire sur la scène internationale	29
Chapitre 3 : Le cadre juridique de la lutte contre la cybercriminalité : un cadre international plus qu'un cadre européen	31
Titre Second - L'Émergence d'un Cadre Juridique Européen de la Sécurité des Réseaux et des Systèmes d'information.....	40
Législation communautaire et co-régulation dans le domaine de la sécurité des réseaux et des systèmes d'information	40
Section 1 : La politique européenne de protection des données	41
Chapitre 1: Enjeux et objectifs de la politique européenne de promotion de la société de l'information	41
Chapitre 2: Le cadre juridique européen de la protection des données : l'affirmation d'une approche européenne de la sécurité.....	46
Chapitre 3 : L'application internationale des principes de la sphère de sécurité (safe harbor)	54
Section 2 : La co-régulation une approche complémentaire à la réglementation communautaire	59
Chapitre 1 : Le plan d'action visant à promouvoir une utilisation sûre d'Internet	60
Chapitre 2 : Les autres mécanismes de réglementation	63
Chapitre 3 : L'agence européenne de la sécurité des réseaux (ENISA).....	67
Conclusion	73
Bibliographie.....	75

INTRODUCTION

La révolution des technologies de l'information change radicalement la société car ses développements touchent à l'ensemble des domaines de l'activité humaine. La généralisation de l'utilisation du courrier électronique ainsi que l'accès à de vastes quantités de données, leur échange et leur diffusion par l'intermédiaire d'Internet¹ sont des illustrations de cette révolution de l'information et des nouvelles technologies et de son intrusion dans la vie quotidienne. En 2002, plus de 90% des entreprises de l'Union européenne disposent d'une connexion Internet et la majorité d'entre elles exploitent un site web; environ 40% des foyers disposent de leur propre connexion.

Ces développements font également apparaître de nouveaux types de délinquance et suscitent l'apparition de nouvelles formes de criminalité. Cette cybercriminalité a pour caractéristique essentielle le fait qu'elle ne se cantonne plus à un espace géographique donné et ne se soucie guère des frontières nationales ou des principes juridiques existants. La propagation à travers le monde des réseaux de virus informatiques dommageables témoigne bien de cette nouvelle réalité. Par ailleurs, l'identification du pays d'origine et des règles applicables à la résolution de conflits et au traitement des délits conduit à une nécessaire adaptation des règles du droit international.

En plus de son caractère transnational, voir immatériel, la question de la sécurité des systèmes d'information est extrêmement sensible car liée à la sûreté de l'Etat, au développement de son économie et au respect de ses citoyens. Alors que la garantie de la sûreté de l'Etat est l'apanage de la souveraineté nationale, les caractéristiques intrinsèques des réseaux et des systèmes d'information et des technologies inter-opérables, ainsi que le développement du cyber-terrorisme conduisent les Etats à envisager des formes de coopération dans le domaine de la sécurité des réseaux et des systèmes d'information. En effet, une approche strictement nationale de la sécurité des réseaux montre très vite ses limites.

Le propos de ce mémoire est de voir comment la coopération entre Etats dans le domaine de la sécurité des réseaux et des systèmes d'information s'exprime par la mise en oeuvre d'un cadre réglementaire européen. L'intervention européenne dans la régulation d'Internet se justifie pleinement au regard de ses domaines de compétence que sont la création d'un marché intérieur, le développement du commerce électronique, la création des réseaux transeuropéens² ainsi que la recherche et le

¹Le Conseil d'Etat apporte la définition suivante de l'espace créé par Internet: « *un nouvel espace d'expression humaine, un espace international qui transcende les frontières [...], un espace hétérogène où chacun peut agir, s'exprimer, travailler, un espace épris de liberté* », Section des rapports et études, *Internet et les réseaux numériques*, La Documentation française, Coll. Etudes du Conseil d'Etat, Paris 1998, p.3

²Titre XV du Traité de Rome instituant les Communautés européennes

développement technologique³.

³Titre XVIII du Traité de Rome instituant les Communautés européennes

La Commission européenne définit la sécurité des systèmes d'information « *comme la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, aux événements accidentels ou aux actions malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles.* »⁴

Cette définition illustre le fait que la sécurité relève à la fois de mesures techniques de protection des systèmes informatiques en même temps que de mesures juridiques de prévention et de dissuasion des délits. Comprise dans son acception la plus large la sécurité des réseaux et des systèmes d'information doit donc être analysée sous le triple angle de la protection des internautes, de celle des données transitant sur Internet et enfin de celle des infrastructures nécessaires au fonctionnement des systèmes d'information.

De même, la notion de cybercriminalité renvoie-t-elle à ces différents aspects. Ce terme désigne en effet, l'ensemble des infractions commises sur ou par un système informatique connecté à un réseau de télécommunications en général et plus particulièrement sur un réseau partageant le protocole TCP-IP, appelé communément Internet. Différentes catégories d'agissements tombent sous l'appellation de cybercriminalité :

- La première catégorie considère les technologies de l'information en tant que cibles d'infractions. Il s'agit en particulier du piratage ou de l'accès frauduleux à un système informatique, de l'atteinte à l'intégrité de données ou d'interceptions illégales.
- La seconde utilise les technologies de l'information en tant que moyen de commettre des actes criminels "classiques", tels que le télémarketing frauduleux, le détournement ou le blanchiment d'argent.
- La troisième, enfin, consiste à utiliser les technologies de l'information en tant que vecteur de "contenus informationnels illicites" tels que la pornographie juvénile, incitation à la haine, racisme et xénophobie.
- Une dernière catégorie désigne l'utilisation d'ordinateurs par des criminels pour les communications et l'entreposage de documents ou de données illicites destinées à la préparation de délits comme la préparation d'actes terroristes.

Cette catégorisation illustre le fait que la cybercriminalité renvoie à la fois au support et au contenu de l'activité illicite et a donc aussi trait au domaine de la protection des données personnelle. Ce mémoire aborde ces différents aspects relatifs à la sécurité des réseaux et des systèmes d'information en traitant de la lutte contre la cybercriminalité, de la garantie de la sécurité des données et de la sécurité des infrastructures des systèmes d'information proprement dite.

⁴Définition tirée du document « Sécurité des réseaux de l'information : Proposition pour une approche politique européenne », Communication de la Commission européenne du 6 juin 2001 (COM(2001)298 final

Dans le domaine de la lutte contre la cybercriminalité pour garantir la sécurité des internautes la mise en oeuvre d'un cadre national aussi complet soit-il montre toute sa limite. Néanmoins, la lutte contre la cybercriminalité et la fraude informatique touche au coeur des prérogatives régaliennes des Etats et repose donc sur une vision intergouvernementale de la coopération internationale. Elle s'organise sur le double plan du droit public international et sur celui de la coopération des forces de police (Titre Premier).

Outre la poursuite des infractions, la politique de la sécurité des réseaux et des systèmes d'information vise essentiellement à instaurer la confiance des utilisateurs. Pour ce faire elle implique de garantir la sécurité des données et des infrastructures. Ces domaines mettent en lumière les deux modes d'action privilégiés par lesquels l'Union européenne agit et se dote d'une réglementation propre à assurer la sécurité des réseaux et des systèmes d'information. Le premier moyen est l'harmonisation des règles juridiques des États membres. Mais, il n'est pas l'unique mode d'action des institutions européennes. En effet, celles-ci tendent à développer un autre mode d'encadrement complémentaire et plus adéquat, compte tenu des caractéristiques de l'Internet et de l'informatique, en constante évolution technologique, la co-régulation (Titre Second).

TITRE PREMIER

SECURITE DES RESEAUX, FRAUDE INFORMATIQUE ET CYBERCRIMINALITE

De l'insuffisance des approches nationales à la nécessité d'une coopération internationale

Depuis la fin des années 1990, avec la croissance puis la banalisation de l'utilisation d'Internet et le développement du commerce électronique ainsi que l'augmentation des actions de fraude informatique et de cybercriminalité, s'est instauré un mouvement de développement des règles législatives destinées à adapter le droit pénal classique aux caractéristiques d'Internet. Ce mouvement s'est notamment accentué à la suite des attentats du 11 septembre 2001 dans le cadre de mesures prises pour lutter contre le terrorisme.

La France, comme de nombreux Etats, s'est dotée d'un ensemble de normes juridiques destiné à lutter contre la cybercriminalité. Le législateur français a petit à petit mis en place un véritable arsenal juridique sécuritaire augmentant la latitude d'action et les moyens de la police judiciaire dans sa lutte contre la cybercriminalité, notamment avec le vote de certaines dispositions relatives à la société de l'information, l'adoption des lois sur la sécurité quotidienne puis de celle sur la sécurité intérieure. Ces récents développements peuvent faire craindre une mise en danger de certains principes fondateurs des libertés publiques. C'est l'objet de la Section 1 de cette première partie.

Néanmoins, cet arsenal juridique national est nécessairement limité du fait même du caractère intrinsèquement transnational de la cybercriminalité. La lutte contre la cybercriminalité nécessite l'élaboration d'une coopération internationale et la création d'un cadre juridique international original. La cybercriminalité qui touche au cœur le droit régalien des Etats s'organise sur le double plan du droit public international et sur

celui de la coopération des forces de police, notamment dans le cadre du troisième pilier communautaire. Ces évolutions sont traitées dans la Section 2 de cette première partie.

Section 1: Les limites du cadre juridique national

Par souci de simplicité, il convient d'aborder le cadre juridique français destiné en référence à deux types d'infractions pénales principales:

- les infractions directement liées aux technologies de l'information et de la communication (TIC) dans lesquelles l'informatique est l'objet même du délit, c'est-à-dire relevant de la fraude informatique;
- et les infractions dont l'exécution est liée ou facilitée par les TIC et pour lesquelles l'informatique n'est qu'un moyen, c'est-à-dire la cybercriminalité.

Les dispositions juridiques françaises spécifiques à la lutte contre la fraude informatique seront présentées dans un premier temps (Section 1) puis dans un deuxième temps, les dispositions spécifiques à la lutte contre la cybercriminalité entendue dans son second sens (Section 2).

Chapitre 1: Le cadre juridique français de la lutte contre la fraude informatique

Contexte et définition de la loi Godfrain

L'urgence de légiférer en matière de sécurité informatique apparaît en France dans les années 1980. Un article du « Canard enchaîné »⁵ publié le 28 novembre 1984 détaille par exemple la manière dont certains de ses journalistes ont pu consulter une base de données sensible à l'aide d'un minitel. Il est ainsi établi devant le grand public qu'un simple minitel et quelques connaissances techniques suffisent pour pénétrer dans les réseaux informatiques des administrations publiques et pour obtenir des informations confidentielles sur des projets nucléaires français.

Il est particulièrement intéressant de relever qu'en 1986, le droit pénal ne connaissait pas la notion de pirate informatique. L'applicabilité du code pénal à certaines formes de la criminalité informatique n'a cependant jamais fait le moindre doute. Le système d'information était lui-aussi relativement mal protégé. Plusieurs textes existaient déjà, comme la loi du 6 janvier 1978 « informatique et libertés » ou la loi du 3 juillet 1985 sur la protection du droit d'auteur comportant un chapitre sur la protection des logiciels. Mais l'absence de répression pénale spécifique et globale commençait à poser problème. En effet, certains agissements restaient en dehors du champ de répression ce qui ne permettait pas de poursuivre certaines catégories de piratages ou d'escroqueries informatiques. Aucune infraction par exemple ne punissait le fait d'accéder sans droit à un système informatique. Aucune disposition pénale ne punissait non plus le fait de prendre le contrôle d'une machine, ordinateur ou réseau informatiques. Or l'apparition et la publicité entourant ce phénomène d'attaques distantes⁶ nécessitait l'adaptation du droit pénal.

⁵Voir, Le Canard enchaîné, 28 novembre 1984, p.4

⁶Une attaque à distance est une agression contre une machine par une personne n'ayant pas les droits sur

elle. Une machine distante est toute machine autre que la sienne et que l'on peut joindre grâce à un protocole à travers un réseau.

Le dépôt par le député Jacques Godfrain d'un projet de loi en août 1986 a pour objectif de mettre en œuvre une répression globale, et conduit à la loi du 5 janvier 1988. Cette loi ajoute au code pénal sept articles entièrement dédiés aux « atteintes aux systèmes de traitement automatisé de données », les articles 323-1 à 323-7 dans le chapitre 3 du livre III du Code pénal intitulé « *des crimes et des délits contre les biens* ».

Les infractions définies par la loi du 5 janvier 1988 sont relatives aux atteintes aux « systèmes de traitement automatisé de données ». Aussi est-il important de définir la notion de système à laquelle fait appel la loi et qui coïncide avec la notion technique de système informatique. Monsieur Theyraud, rapporteur du Sénat définit la notion de système informatique, lors des travaux parlementaires, comme suit :

« tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciels, de données, d'organes entrée-sorties, et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité ».

Néanmoins cette définition n'a pas été retenue tout d'abord dans le souci de ne pas lier l'incrimination à un état trop passager de la technique et ensuite pour ne pas conserver l'exigence d'un dispositif de sécurité du système informatique. En effet, si le système existe et si son objet est bien le traitement automatisé de données, se pose la question de sa protection. La jurisprudence apporte ici une réponse négative⁷, en ne retenant pas l'existence d'un dispositif de sécurité comme une condition préalable à la réalisation de l'infraction. Autrement dit, un système peut parfaitement faire l'objet d'un accès frauduleux quand bien même il ne disposerait d'aucun mécanisme de sécurité.

Internet est ici considéré comme un vecteur de multiplication des infractions réalisées au moyen de l'informatique et de la télématique. Les dispositions de la loi reprises dans le code pénal visant à réprimer les atteintes à la confidentialité et / ou à l'intégrité des données et des systèmes de traitement automatisé des données ainsi que la jurisprudence qui s'est développée par la suite, sont transposables sans difficulté à Internet.

Champ d'application de la loi Godfrain

Les différentes infractions visées par la Loi Godfrain sont les suivantes:

Accès et maintien frauduleux dans un STAD (Système de Traitement Automatisé des Données)

Les infractions de ce type sont traitées dans l'article 323-1 du code pénal comme suit:

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an

7JOUGLEUX Philippe, « de la négligence dans la protection d'un système de traitement informatisé d'informations », *Expertises*, juillet 2000, p.220 s.

d'emprisonnement et de 15 000 euros d'amende. »

Cette disposition vise à sanctionner ceux qui cherchent à prendre connaissance d'informations confidentielles ou non, figurant dans un systèmes de traitement automatisé de données dont l'accès leur est interdit. Il faut d'une part faire la preuve du caractère frauduleux de l'accès au système et d'autre part du caractère intentionnel de la pénétration illicite.

Dans la pratique, la mise en évidence d'un détournement des moyens mis en place pour protéger le système, si elle n'est pas nécessaire, facilite néanmoins la démonstration du caractère frauduleux de l'action. La violation d'un dispositif de sécurité, l'insertion d'un fichier espion enregistrant les codes d'accès ou encore une connexion pirate visant à interroger le système à distance sont autant d'indices de la fraude.

C'est en vertu de cet article 323-1 du Code pénal que la treizième chambre correctionnelle du Tribunal de Grande Instance de Paris, a, dans son Jugement du 25 février 2000 Serge H. / GIE Cartes bancaires⁸, condamné Serge Humpich pour accès et maintien frauduleux dans un système de traitement automatisé des données afin de pouvoir fabriquer de fausses cartes bancaires à puce.

Néanmoins l'accès peut résulter d'une erreur et ne pas être intentionnel. Cependant, même si l'intrusion est le fruit d'une erreur, le simple fait de se maintenir dans le système pourra être constitutif d'une fraude. En effet, l'incrimination de maintien frauduleux vient compléter celle de l'accès frauduleux. Elle vise les situations où l'accès au système a été régulier, alors que le maintien dans ce système ne l'est pas. C'est le cas par exemple lorsque son auteur se trouve privé de toute habilitation. Ainsi une connexion dans un espace réservé d'un système ouvert au public, comme l'espace réservé d'un serveur web, effectuée sans droit d'accès correspondant entre dans cette catégorie d'infraction.

Cette infraction de maintien frauduleux a été invoquée dans l'affaire Génie logiciel et Geste c/Niel et autres⁹, où la Cour d'appel de Paris a considéré que : « *La loi incrimine également le maintien irrégulier dans un système de la part de celui qui, y ayant régulièrement pénétré, s'y serait maintenu frauduleusement* ».

L'accès ou le maintien, pour être qualifiés d'infraction, doivent être frauduleux. Ici réside ce que l'on désigne par élément moral propre à chaque infraction pénale. Cela signifie que l'acte doit être volontaire et ne pas résulter d'une simple erreur et que l'auteur de l'accès ou du maintien doit avoir conscience de l'irrégularité de son acte. La Cour d'appel de Paris l'a rappelé le 5 avril 1994, précisant que l'accès ou le maintien « *doivent être faits sans droit et en connaissance de cause* »¹⁰.

⁸Voir décision du Tribunal correctionnel de Paris, 25 février 2000, sous: http://www.legalis.net/jurisprudence-decision.php3?id_article=1200

⁹CA Paris 11^e ch. Corr. Sect. A., 5 avril 1994, Assistance Génie Logiciel et Geste c/Niel et autres. Dossier Télécommunications, *Les Petites Affiches*, n°80, du 5 juillet 1995, chronique sous la direction du professeur J.Huet

¹⁰Idem

Ainsi, peu importe que l'auteur ait procédé par jeu ou non, l'intention de nuire n'est pas nécessaire. Peu importe aussi le procédé utilisé pour réaliser l'accès, que celui-ci ne concerne qu'une partie du système ou sa totalité, que l'accès soit fait en local ou à distance; peu importe les actes effectués¹¹ sur la machine, une fois l'accès ou le maintien réalisé, l'infraction est constituée.

Les atteintes volontaires au fonctionnement du système

Une deuxième catégorie d'infractions visées par la Loi Godfrain est reprise dans l'article 323-2 du code pénal qui dispose:

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende »

L'élément matériel dans l'article 323-2 est double, puisqu'il désigne à la fois l'entrave ou le faussement du système.

En ce qui concerne l'entrave tout d'abord. Celle ci est synonyme de gêne, d'empêchement pouvant aller jusqu'à l'arrêt du système, et est susceptible d'être qualifiée dans des cas très divers. Par exemple le changement de mot de passe d'un ordinateur ou d'un réseau dans le but de le rendre inutilisable par l'administrateur réseau, ou encore du lancement d'une attaque par « déni de service »¹² (D.O.S.) en simulant un grand nombre de connexions sur un serveur dans le but d'empêcher toute personne de s'y connecter.

L'entrave peut être totale et bloquer de manière permanente les ressources informatiques d'un système de traitement automatisé de données, ou encore partielle ou ponctuelle, empêchant périodiquement l'accès aux ressources nécessaires au bon fonctionnement du système. Un tel cas s'est présenté à la Cour d'appel de Paris en 1994¹³. Il s'agissait d'un directeur technique qui avait bloqué la totalité du système informatique de son entreprise en refusant de communiquer les codes d'accès correspondants. En l'espèce la personne en question ne s'était pas contentée d'une simple abstention, mais avait préalablement modifié les codes dans le but de bloquer le système d'information de l'entreprise, fait qui constituait effectivement une entrave au fonctionnement du système.

11Il existe cependant une exception à ce dernier élément, l'alinéa 2 de l'article 323-1 qui aggrave la peine en cas de dommages au système : *«Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende.»*

12Les attaques par Denial of Service (abrégé DoS, en français déni de service) consistent à paralyser temporairement (rendre inactif pendant un temps donné) des serveurs afin qu'ils ne puissent être utilisés et consultés. Elles sont un fléau pouvant toucher tout serveur mais aussi tout particulier relié à Internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à des sociétés dont l'activité repose sur un système d'information en l'empêchant de fonctionner.

13Cour d'Appel de Paris 11^e ch. Corr. Sect. A., 5 avril 1994, « Assistance Génie Logiciel et Geste c/Niel et autres ». Dossier Télécommunications, Les Petites Affiches, n°80, du 5 juillet 1995 (chronique sous la direction du professeur J.Huet)

Toutefois même si l'incrimination d'entrave est très large du fait des termes employés, la doctrine considère que certains agissements doivent être écartés, notamment les entraves pouvant résulter d'une grève, de la suspension ou de la rupture d'un contrat de prestations de services informatiques.¹⁴

Le faussement, quant à lui, évoque un résultat qui, à cause de l'altération ou de la déformation du système, est différent de ce qu'il aurait dû être. Tel serait par exemple le cas d'un virus informatique qui fausserait le fonctionnement normal des programmes et de la gestion des données. L'article 323-2 constitue un bon fondement pour une action juridique contre les atteintes les plus courantes sur Internet que sont l'insertion de virus¹⁵ informatiques ou de bombes logiques¹⁶. En effet, ceux-ci ont pour effet de modifier ou de supprimer des données et donc de fausser le fonctionnement du système. Si les virus proprement dits sont connus depuis les années cinquante et donc bien avant l'apparition de Internet sous la dénomination « d'automates d'autodestruction de programmes », Internet est un vecteur privilégié pour leur prolifération, comme l'atteste les attaques continues de la toile, telles que celle des récents « I love you » et « mydoom ».

Le délit suppose que l'auteur a conscience de l'entrave au système ou du fait qu'il fausse le fonctionnement du système sans quoi l'infraction ne saurait être constituée. De même il doit avoir agi contre la volonté du possesseur du système. À l'instar de l'accès ou du maintien frauduleux, le texte n'exige pas l'intention de nuire, peu importe donc que l'auteur du délit ait agi par jeu, ou par défi.

Action frauduleuse sur les données

La troisième catégorie d'infraction visée dans la Loi Godfrain est reprise dans l'article 323-3 du Code pénal:

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45 000 euros d'amende »

L'article 323-3 vise les cas où l'action frauduleuse a pour objet principal les données du système. Certains faits sont, à ce titre, indifférents : Le fait que le système soit en cours d'élaboration ou qu'il soit en état de fonctionner ainsi que le fait que la personne ait accédé régulièrement au système ou non n'entrent pas en ligne de compte. L'action incriminée porte, si l'on s'en tient à une lecture étroite du texte, sur les données du système. Dans une conception stricte, on est en droit de penser que l'action frauduleuse sur les programmes, et non les données, ne relève pas de l'article 323-3 du code pénal.

14FÉRAL-SCHUHL, Christiane, *Cyberdroit – le droit à l'épreuve de Internet*, 3ème édition, Dunod, Paris, 2002, p. 43 et s.

15Un virus informatique désigne un programme informatique qui possède la particularité de se reproduire et de se propager en utilisant les capacités du système informatique qui l'héberge.

16Une bombe logique est un programme informatique de destruction réglé sur le temps conçu pour s'activer dans des conditions prédéterminées par son concepteur.

Supposons par exemple qu'une personne introduise une *backdoor*¹⁷ dans un serveur afin de se ménager un accès régulier au système compromis. On pourrait alors plaider le fait que c'est un programme qui a été modifié et non une donnée et que l'article 323-3 ne s'applique pas au cas présent. Néanmoins, le terrain de l'article 323-3 n'est pas le seul fondement sur lequel s'appuyer pour sanctionner l'acte en question. On pense à l'article 323-1, car pour avoir introduit une backdoor dans un programme il faut nécessairement avoir accédé ou s'être maintenu frauduleusement dans le système.

La protection pénale des données informatisées est une démarche intéressante car un grand nombre de techniques de fraude informatique supposent l'introduction, la suppression ou la modification de données au sein du système victime. L'infraction de l'article 323-3 a donc de grandes chances de trouver application dans de nombreux cas. La peine est sévère et s'accompagne de la réparation des dommages causés à la victime.

Contrairement à l'accès ou au maintien frauduleux dans un système, l'auteur doit ici avoir agi intentionnellement, en sachant qu'il introduit, modifie ou supprime des données au sein du système. Plusieurs affaires ont eu lieu dans lesquelles les prévenus avaient confectionné des disquettes de démonstration qui contenaient un virus. À plusieurs reprises les juges ont relaxé les personnes en question faute de la preuve de leur connaissance de la présence *a priori* du programme malveillant¹⁸.

Autres éléments de la loi du 5 janvier 1988

Les infractions présentées constituent le socle de la répression pénale de la criminalité informatique appliquée aux atteintes aux systèmes de traitement automatisé de données en France. Elle ne sont pourtant pas les seules dispositions de la loi du 5 janvier 1988.

L'association de cyber malfaiteurs

Cette infraction est définie dans l'article 323-4 du Code pénal comme suit :

« La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

L'objectif de ces dispositions est de lutter contre les clubs de crackers¹⁹ dont la

17En français « porte dérobée », un backdoor est un petit bout de code introduit intentionnellement par une personne dans un système pour pouvoir ouvrir un accès dérobé à ce système et ainsi en prendre le contrôle quand elle le désire.

18PADOVA Yann, « *Un aperçu de la lutte contre la cybercriminalité en France* », revue de Sciences Criminelles (4), Oct-déc, 2002, p.765 et s.

19Il y a souvent confusions entre le terme hacker et celui de cracker: Les hackers sont des personnes qui s'intéressent de près aux systèmes d'exploitation. Ils cherchent constamment à approfondir leurs connaissances et à les faire partager. Leur but n'est pas de nuire mais au contraire de connaître pour améliorer. Les crashers (ou crackers), par contre, violent des systèmes à distance dans un but de malveillance. Ils détruisent des données et empêchent le fonctionnement de services .

prolifération a été particulièrement forte depuis les années 1980.

Les exemples cités lors des débats parlementaires précédant l'adoption de la Loi Godfrain font référence à des personnes qui s'échangent les mots de passe ou les codes d'accès nécessaires afin de préparer une intrusion malveillante dans un système d'information.

L'article 323-4 ne définit pas la notion de groupement, ni celle d'entente. L'examen de la jurisprudence révèle que les juges retiennent la notion de groupement alors que l'entente résultait d'un simple concours de volontés. À plus forte raison cette notion serait sans doute retenue dans le cadre d'une association vouée à la préparation des délits des articles 323-1 à 323-3. Le nombre minimum de participants pour que l'entente soit constituée, ou le groupement formé importe peu, la jurisprudence l'ayant retenu à partir de deux. Les personnes morales comme physiques sont concernées.

L'entente ou le groupement doivent avoir été établis en vue de la préparation d'une ou plusieurs infractions et se concrétiser par un ou plusieurs faits matériels : échange de mots de passe subtilisés ou encore confection d'un virus destiné à frapper un système donné. Plusieurs jugements ont été rendus sur le fondement de l'article 323-4. Dans un arrêt de la Cour d'appel d'Aix du 2 juin 1993²⁰, l'entente a été retenue alors qu'une personne avait remis des cartes bancaires à un contrefacteur pour qu'il procède à leur ré-encodage.

La tentative

L'article 323-7 du Code pénal dispose :

« La tentative des délits prévus par les articles 323-1 à 323-4 est punie des mêmes peines. »

La répression de la tentative en droit pénal n'est pas systématique pour les délits. L'article 323-7 vient donc combler l'absence de répression en cas d'essai raté de l'une des trois infractions présentées.

Evolutions postérieures à la loi Godfrain

La loi pour la confiance dans l'économie numérique²¹ renforce les dispositions de la loi Godfrain. En effet, elle insère dans le Code pénal un article 323-3-1 selon lequel :

« Le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un programme d'ordinateur ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

Ce nouvel article aggrave également les peines encourues au titre des articles 323-1 à 323-3. Les peines prévues pour l'accès ou le maintien frauduleux dans un système sont doublées. Elles passent d'un an d'emprisonnement et 15 000 euros d'amende à deux ans et 30 000 euros. Lorsque cet accès a causé un dommage, les peines passent à trois ans et 45 000 euros d'amende. Enfin les peines des articles 323-2 et 323-3 sont

20PANSIER Frédéric-Jérôme, *La criminalité sur Internet*, Paris : PUF (Que sais-je ? 3546), 2e éd., 2001
21Adoptée le 21 juin 2004, [LOI n° 2004-575](#) pour la confiance dans l'économie numérique

portées à trois ans et 75 000 euros d'amende en cas de dommage.

Il existe à l'heure actuelle, en France, une panoplie de textes pour réprimer la fraude informatique. Face à ces exactions, le droit est donc loin d'être démuné. Plusieurs infractions sont répertoriées par notre code pénal : l'accès et le maintien frauduleux dans un système ou encore la falsification des données.

Cependant, les spécificités d'Internet rendent difficiles la preuve de l'agissement illicite et l'identification de l'auteur de l'infraction du fait de la volatilité des données, de l'immédiateté de l'action et surtout de la difficulté à localiser la personne effectuant l'action malveillante.

Chapitre 2 : Le cadre juridique français de la lutte contre la cybercriminalité

La loi Godfrain a intégré dans le code pénal les articles nécessaires à la lutte contre la fraude informatique. Ce faisant, elle a aussi jeté les premières bases de la lutte contre la cybercriminalité. Cette loi est symptomatique d'une époque où la pratique des réseaux informatiques n'était encore réservée qu'à une poignée d'initiés. Le développement des réseaux informatiques a démultiplié les possibilités d'infractions par voie informatique et favorisé leur expansion. Dès lors, de nouvelles réflexions sur la sauvegarde de l'ordre public et de la sécurité nationale sur Internet sont apparues dès le milieu des années 90. La nécessité d'augmenter les moyens de lutter contre les personnes utilisant Internet comme moyen pour leurs délits a donné lieu à la mise en place d'un cadre juridique facilitant l'identification et la poursuite des auteurs d'infractions, cadre qui a été renforcé suite aux attentats commis aux Etats-unis le 11 septembre 2001.

L'obligation de la conservation des données de connexion

Définition et enjeux

La conservation des données de connexion est l'une des premières demandes des autorités d'enquêtes afin d'augmenter leur efficacité. Le fait de pouvoir consulter ces données permet, en effet, d'identifier et de localiser les auteurs de fraude informatique ou les auteurs utilisant Internet pour commettre leurs infractions. Cette demande est fortement liée aux caractéristiques intrinsèques d'Internet et notamment la volatilité et l'immatérialité des informations numériques qui rendent extrêmement simples et instantanées la modification et la suppression des preuves.

Les données de connexions sont des éléments techniques automatiquement collectés par le fournisseur d'accès ou de contenu à l'occasion d'une connexion et consignés dans le journal ou fichier log²².

22Un log (ou fichier log) se présente sous la forme d'un fichier texte classique, reprenant de façon

chronologique, l'ensemble des événements qui ont affecté un système informatique et l'ensemble des actions qui ont résulté de ces événements. La traduction française la plus exacte est journal.

Le débat autour de la conservation des données de connexion²³ se concentre sur trois questions principales :

1. Dans quelles circonstances et sous quelles conditions de telles informations peuvent-elles être demandées ?

2. Combien de temps les fournisseurs d'accès peuvent-ils se voir imposer la conservation de ces données ?

3. Quelle est l'étendue de la notion de données à conserver? S'agit-il uniquement des heures de début et de fin de connexion et du numéro IP²⁴ de l'ordinateur de l'utilisateur ou la notion recouvre-t-elle des données plus personnelles telles que les adresses des sites visités et les adresses des messages électroniques ?

Les données conservées constituent des outils d'identification et de traçabilité des individus plus ou moins puissants suivant l'étendue qui est conférée à cette notion.

Une progressive mise en place de l'obligation de conservation des données de connexion

Le rapport du Conseil d'Etat de 1998

Dans son rapport « Internet et les réseaux numériques »²⁵ de juillet 1998, le Conseil d'Etat remarque:

"Les données conservées associées à l'adresse IP par le fournisseur d'accès peuvent permettre de suivre, pas à pas, l'activité d'un internaute (les sites visités, la date et l'heure, les documents téléchargés, la participation à un espace de discussion, les messages électroniques expédiés et reçus) aussi longtemps que ces données sont conservées »

En 1998 déjà, le Conseil d'Etat recommande que les données de connexions ne soient pas détruites trop vite "*afin de faciliter les poursuites et l'établissement de la preuve des infractions*". Constatant que le délai de prescription légale des délits est de trois ans, que la durée de conservation des données relatives aux appels téléphoniques par France Télécom est de un an et que la CNIL recommande alors un délai de conservation maximal d'un an, le Conseil d'Etat propose, sous réserve d'expertise, d'adopter une durée de conservation d'un an.

23M.P FENOLL- TROUSSEAU et G. HAAS, Internet et protection des données personnelles, Paris : Litec 2000, p. 54 et s.

24Sur Internet, les ordinateurs communiquent entre eux grâce au protocole TCP/IP qui utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits), on les note donc sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un entier de 0 à 255. Ces numéros servent aux ordinateurs du réseau pour se reconnaître, ainsi il ne doit pas exister deux ordinateurs sur le réseau ayant la même adresse IP (IP signifie *Internet Protocol*). Par exemple, 194.153.205.26 est une adresse TCP/IP donnée sous une forme technique. Ce sont ces adresses que connaissent les ordinateurs qui communiquent entre eux. C'est l'IANA (*Internet Assigned Numbers Agency*) qui est chargée d'attribuer ces numéros.

25CONSEIL D'ETAT , Section des rapports et études, « *Internet et les réseaux numériques* », La Documentation française, Coll. Etudes du Conseil d'Etat, Paris 1998

Le projet de loi sur la société de l'information

Les conclusions du rapport du Conseil d'Etat sont reprises dans la dernière version du projet de Loi sur la Société de l'Information (LSI) adoptée par le Conseil des ministres le 13 juin 2001. Le projet de loi envisage au sein de son Titre II un Chapitre III intitulé " *L'effacement des données relatives aux communications* ". L'article 14 pose le principe d'effacement ou d'anonymisation de toute donnée de communication dès que celle-ci est achevée. Cette disposition est inspirée de la législation communautaire concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications abordée dans le titre second de ce mémoire.

Le principe ainsi posé contient néanmoins l'exception suivante :

"Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques." (art. 14-II).

Les précisions sur la portée et les modalités de mise en œuvre de la conservation des données sont confiées par le projet de LSI au pouvoir réglementaire. Un décret en Conseil d'Etat doit en effet déterminer, après avis de la Commission nationale de l'informatique et des libertés (CNIL), les catégories de données et la durée de leur conservation selon l'activité des opérateurs et la nature des communications (art. 14-II).

Ce décret doit obéir aux règles fixées par l'article 14-IV du projet de loi, qui précise notamment que les données en cause "*portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers*". Les données ne peuvent pas concerner, en outre, "*le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications*."

La délibération de la CNIL sur le projet de loi sur la société de l'information

Saisie de la question relative à la conservation des données de connexion abordée au sein de la LSI, la Commission nationale informatique et liberté (CNIL)²⁶ constate que les autorités ont déjà la possibilité de procéder à des interceptions de communication sur Internet dans les conditions prévues par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications. Elle remarque ainsi que le projet recherche à étendre, par le biais de la conservation des données de connexion, les possibilités dont devraient disposer les autorités publiques pour fins

26 Délibération 01-018 de la CNIL du 3 mai 2001 portant avis sur le projet de loi sur la société de l'information

d'investigations et de constitution de preuves.

L'obligation de conservation des données dérogeant, selon la CNIL, au droit commun, elle demande que la portée et les modalités de mise en œuvre de cette obligation soient clairement et précisément fixées par le législateur et non par le pouvoir réglementaire. Par ailleurs, la Commission estime qu'une durée de conservation maximale de trois mois serait "*adaptée aux objectifs d'intérêt public poursuivis par le projet de loi*" et parfaitement proportionnée aux intérêts en cause. Enfin, la CNIL demande à ce que les conditions dans lesquelles des données personnelles peuvent être saisies dans le cadre d'une procédure judiciaire soient précisées, compte tenu du fait que ces données sont conservées par un tiers.

L'article 29 de la loi sur la sécurité quotidienne

Suite à un changement gouvernemental qui a rendu le projet de loi sur la société de l'information caduque, celle-ci n'a jamais été adoptée. C'est la loi relative à la sécurité quotidienne du 15 novembre 2001 qui en reprend quasi intégralement les articles concernant la conservation des données de connexion. Cette loi fixe dans le droit positif français certaines mesures sécuritaires spécifiques à Internet, dont notamment la conservation, pendant une période d'un an, des données relatives à une communication et ce "*pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales*" (art.29). Ces données, précise la loi, ne peuvent "*en aucun cas, porter sur le contenu des correspondances échangées ou des informations consultées sous quelque forme que ce soit*", mais concernent seulement l'identité des utilisateurs et les caractéristiques techniques des services fournis par les prestataires de communication comme par exemple les adresses IP, les adresses de messagerie électronique envoyées ou reçues, ainsi que les adresses des sites web visités.

L'obligation de conservation des données de connexion en débat

Cette obligation de conservation des données de connexion donne lieu à de nombreuses récriminations notamment de la part d'associations tels que Iris²⁷ ou I3C²⁸ qui s'inquiètent d'une éventuelle possibilité d'atteintes aux libertés fondamentales, notamment la liberté d'expression. Concernant la crainte d'une atteinte aux libertés fondamentales, il est à noter que le principe d'obligation de conservation des données de connexion respecte les normes juridiques internationales. En effet, qu'il s'agisse de la convention du Conseil de l'Europe du 28 janvier 1981²⁹ sur la protection des personnes ou de la directive européenne sur la protection des données de 1995³⁰, ces deux textes prévoient une exception au principe d'effacement des données à l'issue de la communication lorsqu'il y va de la recherche, de la constatation et de la poursuite des infractions pénales. Cependant, il faut veiller à ce que cette poursuite soit elle-

27IRIS, Imaginons un Réseau Internet Solidaire, <http://www.iris.sgdg.org>

28I3C, Internet Créatif Coopératif et Citoyen, <http://www.i3c-asso.org>

29Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel - STCE no. : 108 disponible sous <http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm>

30Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, [JOUE n° L. 281 du 23.11.1995]

même encadrée par des principes juridiques respectant les libertés fondamentales.

Un autre aspect de la conservation des données de connexion alimente le débat. Il s'agit du coût élevé que celle-ci représente pour les opérateurs et les fournisseurs d'accès à Internet, qui allèguent que cette obligation s'accompagne d'un alourdissement excessif de leur coût de gestion.

Les interceptions

Le secret des correspondances émises par voie des télécommunications est garanti par la loi³¹. Les interceptions de communications, plus connues sous le terme d'"écoutes", sont donc des procédures exceptionnelles permettant de déroger à ce principe dans un cadre juridique clairement établi : « *il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci* »³². Ce cadre a été fixé par la loi de 1991 qui distingue deux type d'écoute : les interceptions judiciaires³³ et les interceptions de sécurité³⁴.

Ces procédures ont été développées à l'origine pour encadrer les interceptions dans le domaine des télécommunications fixes. Du fait de leur généralité, elles s'appliquent à la téléphonie mobile ainsi qu'à Internet puisqu'elles concernent l'ensemble des correspondances « *émises par voie des télécommunications* »³⁵. L'article L. 32 du Code des postes et télécommunications entend en effet par télécommunication « *toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques* ».

Les interceptions judiciaires - Le Code de procédure pénale

Les articles du Code de procédure pénale issus de la loi du 10 juillet 1991 prévoient désormais que les interceptions sont possibles « *en matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement* ». Dans ce cas, le juge d'instruction peut « *prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications.* » (art. 100), et ce pour une durée maximum de quatre mois, durée cependant renouvelable (art. 100-3). Il est à noter que « *les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.* » (art. 100-6). Enfin, l'article 100-7 encadre plus strictement les capacités d'interception pour ce qui concerne les "lignes" d'un député, d'un sénateur ou d'un avocat.

31Le secret des correspondances est notamment inscrit dans l'article 1er de la loi du 10 juillet 1991, et l'article L.32-3 du Code des postes et télécommunications.

32Art. 1er de la loi du 10 juillet 1991

33Art. 100 à 100-7 du Code de procédure pénal

34Loi du 10 juillet 1991

35Art. 1er de la loi du 10 juillet 1991

Les interceptions de sécurité

Les autorités judiciaires pourront avoir accès aux conventions de chiffrement des données chiffrées par le présumé délinquant par l'entremise des prestataires de services de cryptologie. Le nouvel article 11-1 de la loi du 10 juillet 1991 impose cette obligation de remise aux agents autorisés dans les conditions prévues à l'article 4 de ladite loi:

« L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou de la personne que chacun d'eux aura spécialement déléguée. Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées. »

Néanmoins, les procédures de déchiffrement s'inscrivent dans le cadre de l'article 3 de la loi du 10 juillet 1991, c'est-à-dire qu'elles concernent exclusivement *« des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous. »*

Le texte vise les prestataires de façon plus large que dans le projet de LSI, qui faisait porter les obligations sur ceux dont les prestations incluaient *« la gestion de convention secrète »*. Aujourd'hui, il apparaît que tous les prestataires sont concernés à partir du moment où ils fournissent des prestations de cryptologie. Ainsi, toute personne qui procède à l'utilisation de la cryptographie dans la diffusion d'un message quelconque pourrait être visée par cet article. En pratique, il existe des logiciels de cryptographie comme par exemple OpenPGP qui permettent à l'expéditeur, et en conséquence au destinataire, de garder secrète la convention utilisée sans qu'un prestataire n'intervienne. De la sorte, aucun fournisseur de cryptologie ne possède jamais une copie de cette convention. Dans une perspective identique, un prestataire qui héberge les clés privées de ses clients pourrait être contraint de les remettre, étant précisé que techniquement, on ne peut pas brider la fonction de chiffrement des bi-clés de signature électronique. Le champ d'application de cet article se révèle très extensif et soulève des questions relatives à la protection des libertés fondamentales assez importantes. Il faut cependant trouver un équilibre entre les besoins de protection de l'Etat et les droits et libertés individuels.

En cas de non remise ou de non mise en œuvre des conventions permettant de déchiffrer les données conformément à la demande, les personnes sont passibles de deux ans d'emprisonnement et de 30 000 € d'amende (article 11-1 al. 3). Le décret n°2002-997 du 16 juillet 2002³⁶ précise les procédures de mise en œuvre de ces obligations ainsi que la compensation financière qui devra être assurée par l'Etat en

³⁶Décret n° 2002-997 du 16 juillet 2002, Décret relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

application de l'article 11-1 al. 3.

C'est l'intégralité des frais liés à l'obligation de mise en œuvre qui sera compensée, « sur la base des frais réellement exposés par le fournisseur et dûment justifiés par celui-ci » (article 6 du décret). Selon l'article 3 du décret, « les conventions mentionnées (...) permettant le déchiffrement des données s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données. » Une telle définition est très large ; elle vise non seulement toutes les clés de déchiffrement (symétriques et asymétriques), mais aussi les services de messagerie chiffrée, voire les procédés de signature électronique et d'authentification.

Perquisitions et saisies

Le Code de procédure pénale encadre les procédures de perquisition et de saisie³⁷ mises en oeuvre dans le cadre de la lutte contre la cybercriminalité en France.

La perquisition (art. 56 s., 76 et 94 s. du Code de procédure pénale) est destinée à rechercher, en vue de les saisir, tous papiers, effets ou objets susceptibles de faire progresser une enquête. Cette mesure d'investigation peut être effectuée en tous lieux et notamment au domicile d'une personne soupçonnée. La perquisition est menée par un officier de police judiciaire agissant sous la direction et le contrôle de l'autorité judiciaire (procureur de la République ou juge d'instruction). Ses modalités diffèrent selon le cadre juridique de l'enquête (enquête préliminaire, enquête flagrante, information judiciaire). La perquisition doit en principe être effectuée de jour et en présence de la personne chez laquelle elle a lieu.

La saisie (art. 56 s., 76 et 97 s. du Code de procédure pénale) de documents ou d'objets peut être effectuée à la suite d'une perquisition. Elle consiste à mettre à la disposition de l'autorité judiciaire tous biens ou documents susceptibles de concourir à la manifestation de la vérité dans le cadre de l'enquête en cours, de façon à empêcher la destruction d'éléments de preuve.

L'obligation de déchiffrement dans le cadre de procédure pénale

L'article 30 de la loi sur la sécurité intérieure vise à tenir compte du chiffrement de plus en plus fréquent des données saisies ou interceptées. Il complète donc le Code de procédure pénale en créant une procédure de déchiffrement qui s'applique tant aux données collectées dans le cadre de saisies ou perquisitions, qu'aux données obtenues dans le cadre des interceptions judiciaires. Il est à noter que cet article ne prévoit pas la possibilité d'une saisie ou perquisition en ligne, qui restent donc impossibles dans l'état actuel des textes .

L'article prévoit la possibilité pour le procureur de la République, la juridiction d'instruction ou la juridiction de jugement de désigner un tiers qualifié « en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de [ces] informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de chiffrement, si cela apparaît nécessaire ».

³⁷ Voir en particulier les articles 56 à 60 et 76, 706-24, 706-24-1 du Code de procédure pénale

Si « *la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent* », le Procureur de la République, la juridiction d'instruction ou de jugement peuvent avoir recours « *aux moyens de l'Etat couverts par le secret de la défense nationale* ».

Quelques interrogations subsistent quant à l'application de cet article : la question de la rémunération de la prestation de déchiffrement n'est pas évoquée et les conséquences de l'endommagement des données en cas de déchiffrement mal fait ne sont pas abordées. En outre, les garanties sur les conditions et les résultats du déchiffrement des messages pourraient être précisées. En pratique, ces dispositions mettent à la charge des fournisseurs des prestations de cryptologie et des éditeurs de logiciels de chiffrement l'obligation de prévoir des backdoors (portes cachées) dans leurs produits, afin de pouvoir procéder au déchiffrement quand cela leur est demandé par les autorités compétentes.

Dans le cadre de ces procédures l'autorité judiciaire fait appel aux services techniques de déchiffrement sans avoir pour autant les moyens de les contrôler de façon effective puisque qu'ils sont susceptibles d'être protégés par le secret de la défense nationale. Le risque existe que le service décrypteur se montre déloyal, par exemple en indiquant qu'un message n'a pas été décrypté alors qu'il l'a été. Il est évident qu'un texte de loi ne peut être fondé sur le soupçon vis-à-vis de services publics. Il reste que des garanties pourraient être demandées en la matière.

Vers la mise en place d'un arsenal sécuritaire ?

Le 12 et 13 février 2003, la loi sur la sécurité intérieure (LSI) est adoptée par l'Assemblée nationale et le Sénat. Cette loi vient compléter la loi sur la sécurité quotidienne dans le domaine informatique. En effet, cette loi prévoit que les fournisseurs d'accès à Internet doivent mettre à la disposition de l'officier de police judiciaire, sur demande de celui-ci, « *les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent et ce par voie télématique ou informatique dans les meilleurs délais* » (art. 8.1).

Par ailleurs, l'officier de police judiciaire peut, sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, requérir des opérateurs de télécommunications de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs. Cette disposition rend caduque la disposition de l'article 29 de la LSQ qui prévoyait que la conservation des données ne peut, en aucun cas, porter sur le contenu des communications. Enfin, l'article 8 bis de la loi sur la sécurité intérieure permet aux officiers de police judiciaire de procéder à la perquisition en ligne, en accédant « *par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ».

Ces dispositions augmentent de manière considérable les moyens mis à disposition de la police judiciaire. L'ensemble de ces évolutions laissent craindre une dérive sécuritaire. Il faut néanmoins les réintégrer dans leur contexte. La libéralisation de l'utilisation des moyens et des prestations de cryptologie et leur développement consécutif sans précédent a rendu nécessaire la mise en place de tels dispositifs. Néanmoins, il est bon de rappeler que les textes de droit pénal sont d'interprétation stricte et qu'à ce titre leur application n'est pas admissible en dehors des actes qualifiés par le législateur de terrorisme alimenté notamment par le trafic de stupéfiant et le trafic d'armes. Il faut donc rester vigilant quand à l'application de ces nouvelles règles dans les affaires pénales et veiller à la sauvegarde des droits et libertés fondamentales.

Section 2 : La coopération internationale pour la lutte contre la cybercriminalité

Chapitre 1 : De la nécessité d'une coopération internationale

Les limites de l'ordre juridique national en matière de cybercriminalité

La nécessité d'une étroite harmonisation internationale dans le domaine de la cybercriminalité résulte avant tout de la grande mobilité des informations dans les systèmes informatiques. Cette mobilité des données rend possible la perpétration d'une infraction au moyen d'un ordinateur dans un pays pendant que le succès de cet acte criminel se réalise dans un autre pays. Ainsi de tels délits demandent une coopération internationale effective qui est aussi essentielle pour une protection effective des systèmes de télécommunication traversant plusieurs pays. L'exportation des programmes informatiques à l'étranger justifie aussi la nécessité d'une réglementation juridique internationale.

En effet, l'Internet, en tant qu'espace de communication ouvert, s'affranchit de toute contrainte territoriale et permet la diffusion de tout type d'information sans aucune contrainte géographique. En revanche, le droit pénal est une des expressions de la souveraineté des Etats et, en ce sens, possède une dimension territoriale. En effet, en matière pénale, le juge d'instruction et la police judiciaire recherchent classiquement et principalement à localiser et identifier l'auteur d'une infraction et à préserver les éléments de preuve pour matérialiser l'infraction qui peuvent se trouver sur le territoire d'un autre Etat.³⁸ Selon l'ordre juridique national applicable dans le pays de destination de l'information, celle-ci pourra être considérée comme licite ou illicite, souvent en fonction de la force variable des principes de liberté d'expression et de respect de la vie privée.

En résumé, la lutte contre la cybercriminalité se heurte à trois contraintes principales :

- l'anonymat qui peut être très efficacement organisé sur les réseaux ;
- la volatilité des informations, c'est-à-dire la possibilité de modifier et de supprimer des éléments de preuve quasi instantanément, inhérente à leur nature numérique ;
- le caractère généralement transnational des comportements délictueux.

Dans beaucoup de pays, les lois existantes sont insuffisantes. Sur 52 pays interrogés par la firme américaine Mc Connell International dans une étude réalisée pour le Conseil de l'Europe³⁹, une dizaine seulement ont adapté de façon substantielle leur législation pour se protéger des attaques informatiques; une dizaine ont opéré des mises à jour partielles et treize autres sont en train de s'y préparer. Et ce rapport

38Xavier LE CERF, « Lutte contre la cybercriminalité : le Projet de convention du Conseil de l'Europe sur la cybercriminalité » www.caprioli-avocats.com, Première publication : Juriscom.net, 19 avril 2001

39Dossier « Cybercriminalité » du Conseil de l'Europe accessible sur <http://www.coe.int>

d'expertise de conclure, « *les pays où les protections juridiques ne sont pas adéquates, deviendront moins capables d'entrer dans la concurrence de la nouvelle économie* » .

Il est intéressant de noter que les législations nationales en matière de criminalité informatique sont globalement récentes. Quelques divergences peuvent être relevées notamment en matière d'incrimination du piratage. Ainsi aux Etats-Unis, l'accès non autorisé à un système informatique n'est-il incriminé que s'il s'agit d'un ordinateur d'une administration publique. Au Japon, cette infraction pénale n'a été créée que par une loi d'août 1999. La Russie fait exception puisque le nouveau code pénal en vigueur depuis le 1er janvier 1997 ne qualifie pas comme une infraction pénale l'accès sans autorisation à un ordinateur. Tous les pays du G8 ont par contre des lois qui assurent la protection de la confidentialité, de l'intégrité et de la disponibilité des données et des systèmes informatiques et ont le pouvoir de poursuivre quiconque y porte atteinte.

En outre, les pays du G8 ont mis en place des structures spécifiquement dédiées à la lutte contre la criminalité de haute technologie. A titre d'illustration, en Italie, "le service de la police de la communication" est chargé de poursuivre toutes les infractions commises en matière de courrier postal, d'informatique et de communication téléphonique. Ce service central est appelé à être complété par la création de plusieurs centres régionaux. Au Japon, l'agence nationale de police a créé au début de 1996, une unité de recherche sur la sécurité des systèmes d'information. Ce service inclut des ingénieurs ainsi que des enquêteurs. En Russie, une division spéciale a été créée en 1998 au sein du ministère de l'intérieur afin de lutter contre la criminalité informatique⁴⁰.

La lutte contre la cybercriminalité ne peut se concevoir que dans un cadre de coopération internationale. Le caractère transnational des réseaux de communication et des systèmes informatiques renforce considérablement les difficultés que rencontrent déjà, au niveau national, les services judiciaires et répressifs pour traquer les délinquants informatiques. Dès lors, le risque est grand, aujourd'hui, de voir apparaître des "paradis virtuels" comparables aux paradis fiscaux, implantés dans des Etats assurant l'impunité des comportements incriminés dans d'autres pays. C'est pourquoi, les enceintes internationales se sont saisies récemment de la problématique de cette nouvelle forme de criminalité.

L'Organisation de Coopération et de Développement Economique (OCDE) a ainsi traité de la question des paradis virtuels. Le Conseil a adopté une recommandation le 25 juillet 2002, donnant des « Lignes directrice régissant la sécurité des systèmes et réseaux d'information »⁴¹. La mise en oeuvre de ces lignes directrices a été entérinée par un plan d'application⁴² prévoyant entre autres un questionnaire d'enquête sur les

40PANSIER Frédéric-Jérôme. *La criminalité sur Internet*. Paris : PUF (Que sais-je ? 3546), 2e éd., 2001, 128 p.

41OCDE, « Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité », Recommandation du Conseil de l'OCDE, 1037ème session, 25 juillet 2002, 29 p.

42Le plan d'application de l'OCDE a été approuvé par les pays membres de l'OCDE en 2002 et a été republié, après de nouvelles révisions, sous forme de document déclassifié, sous la cote DSTI/ICC/REG(2003)5/REV1, par le Forum mondial de l'OCDE sur la sécurité des systèmes et

mesures prises par les pays membres de l'OCDE pour la mise en oeuvre de ces lignes directrices.

réseaux d'information d'Oslo

Dans la synthèse des réponses faites à ce questionnaire met en lumière l'importance de la coopération internationale pour les Etats membres de l'OCDE, qui la place en troisième position d'importance dans la classification des mesures pour lutter contre la cybercriminalité⁴³.

Une harmonisation internationale du droit et des procédures ainsi qu'une étroite coopération judiciaire est inévitable et particulièrement nécessaire face à une cybercriminalité de plus en plus organisée et internationalisée. Cette harmonisation, qui se fera sans aucun doute, est devenue une priorité majeure des Etats qui sont entrés dans la société de l'information, avec une volonté forte d'y associer le plus grand nombre d'Etats possible. C'est l'objectif que les Etats membres du Conseil de l'Europe se sont fixés, conformément aux bases qui ont été définies par le G8.

Lors du sommet du G8 de Paris sur la cybercriminalité, en mai 2000, le Président de la République Française a évoqué le « *besoin d'un Etat de Droit international, un cadre juridique universel à la mesure du caractère mondial de l'Internet. Un cadre qui dans le respect des souverainetés, définit les infractions soumises et fixe les procédures admises pour les établir et les réprimer* ».

Cette aspiration à la construction de cet "Etat de Droit international" et à la création d'un cadre juridique international illustre la nécessité d'une coopération internationale, en complément des ordres juridiques nationaux pour combattre la cybercriminalité.

Les caractéristiques intrinsèquement transnationales de la cybercriminalité

Les acteurs économiques sont des cibles de choix pour la cybercriminalité, mais les administrations publiques ou les simples citoyens ne sont pas pour autant à l'abri. Une enquête dans les milieux d'affaires aux Etats-Unis a révélé que 85% des entreprises sondées ont été victimes d'actes de piratage. En Grande-Bretagne, un rapport de la Communications Management Association (CMA) affirme qu'un tiers des grandes entreprises et des administrations publiques du pays ont été l'objet d'attaques informatiques. Aux Etats-Unis, le Pentagone à lui seul, a enregistré en 2001 plus de 22000 agressions électroniques contre ses systèmes et le FBI a recensé 5000 infrastructures extrêmement vulnérables à la criminalité informatique capable selon son directeur Ronald L. Dick, "de déstabiliser l'économie entière d'un pays."

Mesurer l'impact économique de la cybercriminalité n'est pas chose facile dans la mesure où les faits dénoncés ne représentent que la partie émergée de l'iceberg. Un tiers seulement des victimes déclareraient les faits selon plusieurs études réalisées en Europe et aux Etats-Unis. On estime que la fraude sur les cartes de crédit s'élève à quelque 400 millions de dollars par an. Les attaques de virus ont été chiffrées à près de 12 milliards de dollars. Enfin, le manque à gagner pour les industries victimes d'atteintes à la propriété intellectuelle et de contrefaçons atteindrait 250 milliards de dollars par an, soit près de 5% des échanges mondiaux⁴⁴.

43 OCDE, Direction de la Science, de la Technologie et de l'Industrie, Comité de la politique de l'information, de l'informatique et des communications, Groupe de travail sur la sécurité de l'information et la vie privée, « Synthèse des réponses à l'enquête sur la mise en œuvre des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité », DSTI/ICPP/REG(2003)8/FINAL, Non classifié, 29 juin 2004, p.9

44Idem

Un des aspects propre aux infractions qui se multiplient sur Internet est leur diversité. Certaines d'entre elles sont proches du canular mais d'autres affaires illustrent des dangers bien réels. On peut considérer, à la limite qu'Internet réunit pratiquement tous les ingrédients pour réaliser le crime parfait: anonymat, volatilité des preuves, absence de frontières et présence policière très limitée. C'est ce qu'illustrent les cas suivants.

Tout d'abord, l'extension du virus I love you, qui a débuté au 4 mai 2000 aux Philippines et s'est propagé à la vitesse de l'éclair de l'Asie à l'Europe en passant par les Etats-Unis. 65% des entreprises américaines de plus de 200 employés ont été infectées par le virus. Le courrier électronique de l'administration fédérale suisse a été paralysé pendant plus de 24 heures. Il est impossible de dresser la liste complète des dégâts et certains experts estiment le préjudice à plusieurs milliards de dollars.

Les dégâts occasionnés par ce virus , qui n'est qu'un parmi tant d'autres, ainsi que son mode de fonctionnement et surtout la quasi-immédiateté avec laquelle celui-ci s'est propagé mettent en exergue la dimension transnationale de la cybercriminalité.

Un autre domaine de prédilection de la cybercriminalité qui concerne la pédophilie fait valoir l'impuissance d'une approche nationale. Selon le responsable de la Division française pour la répression des atteintes aux personnes et aux biens (DNRAPB), le commissaire Jean-François Cossé, "350 à 500.000 clichés à caractère pédophile" circulent par messageries et sont consultables sur le Web ". La pédophilie est devenu "un délit de masse" estime pour sa part un représentant du BKA, la police fédérale allemande. En l'espace d'un an le nombre de sites pornographiques infantiles en langue allemande aurait augmenté de 100%. L'un d'entre eux a accueilli la visite de 500 000 internautes en très peu de temps. Le phénomène ne connaît pas de frontières et se développe de manière inquiétante dans les anciens pays de l'Est de l'Europe et en Russie.

Face au développement de la criminalité informatique, une nouvelle conscience des dangers et des enjeux liés à ces nouvelles formes de crimes et délits voit le jour. Lors de la conférence sur le crime international organisée en janvier 2001 par la police de Singapour et réunissant plus d'une centaine d'experts internationaux, l'ancien président d'Interpol, le canadien Norman Inkster y a dénoncé Internet comme étant « *l'espace de plus forte croissance du crime dans le monde.* »⁴⁵

Dans ce contexte, une réflexion s'est engagée à tous niveaux, national, européen et international, pour définir moyens à mettre en oeuvre pour renforcer l'action judiciaire et policière sur les réseaux. En France, le parlementaire Christian Paul, dans un rapport⁴⁶ adressé au premier ministre en 2000, observe que les lois restent essentiellement tributaires de cadres nationaux, rendant les pouvoirs de perquisition difficiles et longs à mettre en oeuvre.

Après l'énumération et la description du caractère transnational de la cybercriminalité, il convient d'analyser plus précisément les efforts entrepris au niveau international et européen.

45Dossier « Cybercriminalité » du Conseil de l'Europe accessible sur <http://www.coe.int>

46PAUL Christian, « Du droit et des libertés sur Internet », rapport remis au Premier ministre, le 19 juin 2000, Paris, la documentation française, 2000, p. 29 et s.

Chapitre 2: Les outils de la coopération judiciaire sur la scène internationale

Le développement de la criminalité sur Internet, comme on l'a souligné plus haut, bouleverse les règles classiques de compétence: les infractions peuvent être commises simultanément dans plusieurs pays, les investigations doivent souvent être effectuées à l'étranger. Tout ceci rend nécessaire la mise en place de services compétents pour améliorer le traitement des procédures lorsque les enquêtes doivent se poursuivre à l'étranger.

Dans une telle situation, beaucoup de pays pourraient considérer qu'une perquisition transfrontalière sur réseau, sans l'autorisation des autorités compétentes du pays concerné, violerait leur souveraineté. À ce titre la recommandation du 11 septembre 1995⁴⁷ du Conseil de l'Europe incitait déjà les États membre à renforcer la coopération internationale dans la mesure où les flux d'information parcourant les réseaux informatiques internationaux ne respectent pas les frontières nationales et le principe de territorialité, alors que les autorités chargées de l'enquête sont strictement liées par leur compétence nationale. Cette recommandation préconisait donc une coopération renforcée passant par l'échange de données et la possibilité d'organiser des enquêtes et des saisies transfrontalières.

Il convient d'évoquer ici le rôle de deux organisations actives dans la coopération internationale pour la lutte contre la cybercriminalité: Interpol et Europol.

Interpol

Une des organisations principales dans la lutte contre la cybercriminalité est certainement Interpol. Organisation Internationale de Police criminelle (OIPC) créée en 1929, Interpol vise à améliorer la coopération policière dans le monde grâce à des bureaux dans 178 pays membres (BCN). Ces bureaux sont des services de police permanents composés de policiers agissant dans le cadre de leur législation nationale. Ils constituent le relais national aux opérations de police sollicitées par les autres États membres. Le BCN-France, antenne d'Interpol, est rattaché à la Direction centrale de la Police Judiciaire au sein de la sous Direction des ressources et liaison dans la Division des relations internationales.

Le rôle d'Interpol est de faciliter pour ses membres la lutte contre le trafic de stupéfiants, le terrorisme, la criminalité informatique ou économique. Interpol dispose d'un système de communication informatique commun à tous les pays membres et d'une base de données criminelles internationales.

Interpol porte à la connaissance des services de police nationaux certains renseignements relatifs à des infractions, des délinquants et des victimes. À cet égard, il est procédé à l'établissement des notices signalétiques internationales individuelles relatives aux disparitions des personnes et notamment des mineurs et aux délinquants

⁴⁷Recommandation n° R (95) 12 du comité des ministres aux États membres sur la gestion de la justice pénale (adoptée par le comité des ministres le 11 septembre 1995, lors de la 543e réunion des délégués des ministres), accessible sur www.coe.int

susceptibles de récidiver. Les infractions collectées entrent directement en procédure.

Depuis juillet 1999, Interpol a développé un site Web à deux niveaux d'accès public et restreint, afin de donner une plus large diffusion aux notices avec l'autorisation BCN. Interpol réalise des opérations de police judiciaire d'envergure tels l'opération "Cathédrale" par exemple, lancée en 1998, qui a permis le démantèlement d'un réseau diffusant plus de 750 000 clichés de pornographie infantile et qui s'est traduite par l'arrestation de 107 personnes dans 12 pays. Il convient de souligner les efforts d'Interpol en vue de constituer une base de données d'images pédophiles, grâce au logiciel excalibur d'analyse et de comparaison automatique par le contenu (www.excalib.com).

Europol⁴⁸

L'office européen de police⁴⁹ – Europol – siégeant à La Haye au Pays-Bas, est un organe policier chargé du traitement des renseignements relatifs aux activités criminelles. Son objectif consiste à améliorer l'efficacité des services compétents des Etats membres et intensifier leur coopération dans le cadre de la prévention et la lutte contre les formes graves de criminalité internationale organisée⁵⁰.

Progressivement, le mandat d'Europol a été élargi. Europol est compétent dès lors que les infractions concernées impliquent une structure ou une organisation criminelle organisée et deux Etats membres ou plus. Initialement limitées au soutien des activités de répression dans les domaines du trafic de stupéfiants, de véhicules volés, de matières nucléaires et radioactives, les filières d'immigration, le faux monnayage et la falsification d'autres moyens de paiement, la traite des êtres humains - y compris la pornographie infantile -, le terrorisme et le blanchiment d'argent, les compétences d'Europol sont aujourd'hui étendues aux atteintes à la vie, à l'intégrité physique et à la liberté, aux atteintes au patrimoine, aux biens publics, au commerce illégal ainsi qu'aux atteintes à l'environnement.

Europol est donc compétent dans la lutte contre la criminalité informatique ainsi que pour l'ensemble des formes de criminalité utilisant Internet. Concrètement, Europol intervient :

- en facilitant l'échange d'informations, conformément aux dispositions nationales ;
- en fournissant des analyses opérationnelles pour les opérations menées par les Etats membres ;
- en fournissant des rapports de type stratégique et des analyses des activités criminelles réalisées à partir d'informations et de renseignements communiqués par les Etats membres, recueillis par Europol ou issus d'autres sources ;

48L'adresse du site officiel d'Europol est <http://www.europol.eu.int>

49La création d'Europol était prévue par le traité de Maastricht sur l'Union européenne, du 7 février 1992. Installé à La Haye, aux Pays-Bas, l'Office a démarré ses activités le 3 janvier 1994. Alors connu sous le nom de «Unité Drogues Europol» (EDU), il limitait son action à la lutte contre la drogue. Progressivement d'autres domaines importants de la criminalité sont venus élargir ses activités. Le mandat d'Europol a été étendu le 1er janvier 2002 à toutes les formes graves de la criminalité internationale visées à l'annexe de la convention Europol. La convention Europol a été ratifiée par tous les États membres et est entrée en vigueur le 1er octobre 1998. De nombreuses décisions d'ordre juridique en relation avec cette convention ont précédé le démarrage effectif de l'ensemble des activités de l'Office, le 1er juillet 1999.

50Les missions d'Europol sont décrites dans les articles 29 à 32 du Traité sur l'Union européenne adopté à Maastricht et révisé par les traités d'Amsterdam et de Nice.

- et en apportant son expertise et son assistance technique aux enquêtes et aux opérations menées au sein de l'Union européenne.

La liaison entre Europol et la France est assurée par l'unité nationale Europol. Elle est implantée au sein du ministère de l'intérieur à la direction centrale de la police judiciaire. De plus, la gendarmerie, la douane et l'INSEE participent à cette structure.

La convention Europol demande qu'Europol installe et gère un système informatisé permettant l'introduction, l'accès et le traitement des données qui comprend des systèmes d'informations, d'analyse et d'index. Ce système informatisé peut stocker et utiliser les données nécessaires à l'accomplissement des fonctions d'Europol. Les données introduites sont relatives aux personnes mises en cause pour avoir commis ou participé à une infraction relevant de la compétence d'Europol conformément à l'article 2 de la convention Europol.

Le système d'analyse intègre les fichiers de travail qui ont pour objet d'assister les services compétents des Etats membres dans la répression et la lutte contre les formes de criminalité comprises dans le mandat d'Europol. Les informations susceptibles d'être collectées proviennent de sources ouvertes accessibles aux analystes d'Europol, mais également d'informations transmises par les services d'enquêtes des Etats membres. Le système d'index indique à chaque officier de liaison des Etats membres que des données concernant son Etat membre d'origine ont été intégrées dans un fichier d'analyse clairement identifié.

Chapitre 3 : Le cadre juridique de la lutte contre la cybercriminalité : un cadre international plus qu'un cadre européen

Le caractère intergouvernemental de la lutte contre la cybercriminalité

La globalité de la révolution de l'information souligne les limites inhérentes à toute intervention unilatérale. La réaction naturelle des sujets de droit international, Etats comme institutions communautaires ou organisation internationale, consiste à recourir à la négociation de manière à ordonner ce qui apparaît comme un défi transnational à relever. Cette approche s'inspire de nombreux exemples de gestion de problèmes transnationaux par la négociation internationale, comme par exemple en matière de protection de l'environnement.

En revanche, cette approche ne remet pas en cause les principes même de la territorialité et de la souveraineté en droit international classique. En d'autres termes, si les Etats, premiers sujets du droit international, admettent l'existence de problématiques transnationales, ces derniers répugnent naturellement à remettre en cause l'exercice des responsabilités et compétences propres à l'exercice de leur souveraineté (c'est-à-dire la sécurité intérieure ou l'ordre public). En matière de coopération internationale comme en matière de régulation unilatérale, le territoire demeure donc le principal paradigme d'analyse d'Internet. Reste alors à déterminer les objectifs de la coopération internationale et les difficultés qu'elle rencontre dans un environnement électronique.

Les objectifs du recours à la coopération internationale en matière de réglementation d'Internet sont clairs : il s'agit de poser des principes communs à tous les États. Ces derniers demeurent libres de donner ou de refuser leur consentement à de telles tentatives et conservent ainsi le plein exercice de leur souveraineté. De plus, une collaboration importante en matière d'application de ces principes viendrait garantir l'effectivité des mesures adoptées. C'est également dans ce sens que c'est prononcé le député Martin-Lalande dans un rapport adressé au Premier Ministre en 1998⁵¹:

« 58. Inscrire la fraude informatique dans le troisième pilier européen afin de permettre au minimum une collaboration intergouvernementale sur ces problèmes ainsi qu'une coopération judiciaire et policière »

« 127. Développer la coopération judiciaire et policière au sein de l'Union européenne pour permettre d'avancer vers une solution internationale globale. »

Dans son rapport de 1998, le Conseil d'Etat souligne à son tour que la coopération internationale en matière de lutte contre la cybercriminalité est indispensable, même si elle n'en est pas moins une opération délicate et compliquée :

« [...] Les progrès sont fort lents et les réticences des États qui craignent une perte de souveraineté importantes; même entre pays démocratiques comparables comme ceux du Conseil de l'Europe, les différences de sensibilité restent fortes et donc la définition des infractions communes délicate; dès lors, seule la détermination politique des États à mener une action contre les « paradis virtuels » et la délinquance de la haute technologie peut les conduire à accepter l'abandon d'une partie de leur souveraineté afin de garantir l'efficacité de l'action répressive internationale. »⁵²

Les initiatives au sein de l'Union européenne

C'est tout d'abord au sein de l'Union européenne qu'il faut étudier les efforts de coopération internationale. Depuis l'Acte unique européen de 1987 qui a consacré la notion d'une Communauté européenne sans frontière, l'idée d'un espace judiciaire européen s'est imposée mais la coopération judiciaire civile et pénale est restée jusqu'au Traité de Maastricht de 1992 hors du cadre des compétences des institutions européennes. Le Traité sur L'Union européenne de Maastricht dans son Titre VI intègre dans le champs communautaire, la coopération judiciaire. Celle ci relève d'un ordre particulier, celui du troisième pilier (Titre VI du Traité sur L'Union européenne) avec des compétences, des modes de décisions et des priorités propres. En effet, la coopération judiciaire, question d'intérêt commun entre Etats membres, touche au cœur même des droits régaliens et les Etats membres n'ont pas souhaité intégrer ces domaines au pilier communautaire constitué par le traité sur la Communauté européenne.

51MARTIN-LALANDE Patrice, « Internet : un vrai défi pour la France », Rapport présenté au Premier Ministre, La Documentation française, Paris, 1998, Propositions 58 et 127

52 Rapport du Conseil d'État, « Internet et les réseaux numériques », rapport de la section des rapports et des études du Conseil d'État, Paris : la Documentation française, 1998, p.200

Le développement des compétences communautaires en matière de coopération judiciaire pénale a été jusqu'à présent particulièrement important et a aussi abordé la lutte contre la cybercriminalité.

Dès le 24 février 1997, le Conseil de l'Union européenne a adopté une action commune⁵³ relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants. Dans ce cadre, les Etats membres ont accepté de réformer leur législation afin d'ériger en infractions pénales certains comportements comme:

« l'exploitation sexuelle des enfants aux fins de la production de matériel pornographique, y compris la production, la vente et la distribution ou d'autres formes de trafic de matériel de ce type, et la détention de ce type de matériel »⁵⁴.

Dépourvue d'effet direct en droit interne, comme l'ensemble des initiatives européennes concernant la coopération pénale, cette action a néanmoins eu des conséquences dans l'ensemble des Etats Membres. En effet, résultat d'une négociation communautaire et d'un engagement politique, une action commune lie les Etats Membres quant au résultat à atteindre. La France a introduit dans son code pénal par la loi du 17 juin 1998, l'article 227-23 qui répond aux objectifs de l'action commune du Conseil.

En juin 1997, un programme d'action de lutte contre la criminalité organisée contenant trente recommandations destinées à promouvoir une coopération pratique et éventuellement un rapprochement de certaines législations nationales est adopté par le Conseil⁵⁵. Quelques mois plus tard, l'adoption du Traité d'Amsterdam précise l'étendu et les objectifs, notamment la lutte contre la criminalité, de la coopération judiciaire pénale qui demeure au sein du troisième pilier. Par la suite, un nouveau programme d'action de décembre 1998 propose différentes mesures pour renforcer la coopération judiciaire.

Le Conseil européen de Tampere des 15 et 16 octobre 1999 a reconnu spécifiquement une nouvelle fois la nécessité de rapprocher les législations nationales dans le domaine de la lutte contre la cybercriminalité. Les États membres reconnaissent alors la nécessité de parvenir à un accord sur les définitions et sur les sanctions applicables à certains actes criminels. La criminalité qui utilise les technologies avancées est un des actes compris dans cette liste⁵⁶.

53 Une « action commune » est l'appellation donnée par le Traité de Maastricht aux décisions-cadres définies dans le Traité d'Amsterdam dans l'article 34 du Traité sur l'Union européenne comme des mesures visant le rapprochement des dispositions législatives et réglementaires des Etats membres.

54 Action commune 97/154/JAI, du 24 février 1997, adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la lutte contre la traite d'êtres humains et l'exploitation sexuelle des enfants [publiée dans le Journal Officiel de l'Union Européenne (abrégé **JOUE** par la suite) L 63 du 04.03.1997].

• 55 Acte du Conseil du 18 décembre 1997 établissant, sur la base de l'article K.3 du traité sur l'Union européenne, la convention relative à l'assistance mutuelle et à la coopération entre les administrations douanières [JOUE C 024 du 23/01/1998]

56 Point 48 des conclusions du Conseil européen de Tampere

C'est ce que souligne le Commissaire européen responsable de la justice et des affaires intérieures, M. Antonio Vitorino:

«Le droit pénal des États membres comporte des vides juridiques importants susceptibles d'entraver la capacité des services de police et des autorités judiciaires à lutter contre la criminalité visant les systèmes d'information. Compte tenu de la nature transnationale du piratage, des virus et des attaques par déni de service, il importe que l'Union européenne prenne des mesures dans ce domaine afin de garantir l'efficacité de la coopération des services de police et des autorités judiciaires. La nécessité de rapprocher les dispositions relatives aux délits et aux peines dans ce domaine avait été reconnue par le Conseil de Tampere en octobre 1999»⁵⁷

L'impulsion décisive est donnée en mars 2000 au Conseil européen de Lisbonne qui lance la stratégie de Lisbonne. Celle-ci indique l'importance stratégique de la société de l'information dans le développement d'une économie compétitive fondée sur la connaissance. C'est à la suite de cette initiative politique que la Commission présente le plan d'action global « e-Europe » qui vise à développer les possibilités offertes par les nouvelles technologies et notamment, améliorer la sécurité des réseaux informatiques et est abordé dans le titre second de ce mémoire.

À la suite du Sommet de Lisbonne, une proposition de décision-cadre⁵⁸ concernant les attaques visant les systèmes d'information est lancée le 23 avril 2002⁵⁹. La décision-cadre⁶⁰ relative aux attaques visant les systèmes d'information se consacre tout particulièrement aux principaux types d'infractions pénales apparus dans le domaine des systèmes d'information, tels que le piratage, l'exécution de logiciels malveillants et les attaques par déni de service.

Elle vise à rapprocher les droits pénaux des pays de l'Union européenne pour faire en sorte que les services de police et les autorités judiciaires aient les moyens d'agir contre cette nouvelle forme de criminalité et de cibler les comportements graves. Cette décision apporte une définition communautaire des infractions contre les systèmes d'information en prévoyant des « règles minimales relatives aux éléments constitutifs des infractions ». La décision-cadre institue des délits communs d'accès illicite à un système d'information et d'interférence illicite avec celui-ci. Des circonstances aggravantes sont même prévues afin de lutter contre le terrorisme et le crime organisé.

57Communiqué de presse de la Commission européenne, Bruxelles, le 23 avril 2002, réf. IP/02/601

58Une décision-cadre est un instrument utilisée pour rapprocher les dispositions législatives et réglementaires des Etats membres (définie dans l'article 34 du Traité sur l'Union européenne). Proposée à l'unanimité à l'initiative de la Commission ou d'un Etat membre, elle doit être adoptée à l'unanimité. Elle n'a pas d'effet direct sur le droit interne des Etats membres et lie les Etats membres quant au résultat à atteindre.

59Proposition de décision-cadre du Conseil relative aux attaques visant les systèmes d'information [COM(2002) 173 final - JOUE C 203 E du 27.08.2002]

60Pour l'instant le processus législatif concernant la décision cadre n'en est qu'à l'accord politique du Conseil, le Parlement ayant donné son avis en première lecture. La dernière version sur laquelle s'est accordée le conseil est disponible sur le site du Conseil à l'adresse suivante : <http://register.consilium.eu.int/pdf/fr/03/st08/st08687-re01fr03.pdf>

Les deux infractions suivantes sont définies par la décision cadre :

1.- l'accès illicite à des systèmes d'information : le fait d'accéder, intentionnellement et sans en avoir le droit à « *toute partie d'un système d'information faisant l'objet de mesures de protection particulières, ou avec l'intention de porter préjudice à une personne physique ou morale, ou avec celle d'obtenir un avantage économique* » (art. 3).

2.- l'interférence illicite avec des systèmes d'information : le fait de « *perturber gravement ou d'interrompre le fonctionnement d'un tel système en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données informatiques* » ou le fait « *d'effacer, de détériorer, d'altérer, de supprimer ou de rendre inaccessibles des données informatiques lorsque l'acte est commis avec l'intention de porter préjudice à une personne physique ou morale.* » (art. 4).

Cette décision-cadre témoigne d'une prise de conscience de la part des Etats membres de l'Union européenne de la nécessité de la définition d'un cadre juridique au niveau européen pour traiter du problème de la cybercriminalité. Il convient néanmoins de souligner les insuffisances des initiatives européennes en la matière liées à la complexité du mode de décision (unanimité; rôle du Parlement européen réduit), propre à la coopération judiciaire pénale. Aussi, les compétences européennes se limitent à la facilitation de la coopération et de la coordination des actions des Etats qui restent souverains en la matière.

Le Conseil de l'Europe, lieu de création d'un cadre juridique de lutte contre la cybercriminalité

Il convient de noter que les premiers actes en matière de coopération judiciaire pénale ont été élaborés dans le cadre du Conseil de l'Europe dès 1957 (conventions sur l'extradition). En 1997, le Conseil de l'Europe développe un instrument international contraignant qui s'efforce d'appréhender la problématique des réseaux dans leur dimension globale. La convention a vocation universelle et est ouverte à la signature d'Etats non européen. Les 44 pays membres⁶¹ du Conseil de l'Europe (dont les 25 Etats membres de l'Union européenne) ont participé à l'élaboration de ce texte ainsi que le Canada, les Etats-Unis, le Japon - observateurs auprès de l'organisation - et l'Afrique du Sud. Ces derniers peuvent donc adhérer à la Convention qui étend ainsi son champ d'application à la plus grande partie du trafic informatique mondial. En outre, le texte ne se limite pas au traitement de la cybercriminalité *stricto sensu*. Il s'applique aussi à toute infraction pénale quelle que soit sa nature, dès lors qu'il est nécessaire de recueillir une preuve électronique. Les domaines dans lesquels la convention pourrait être mise en œuvre sont par conséquent très nombreux.

61 Ces pays sont: Albanie, Allemagne, Andorre, Arménie, Autriche, Azerbaïdjan, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Géorgie, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, "L'ex-République yougoslave de Macédoine", Liechtenstein, Lituanie, Luxembourg, Malte, Moldovie, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Russie, Saint-Marin, Slovaquie, Slovénie, Suède, Suisse, Turquie et l'Ukraine.

La Convention sur la lutte contre la cybercriminalité a été signée le 23 novembre 2001 et est entrée en vigueur le 18 mars 2004 date à laquelle la Lituanie a ratifié la Convention⁶². La Convention constitue un instrument novateur qui tente d'apporter des réponses concrètes aux problèmes soulevés par le monde des réseaux, soit en adaptant les principes juridiques classiques de l'entraide judiciaire lorsque ceux-ci paraissent incapables de s'appliquer de manière efficiente au nouveau contexte des réseaux, soit en retenant des solutions qui s'inspirent des travaux menés dans d'autres enceintes, notamment le G 8⁶³.

Le Conseil de l'Europe a donc créé, au début de l'année 1997, un Comité d'experts sur la criminalité dans le cyber espace chargé d'élaborer un projet de convention internationale sur:

- les nouvelles formes d'infractions commises dans le cyber espace;
- les aménagements des législations nationales susceptibles de faciliter la coopération internationale;
- les adaptations nécessaires des instruments procéduraux d'investigation (perquisition des systèmes informatiques, valeur probante des preuves électroniques...);
- les conflits de compétence entre juridictions;
- les questions de coopération internationale en matière d'enquêtes informatiques.

L'objectif fixé est l'élaboration d'un instrument spécifique contraignant. Pour répondre à cet objectif, l'assemblée parlementaire du Conseil de l'Europe a donné son accord pour que le projet de Convention sur la cybercriminalité soit ratifié par les ministres des 43 Etats membres du Conseil de l'Europe. Les Etats-Unis, le Japon et le Canada, non-membres du Conseil de l'Europe qui ont participé à la rédaction de ce texte ont la possibilité de le ratifier. En effet, toute la portée de ce texte réside dans le fait qu'il peut avoir des effets au-delà des frontières de l'Europe et qu'il constitue un équilibre entre la volonté de favoriser le développement des technologies de l'information et de réprimer les comportements frauduleux qui y sont liés.

La Convention prévoit une harmonisation des législations nationales en déterminant des incriminations pénales spécifiques pour les comportements délictueux liés aux technologies de l'information et favorise la coopération policière et judiciaire en opérant un rapprochement des procédures pénales nationales. Les infractions visées ont pour objet tout particulièrement de réprimer les comportements portant atteinte à la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques. Afin de réprimer ces infractions, la Convention prévoit des procédures adaptées. À ce titre, elle impose notamment aux Etats d'habiliter leurs autorités compétentes à perquisitionner les systèmes informatiques, saisir les données qui y sont stockées et procéder à des injonctions de produire de telles données.

⁶²Or la Lituanie est le cinquième Etat à l'avoir ratifié et l'article 36 de la Convention stipule que celle-ci entre en vigueur trois mois après la ratification par cinq Etats signataires dont au moins trois membres du Conseil de l'Europe.

⁶³En décembre 1997, les Etats du G7-P8 au sommet de Washington adoptent dix principes et un plan d'action pour lutter contre la cybercriminalité. Dans ce cadre deux grandes conférences ont été organisées réunissant les membres du G8, l'une à Paris en mai 2000 et l'autre à Okinawa en juillet 2000. De même la cybercriminalité est au coeur de la réunion de février 2001 à Milan des ministres de la Justice et de l'intérieur du G8. C'est grâce à ces rencontres que des pays non-membres du Conseil de l'Europe, tel que le Japon, la Canada et les Etats Unis sont signataires de la Convention pour la lutte contre la cybercriminalité.

La convention vise, tout d'abord, à harmoniser les législations nationales en ce qui concerne les incriminations dans le domaine du cyber-espace. Dans cette perspective, elle fournit une énumération des comportements pour lesquels chaque Etat s'oblige à instaurer des sanctions pénales dans son droit interne. Elle tend également à compléter l'arsenal juridique des Etats en matière de procédure pénale, afin d'améliorer la capacité des services de police à mener en temps réel leurs investigations et à collecter des preuves sur le territoire national avant qu'elles ne disparaissent.

Enfin, la convention s'efforce d'adapter les règles classiques des conventions du Conseil de l'Europe en matière d'extradition et d'entraide répressive de 1957 et 1959. L'entraide judiciaire internationale se trouvera facilitée par l'adoption entre les Etats signataires de normes pénales minimales en matière d'incriminations et de règles de procédure pénale communes. Les autorités judiciaires peuvent ainsi répondre aux nouveaux enjeux posés par ces réseaux.

Un protocole additionnel à la convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques d'accord, a été négocié à la demande de la France. Il améliore la lutte contre les actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, en harmonisant le droit pénal pour la répression des comportements tels que la diffusion de matériel raciste et xénophobe ou les insultes et menaces motivées par des considérations racistes et xénophobes. En outre, il facilite l'extradition et l'entraide judiciaire pour la répression de ces agissements. Ce protocole permet de lutter de façon plus complète contre l'expression publique de propos ou de thèses négationnistes ou révisionnistes, ainsi que l'approbation ou la justification publique des faits de génocide ou de crime contre l'humanité

Les grandes lignes de la Convention

La Convention détermine trois principaux axes de réglementation : l'harmonisation des législations nationales concernant la définition des crimes, la définition des moyens d'enquêtes et de poursuites pénales adaptés à la mondialisation des réseaux et la mise en place d'un système rapide et efficace de coopération internationale.

a. Les infractions répertoriées

Les infractions retenues sont toutes soumises à deux conditions: les comportements incriminés doivent toujours être commis de façon intentionnelle et "sans droit" pour que la responsabilité pénale soit engagée. Elles sont répertoriées en quatre grandes catégories:

- les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes : accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs;
- les infractions informatiques : falsification et fraude informatiques;
- les infractions se rapportant au contenu : actes de production, diffusion, possession de pornographie infantile avec un protocole additionnel sur la propagation d'idées racistes et la xénophobie à travers les réseaux;
- les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

: la distribution à grande échelle de copies illégales d'oeuvres protégées etc.

b. De nouvelles procédures

La convention prévoit des règles de base qui faciliteront la conduite d'enquêtes dans le monde virtuel et qui représentent de nouvelles formes d'entraide judiciaire. Ainsi sont prévues : la conservation des données stockées la conservation et divulgation rapide des données relatives au trafic, la perquisition des systèmes et la saisie de données informatiques ainsi que la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu.

Ces dispositions sont soumises aux conditions légales des pays signataires qui doivent garantir le respect des Droits de l'homme et l'application du principe de proportionnalité. En particulier, les procédures ne pourront être engagées que sous certaines conditions, tel que, selon le cas, l'autorisation préalable d'un magistrat ou d'une autre autorité indépendante.

c. Les règles de la coopération internationale

À côté des formes traditionnelles de coopération pénale internationale prévues notamment par les conventions européennes d'extradition et d'entraide judiciaire en matière pénale, la nouvelle Convention exige des formes d'entraide correspondant aux pouvoirs définis préalablement par la Convention et, en conséquence, que les autorités judiciaires et services de police d'un Etat puissent agir pour le compte d'un autre pays dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes ni de perquisitions transfrontalières. Les informations obtenues devront être rapidement communiquées. Un réseau de contacts disponibles 24 heures sur 24 et sept jours sur sept est mis sur pied afin de prêter une assistance immédiate aux investigations en cours.

d. La juridiction

Chaque pays doit établir sa compétence lorsque l'infraction est commise sur son territoire, à bord d'un bateau ou d'un avion immatriculé chez lui ou lorsque l'un de ses ressortissants en est l'auteur si l'infraction ne relève de la compétence territoriale d'aucun autre Etat.

La Décision-cadre du Conseil des Ministres de l'Union européenne relative aux attaques visant les systèmes d'information, présentée auparavant, reprend dans une large mesure le contenu, mais aussi la structure de la Convention sur la cybercriminalité du Conseil de l'Europe. Rien d'étonnant à ce fait. Des différences importantes n'auraient de toute façon pas été possibles puisque tous les Etats membres de l'Union européenne ont signé la Convention sur la cybercriminalité.

L'utilité de la décision-cadre est de transcrire une grande partie des principes et des définitions de la Convention du Conseil de l'Europe en droit européen. Il est certain que cette utilité est réduite, dans la pratique. Ceci s'explique sans doute davantage par les caractéristiques spécifiques de la criminalité sur Internet – et notamment sa dimension éminemment internationale – ainsi que par les difficultés inhérentes au processus décisionnel du troisième pilier requérant l'unanimité qui font du Conseil de l'Europe un lieu plus adéquat pour traiter de cybercriminalité.

Ainsi l'action du Conseil de l'Europe doit être louée puisque le principal texte juridique qui encadre la coopération et la coordination internationale dans ce domaine reste sa Convention sur la cybercriminalité.

Néanmoins, si la lutte contre la fraude informatique et la cybercriminalité reste en grande partie de la compétence des Etats, d'autres aspects de la sécurité des réseaux et des systèmes d'informations sont désormais au coeur de l'action réglementaire des institutions communautaires et participent de l'émergence d'une sécurité proprement européenne des réseaux et des systèmes d'information.

TITRE SECOND

L'EMERGENCE D'UN CADRE JURIDIQUE EUROPEEN DE LA SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION

Législation communautaire et co-régulation dans le domaine de la sécurité des réseaux et des systèmes d'information

L'action des institutions communautaires dans le domaine de la sécurité des réseaux et des systèmes d'information est double. L'objectif de cette seconde partie est de mettre en lumière les deux modes d'action privilégiés par lesquels l'Union européenne agit sur la réglementation propre à assurer la sécurité des systèmes d'information.

Le premier moyen est l'harmonisation des règles juridiques des États membres. Ce moyen d'action classique des institutions communautaires est dans le domaine de la sécurité des réseaux illustré par la mise en place d'un cadre juridique de la protection des données. En effet, la garantie de la sécurité des réseaux et des systèmes d'information est conditionnée par l'assurance que les données transportées et traitées par ces systèmes sont fiables et intègres. De plus, la préservation des valeurs fondamentales sur lesquelles se sont accordées les États membres de l'Union européenne exige un cadre juridique strict protégeant la vie privée des internautes. (Section 1)

Si l'harmonisation réglementaire est un des moyens les plus puissants dont usent les institutions européennes pour mettre en place un cadre juridique homogène, il n'est pas leur unique mode d'action. En effet, celles-ci tendent à développer un autre mode d'encadrement complémentaire et plus adéquat, compte tenu des caractéristiques de l'Internet et de l'informatique, en constante évolution technologique, la co-régulation. Il s'agit de promouvoir et d'encadrer un partenariat entre secteur privé et public pour la mise en oeuvre de la sécurité européenne des réseaux et des systèmes d'information. Ce mode d'action repose sur la promotion de l'auto-régulation et la mise en place de programmes de recherche et de sensibilisation mettant en oeuvre les principes sur lesquels se fondent la sécurité européenne des réseaux et des systèmes d'information.

L'établissement d'une agence européenne chargée de la sécurité des réseaux et de l'information illustre cette nouvelle forme de la régulation européenne qui coordonne les politiques nationales et encadrent les initiatives privées. (Section 2).

Section 1 : La politique européenne de protection des données

Chapitre 1: Enjeux et objectifs de la politique européenne de promotion de la société de l'information

Les fondements juridiques de l'harmonisation communautaire

Le premier objectif de la l'intervention européenne dns le domaine de la société de l'information est l'établissement d'un marché unique. L'intervention européenne trouve sa justification essentiellement dans la mesure où le maintien de régimes juridiques nationaux⁶⁴ différents risque de créer des barrières aux flux intra-européens ou conduisent à des distorsions réglementaires propices à l'établissement d'un service de la société de l'information dans un État plutôt que dans un autre. La libre circulation des services et la liberté d'établissement sont donc les deux fondements sur lesquels s'appuient les institutions européennes pour justifier leur intervention réglementaire. C'est donc par l'intermédiaire de l'harmonisation des réglementations nationales que les entraves à l'établissement du marché unique sont abordées. L'harmonisation peut prendre plusieurs formes. Elle peut s'opérer par le biais détourné des mécanismes de reconnaissance mutuelle qui conduisent nécessairement à un certain degré d'harmonisation⁶⁵. L'harmonisation peut être minimale – dans ce cas ce ne sont que les aspects essentiels d'une réglementation qui sont harmonisées ce qui autorise des mesures nationales plus sévères – optionnelle – le choix de certaines dispositions étant laissé aux Etats membres – ou bien totale ou maximale – lorsque l'ensemble des aspects d'une réglementation est harmonisé au niveau communautaire.

Les bases juridiques de l'action communautaire dans le domaine de la société de l'information repose sur les principaux éléments suivants :

- la politique des télécommunications dont la base juridique réside dans l'article 95 (harmonisation du marché intérieur), les articles 81 et 82 (concurrence) ainsi que les articles 47 et 55 (droit d'établissement et services) du traité sur la Communauté européenne (TCE) ;
- le soutien au développement en matière de technologies de l'information et des communications, sur la base des articles 163 à 172 (recherche et développement) du TCE ;
- la création des conditions nécessaires à la compétitivité de l'industrie (des télécommunications) de la Communauté, conformément à l'article 157 du TCE ;
- la promotion des réseaux transeuropéens dans les secteurs des transports, de l'énergie et des télécommunications, comme prévu aux articles 154, 155 et 156 du TCE.

64BLANDIN-OBERNESSER, Annie, L'Union européenne et Internet, Travaux de la Commission pour l'étude des Communautés européennes (CEDECE). Rennes : Editions Apogée, Publication du Pôle Universitaire Jean Monnet de l'Université de Rennes I, 2001

65 Le principe de la reconnaissance mutuelle oblige les autorités publiques d'un Etat membre à reconnaître la conformité d'un produit ou d'un service à leur réglementation nationale dès que ce produit ou service est délivré en conformité avec la réglementation nationale d'un autre Etat membre.

Ainsi au regard, de l'énoncé des domaines de compétences des institutions européennes, l'intervention réglementaire européenne dans le domaine de la sécurité des réseaux et de la protection des données est justifiée juridiquement. De plus, qui dit protection des données dit aussi protection de la vie privée qui est l'un des droits fondamentaux inscrit au rang des valeurs essentielles de l'Union européenne. L'intervention européenne visant à protéger les libertés fondamentales a été consolidé depuis l'adoption de la Charte européenne des libertés individuelles⁶⁶.

Les objectifs: l'établissement de la confiance et la promotion des nouvelles technologies

La justification de l'action européenne dans le domaine des nouvelles technologies de l'information réside dans le rôle qu'elles jouent dans la croissance économique. En effet, très vite le développement des technologies de l'information est apparu comme l'un des moteurs fondamentaux du développement de l'économie de demain. C'est pourquoi, les institutions européennes se sont penchées avec intérêt sur les moyens de développer un cadre favorable à leur épanouissement.

Or le développement d'Internet passe nécessairement par la mise en place d'un réseau d'infrastructures plus sûre et par une connexion du maximum d'européens à la toile. La nécessité d'adapter le cadre juridique à l'émergence des nouvelles technologies de l'information concerne donc essentiellement la législation relative aux télécommunications. La réponse essentielle qu'apporte l'Europe à la mise en place d'une société de l'information se concentre sur la libéralisation du secteur des télécommunications. Bien qu'Internet ne soit pas la raison essentielle de cette libéralisation, qui procède en fait de la philosophie générale du marché commun, les nouvelles technologies de l'information (câble, téléphonie, et l'ensemble des moyens de communication) prennent part à l'accélération de ce processus.

L'ouverture du marché des télécommunications à la concurrence a eu l'effet d'un catalyseur sur un marché autrefois réservé aux oligopoles. Afin d'accompagner cette évolution, les instances décisionnelles européennes ont adopté une législation en phase avec les progrès technologiques et les exigences du marché. Cette évolution s'est traduit par l'adoption d'un nouveau cadre réglementaire relatif aux communications électroniques dont l'objectif principal est de renforcer la concurrence en facilitant l'arrivée des nouveaux entrants et de stimuler les investissements dans le secteur.

Mais le développement d'infrastructures propres à favoriser l'expansion d'Internet et son utilisation est certes fondamental mais inutile si ne s'y adjoignent pas des mesures concrètes propres à donner une réelle confiance aux futurs utilisateurs des services virtuels censés être à l'origine de la croissance économique. La garantie de la sécurité des transactions et des données qu'elles contiennent, qui conditionne la confiance des

⁶⁶Charte des droits fondamentaux de l'Union européenne, approuvée au Conseil européen de Nice en décembre 2000 et intégrée dans la deuxième partie du projet de Constitution européenne adopté par les Chefs d'États et de gouvernement au printemps 2004.

utilisateurs, est le terreau sans lequel les fruits escomptés du développement des nouvelles technologies ne sauraient mûrir.

C'est bien dans ce sens que le législateur français a choisi de baptiser la loi encadrant le développement de l'économie numérique "loi pour la confiance dans l'économie numérique". Cet enjeu de la confiance n'est en aucun cas trivial et constitue le revers indissociable des intentions économiques des institutions européennes. Le terme de confiance n'est pas neutre puisqu'il renvoie à la fois à la notion d'assurance et de croyance dans le développement futur des nouvelles technologies mais aussi à celui de sécurité. La nécessité de développer un cadre sûr et transparent va de soit avec le développement croissant des applications économiques d'Internet. Les investissements et les échanges nécessitent un cadre cohérent qui puisse garantir le respect de règles fondamentales de confidentialité et de sécurité. La Commission en est bien consciente lorsqu'elle énonce qu'il est :

« Indispensable que soit mis en oeuvre un environnement juridique qui, d'une part, incite l'investissement, et d'autre part, garantisse qu'ils serviront pour le mieux l'intérêt général »⁶⁷

Ainsi la mise en place d'un cadre juridique capable de renforcer la sécurité des systèmes d'information est elle au cœur de la double mission de l'Union européenne: promouvoir le développement d'un marché unique dans le domaine des nouvelles technologies et assurer la confiance des usagers et la sécurité de ces technologies.

La protection des données et sécurité dans la société de l'information

Un des aspects fondamentaux de la sécurité des systèmes d'information concerne les données qui circulent sur ces réseaux. En effet, un système d'information a comme fonction de faire circuler de l'information, c'est-à-dire de la traduire en données qui font l'objet d'un transport avant d'être communiquées à leur destinataire. La protection de ces données est un élément essentiel du développement de la société de l'information et à ce titre a été considéré comme l'un des tous premiers objectifs des autorités publiques qui ont la charge de veiller à la mise en place d'une société de l'information sûre.

Dès 1978, par exemple, cette exigence de sécurité est inscrite dans la loi française, notamment dans l'article 29 de la Loi informatique et libertés qui indique que :

« Toute personne ordonnant ou effectuant un traitement informatique nominatif d'information s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. »⁶⁸

Le non respect de ces précautions est d'ailleurs sanctionné par l'article 226-17 du Code pénal qui stipule que :

« Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles (...) est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

⁶⁷COMMISSION EUROPEENNE, « Croissance, compétitivité, emploi - Les défis et les pistes pour entrer dans le XXI ème siècle », Livre blanc de la Commission européenne, OPOCE, supplément 6/93 (1993), p. 183

⁶⁸Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel (abrégé JO par la suite) du 7 janvier 1978 et rectificatif au *J.O.* du 25 janvier 1978

De la même façon, l'OCDE inscrit la sécurité des données comme indispensable au respect de la démocratie; le 5ème principe qu'elle érige dans ses lignes directrices régissant la sécurité des systèmes et réseaux d'information⁶⁹:

« La sécurité doit être assurée dans le respect des valeurs reconnues par les sociétés démocratiques, et notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations à caractère personnel, l'ouverture et la transparence ».

De la même façon, la Commission européenne, dans sa communication au Conseil du 6 juin 2001, fait de la garantie de l'intégrité comprise comme la « *confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et non pas été modifiées* »⁷⁰ et la confidentialité des données entendue comme « *comprenant la protection des communications ou des données stockées contre l'interception et la lecture par des personnes non autorisées* »⁷¹ deux des exigences génériques de la politique de la sécurité des réseaux. Aussi la protection des données est-elle apparue comme un domaine prioritaire de l'action législative européenne destinée à sécuriser Internet et à garantir certaines valeurs fondamentales telle que le respect de la vie privé afin d'en accroître son attractivité⁷².

Le plan d'action e-Europe et le paquet télécom

Le livre blanc de la Commission "Croissance, compétitivité et emploi" publié en 1993 soulignait déjà l'importance de la société de l'information comme clé de la croissance économique, la compétitivité, la création d'emplois et l'amélioration de la qualité de vie des Européens. Dans le prolongement du livre blanc, le Commissaire Bangemann établit un rapport intitulé "l'Europe et la société de l'information planétaire"⁷³, destiné à formuler des recommandations quant à la façon dont l'Union pourrait contribuer à instaurer un cadre réglementaire, technologique et social favorable à la société de l'information. Ce rapport conduisit à l'adoption, le 19 juin 1994 lors du Conseil européen d'Essen, du premier plan d'action de l'Union européenne en la matière, "Vers la société de l'information en Europe". Ce plan d'action visait essentiellement à accélérer la libéralisation des services et infrastructures de télécommunications qui eut lieu en 1998, à développer et réorienter les programmes de recherche dans le domaine des technologies de l'information et de la communication, et à intégrer la promotion de la société de l'information dans l'ensemble des politiques communautaires.

69OCDE, « Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité », Recommandation du Conseil de l'OCDE, 1037ème session, 25 juillet 2002, p. 21

70Communication au conseil du 6 juin 2001: « Sécurité des réseaux et de l'information : Proposition pour une approche politique européenne », COM (2001), 0298, p. 5

71Idem

72POULLET, Yves « Vers la confiance : Vues de Bruxelles: un droit européen de l'internet ? », dans CHATILLON, Georges - Le droit international de l'Internet : actes du colloque organisé à Paris les 19 et 20 novembre 2001. Bruxelles : Bruylant, 2002, cop. 2003 - 693 p.

73Rapport du groupe de hautes personnalités sur "l'Europe et la société de l'information planétaire" - Recommandations du Conseil européen – Bulletin de l'Union européenne, Secrétariat général, Bull. 6-1994, point 1.2.9 et Supplément 2/94

En 1999, la politique de l'Union européenne en matière de société de l'information prend un nouvel élan. Dans un contexte de forte croissance économique du e-commerce et des services liés à la société de l'information et à Internet, il paraît nécessaire de coordonner davantage les politiques des États membres dans ce domaine. Une première communication est adoptée par la Commission en décembre 1999 et reçoit le soutien du Conseil européen de Lisbonne de mars 2000, qui fixe comme nouvel objectif stratégique de l'Union pour la prochaine décennie de "devenir l'économie de la connaissance la plus compétitive et la plus dynamique du monde". Pour y parvenir, le Conseil européen demande à la Commission d'élaborer un plan d'action e-Europe qui est adopté en juin 2000 au sommet de Feira. Le plan d'action « e-Europe 2002 – une société de l'information pour tous »⁷⁴ définit une série d'objectifs-clés que les États membres doivent atteindre d'ici à la fin 2002.

En juin 2002, le Conseil européen de Séville approuve le nouveau plan d'action e-Europe 2005⁷⁵ qui succède à e-Europe 2002. L'un de ces principaux objectifs est de faire en sorte que la société de l'information soit profitable à tous à travers l'Union européenne de façon cohérente et équitable. À cet effet, il a été instauré un cadre juridique clarifié couvrant la mise au point, l'acceptation et la diffusion de nouvelles technologies et applications. Ce cadre vise à promouvoir l'accès à Internet et le commerce électronique, et définit aussi des normes techniques communes pour les télécommunications mobiles (GSM, UMTS), la télévision numérique (DVD) et la radio. Il comporte également des dispositions en matière d'analyse comparative afin de garantir la cohérence du financement des applications, de la réglementation et de l'acceptation des technologies dans tous les pays.

Simultanément au lancement du plan e-Europe 2005 est adopté un nouvel ensemble de propositions législatives proposé par la Commission en 2000, le "paquet télécom". Celui-ci complète l'achèvement du marché intérieur et la libéralisation des services et infrastructures de télécommunications mis en place depuis le 1er janvier 1998. Le "paquet télécom" vise à adapter le cadre existant à la convergence entre télécommunications, informatique et médias provoquée par Internet, et à lui conférer une plus grande souplesse afin de pouvoir réagir à l'évolution rapide du marché et des techniques. Le paquet telecom se compose des cinq directives d'harmonisation suivantes adoptées en 2002 : une directive cadre relative au cadre réglementaire commun⁷⁶ et les directives "accès et interconnexion"⁷⁷, "autorisation"⁷⁸, "service

74 « eEurope 2002 - une société de l'information pour tous » : projet de plan d'action préparé par la Commission européenne en vue du Conseil européen de Feira, 19-20 juin 2000, COM (2000) 330 final

75 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions : eEurope 2005 : une société de l'information pour tous : plan d'action à présenter en vue du Conseil européen de Séville des 21 et 22 juin 2002, Com (2002) 263 final

76 Directive 2002/21/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques [JOUE L 108 du 24.04.2002].

77 Directive 2002/19/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion [JOUE L 108 du 24.04.2002].

78 Directive 2002/20/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à l'autorisation de réseaux et de services de communications électroniques [JOUE L 108 du 24.04.2002]

universel et droits des utilisateurs"⁷⁹ et "protection de la vie privée"⁸⁰. À cela s'ajoutent la décision de 2002 relative à la "politique en matière de spectre radioélectrique"⁸¹ ainsi que le règlement⁸², adopté en décembre 2000 relatif au "dégrouper de l'accès à la boucle locale".

Il convient de relever le fait que la question de la protection des données et de la vie privée est intégrée dans le « paquet télécom ». Ce faisant, l'Union européenne indique clairement qu'elle considère la réglementation de la protection des données comme une nécessité pour le bon fonctionnement du réseaux.

Chapitre 2: Le cadre juridique européen de la protection des données : l'affirmation d'une approche européenne de la sécurité

La promotion de la confiance dans les nouvelles technologies, en particulier Internet nécessite d'assurer un niveau élevé de sécurité et de protection de la vie privée. C'est pourquoi l'Union européenne a adopté un cadre très strict destiné à protéger les données transitant sur le réseau et donc à assurer la sécurité des utilisateurs par l'adoption de la directive 95/46/CE⁸³ et la directive 2002/58/CE⁸⁴.

La directive 95/46/CE sur la protection des données

Contexte et objectif

La première directive sur la protection des données à caractère personnel date de 1995. Son objectif est d'harmoniser les législations nationales relatives au traitement de données à caractère personnel et de protéger, en la matière, les droits et les libertés des personnes concernées, en particulier le droit à la vie privée. Le Parlement européen et le Conseil estiment que si la circulation et le transfert des données à caractère personnel d'un État membre vers un autre doit être possible, les droits fondamentaux des personnes doivent être protégés. *

79 Directive 2002/22/CE du Parlement européen et du Conseil, du 7 mars 2002, concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques [JOUE L 108 du 24.04.2002]

80 Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [JOUE L 201 du 31.07. 2002]

81 Décision 676/2002/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à un cadre réglementaire pour la politique en matière de spectre radioélectrique dans la Communauté européenne [JOUE L 108 du 24/04.2002]

82 Règlement (CE) n° 2887/2000 du Parlement européen et du Conseil du 18 décembre 2000 relatif au dégroupage de l'accès à la boucle locale [JOUE n° L 336 du 30.12.2000]

83 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, (directive " protection des données") [JOUE n° L. 281 du 23.11.1995]

84 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques"), [JOUE n° L. 201 du 31.07.2002]

Dans le courant des années 1990, les institutions nationales et internationales accordent de plus en plus d'attention à cette problématique, car les acteurs économiques et sociaux recourent toujours plus au traitement de données à caractère personnel. À la même époque, l'influence possible de l'utilisation des nouvelles technologies sur la vie privée du citoyen commence à prendre des contours clairs, car l'arrivée d'applications informatiques de plus en plus puissantes simplifie le traitement et la conservation de grandes quantités de données personnelles et permet aussi d'établir des liens entre ces données à une plus grande échelle.

Dans l'Union européenne, la question de l'échange et de la libre circulation de données à caractère personnel par des entreprises dans le cadre du marché unique amène les États membres à envisager une harmonisation des législations nationales. La grande diversité des approches nationales suscite une insécurité juridique qui ne profite ni aux entreprises européennes ni aux citoyens européens qui ignorent précisément les garanties dont ils peuvent disposer à l'égard de leurs données à caractère personnel.

La directive procède d'un ensemble de règles assez complexes et comporte, outre un certain nombre de grands principes, une liste d'exceptions à ces principes. Elle s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Le traitement de données effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques est exclu. Il en est de même pour les traitements mis en oeuvre pour la sécurité publique, la défense ou la sûreté de l'État⁸⁵, éléments essentiels à la souveraineté des États.

Définition

Les deux termes de "traitement" et "données à caractère personnel" sont les concepts clés de la directive 1995/46/CE.

Traitement

L'article 2b de la directive stipule qu'il faut entendre par traitement de données à caractère personnel :

« toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

Les trois principaux éléments de la définition sont donc la présence de données à

⁸⁵Ce qui a permis le renforcement des moyens mis à la disposition de la police judiciaire en France par exemple, comme on l'a vu plus haut dans la description des évolutions de la Loi Godfrain notamment avec les dispositions de la Loi sur la Sécurité Intérieure

caractère personnel, la neutralité de la technologie, et naturellement l'acte de l'opération.

La notion de traitement ne se limite manifestement pas aux opérations à caractère automatisé, de sorte que des opérations simplement manuelles peuvent y satisfaire.

Les opérations elles-mêmes ne sont pas définies plus précisément dans la directive, mais l'article 2 b énumère en revanche une longue liste non-exhaustive des actes considérés comme des opérations. Il s'agit notamment de la collecte, de la conservation, de la modification, de la consultation, de la mise à disposition, du rapprochement ou de l'effacement de données à caractère personnel. Il apparaît tout de suite clairement que cette notion comprend presque tout acte susceptible d'être réalisé avec des données à caractère personnel. L'article indique d'ailleurs aussi explicitement qu'il ne doit pas être nécessairement question d'une série d'opérations pour que l'on puisse parler de traitement. Si l'on pose une seule fois un acte repris dans la longue énumération, il peut déjà être question de traitement.

Données à caractère personnel

L'article 2 a définit les données à caractère personnel comme suit:

« Toute information concernant une personne physique identifiée ou identifiable (personne concernée) est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. »

Il s'agit donc, une nouvelle fois, d'un concept très large, où la possibilité d'identification d'un individu spécifique est utilisée comme critère de classification à titre de donnée à caractère personnel ce qui est cohérent avec l'objet de la directive. Tout comme pour la définition de la notion de traitement, on utilise de nouveau ici une énumération non-exhaustive, cette fois pour donner une indication d'éléments qui peuvent être qualifiés d'identifiants. Par conséquent, le juge devra chaque fois évaluer, pour cette disposition, la qualification in concreto.

Les principes directeurs de la directive

La directive vise à protéger les droits et les libertés des personnes par rapport au traitement de données à caractère personnel en établissant des principes directeurs déterminant le caractère licite de ces traitements. Ces principes sont les suivants :

La qualité des données

Les données à caractère personnel doivent notamment être traitées loyalement et licitement, et collectées pour des finalités déterminées, explicites et légitimes. Elles

doivent en outre être exactes et, si nécessaire, mises à jour.

La légitimation des traitements de données

Il s'agit là du fameux système dit de "l'opt-in" (ou accord préalable).

Ce système implique que le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement, ou si le traitement est nécessaire aux actions suivantes:

- à l'exécution d'un contrat auquel la personne concernée est partie;
- au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
- à la sauvegarde de l'intérêt vital de la personne concernée;
- à l'exécution d'une mission d'intérêt public;
- à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement.

Les catégories particulières de traitements

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions publiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle doit être interdit. Cette disposition est assortie de réserves concernant, par exemple, le cas où le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou aux fins de la médecine préventive et des diagnostics médicaux.

L'information des personnes concernées par les traitements de données

Un certain nombre d'informations (identité du responsable du traitement, finalités du traitement, destinataires des données etc.) doivent être fournies par le responsable du traitement à la personne auprès de laquelle il collecte des données la concernant.

Le droit d'accès aux données et de rectification de ces données

Toute personne concernée doit avoir le droit d'obtenir du responsable du traitement:

- la confirmation que des données la concernant sont ou ne sont pas traitées et la communication des données faisant l'objet des traitements;
- la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive - notamment en raison du caractère incomplet ou inexact des données;
- ainsi que la notification de ces modifications aux tiers auxquels les données ont été communiquées.

Le droit d'opposition aux traitements de données

La personne concernée doit avoir le droit de s'opposer, pour des raisons légitimes, à ce que des données la concernant fassent l'objet d'un traitement. Elle doit également pouvoir s'opposer, sur demande et gratuitement, au traitement des données envisagé à des fins de prospection. Elle doit enfin être informée avant que des données ne soient communiquées à des tiers à des fins de prospection et doit se voir offrir le droit de s'opposer à cette communication.

Les exceptions et limitations

Les principes relatifs⁸⁶ à la qualité des données, à l'information de la personne concernée, au droit d'accès et à la publicité des traitements peuvent voir leur portée limitée afin de sauvegarder, entre autres, la sûreté de l'Etat, la défense, la sécurité publique, la poursuite d'infractions pénales, un intérêt économique ou financier important d'un État membre ou de l'Union européenne ou de la protection de la personne concernée.

La confidentialité et la sécurité des traitements

Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données personnelles, ne peut les traiter que sur instruction du responsable du traitement. Par ailleurs, le responsable du traitement doit mettre en œuvre les mesures appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé;

La notification des traitements auprès d'une autorité de contrôle

Le responsable du traitement doit adresser une notification à l'autorité de contrôle nationale préalablement à la mise en œuvre d'un traitement. Des examens préalables sur les risques éventuels au regard des droits et libertés des personnes concernées sont effectués par l'autorité de contrôle après réception de la notification. La publicité des traitements doit être assurée et les autorités de contrôle doivent tenir un registre des traitements notifiés.

Toute personne doit disposer d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question. En outre, les personnes ayant subi un dommage du fait d'un traitement illicite de leurs données personnelles ont le droit d'obtenir réparation du préjudice subi.

Les transferts de données à caractère personnel d'un État membre vers un pays tiers ayant un niveau de protection adéquat sont autorisés. En revanche, ils ne peuvent être effectués vers un pays tiers ne disposant pas d'un tel niveau de protection, sauf dérogations limitativement énumérées.⁸⁷

La directive vise à favoriser l'élaboration de codes de conduite nationaux et communautaires destinés à contribuer à la bonne application des dispositions nationales et communautaires. Chaque État membre doit en outre prévoir qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées en application de la présente directive.

Un groupe de protection des personnes à l'égard du traitement des données à caractère personnel est institué, composé de représentants des autorités de contrôle

86M.P FENOLL- TROUSSEAU et G. HAAS, *Internet et protection des données personnelles*, Paris : Litec 2000, p. 65 et s.

87Cette disposition sera étudiée en détail dans la suite de ce mémoire

nationales et communautaires et d'un représentant de la Commission⁸⁸.

88Il s'agit du groupe de travail article 29, voir la suite ce mémoire

Application de la directive

Dans son rapport⁸⁹ sur la mise en oeuvre de la directive, de novembre 2003, la Commission note qu'en dépit des retards et des lacunes constatés dans sa mise en oeuvre, la directive a rempli son objectif principal qui est de lever les obstacles à la libre circulation des données à caractère personnel entre les États membres. Elle estime par ailleurs que l'objectif visant à garantir un haut niveau de protection dans la Communauté a été atteint puisque la directive a fixé certaines normes de protection des données parmi les plus élevées au monde.

Elle note néanmoins que la législation en matière de protection des données diverge encore notablement entre les États membres. Or, ces disparités empêchent les organisations multinationales de définir des politiques pan européennes en matière de protection des données.

Afin d'assurer une meilleure application de la directive sur la protection des données, la Commission a adopté un programme de travail comportant un certain nombre d'actions devant être menées jusqu'à la fin 2004. Ces actions comprennent les initiatives suivantes:

- discussions avec les États membres et les autorités chargées de la protection des données sur les changements à apporter à leur législation nationale pour la rendre intégralement conforme aux exigences de la directive;
- association des pays candidats aux efforts visant à une application de meilleure qualité et plus uniforme de la directive;
- amélioration de la notification de l'ensemble des actes légaux transposant la directive;
- simplification des conditions des transferts internationaux de données;
- promotion des technologies renforçant la protection de la vie privée;
- promotion de l'auto-réglementation et des codes de conduite européens.

Cette directive constitue le socle de la politique communautaire en matière de protection des données. Cependant, au vue des évolutions technologiques et des spécificités du secteur des télécommunications, une seconde directive propre aux communications électronique a été adoptée par les institutions européennes.

⁸⁹Rapport de la Commission [COM(2003) 265 final - Non publié au JOUE] Premier rapport sur la mise en oeuvre de la directive relative à la protection des données (95/46/CE).

La directive 2002/58/CE sur la protection de la vie privée dans les communications électroniques

Contexte et objectifs de la directive

Le Livre vert relatif à la convergence des secteurs des télécommunications, des médias et des technologies de l'information⁹⁰, met en avant l'absolue nécessité de revoir la législation concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des télécommunications compte tenu des évolutions technologiques spécifiques à ce secteur. En effet les institutions communautaires considèrent que la protection des données personnelles est la condition sine qua non de l'obtention de la confiance des utilisateurs des services de la société de l'information et par conséquent un des éléments clés de leur développement.

La directive 2002/58/CE⁹¹ complète la directive 1995/46/CE précédemment évoquée dont le champs d'application est plus large. En outre, elle remplace une première Directive 1997/66/CE⁹² du 15 décembre 1997 sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

La directive 2002/58/CE aborde des sujets survenus suite aux évolutions technologiques du secteur comme la conservation des données relatives au trafic par les États membres pour cause de surveillance policière, la transmission de communications non sollicitées, l'usage de « spyware » (ou cookies) et la reprise de données à caractère personnel dans les annuaires d'abonnés.

La directive contient quelques principes auxquels tout traitement licite doit satisfaire. Il importe à cet effet de noter que les principes de la directive 1995/46/CE demeurent valables en ce qui concerne les traitements tombant sous le champ de directive 2002/58/CE. En effet, les nouvelles dispositions de cette dernière directive sont complémentaires avec la Directive 1995/46/CE et ne remplacent pas ses dispositions, sauf en cas de conflit.

Les principes directeurs de la directive

Confidentialité des communications

La directive rappelle, comme principe de base, que les États membres doivent garantir, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications électroniques. En particulier, ils doivent interdire à toute autre personne que les utilisateurs d'écouter, d'intercepter, de

90Livre vert sur la convergence des secteurs des télécommunications, des médias et des technologies de l'information, et les implications pour la réglementation - Vers une approche pour la société de l'information, [COM\(97\) 623](#) final, Non publié au JOUE

91Cette directive est transposée depuis le 9 juillet 2004 par la [LOI n° 2004-669](#) relative aux communications électroniques et aux services de communication audiovisuelle

92Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications [JOUE n° L. 024 du 30.01.1998]

stocker les communications sans le consentement des utilisateurs concernés.

Rétention des données

Concernant la question sensible de la rétention des données, la directive stipule que les États membres ne peuvent lever la protection des données que pour permettre des enquêtes criminelles ou préserver la sécurité nationale, la défense et la sécurité publique. Une telle mesure ne peut être adoptée que lorsqu'elle constitue une « *mesure nécessaire, appropriée et proportionnée dans une société démocratique* ».

Messages électroniques non sollicités (ou spamming)

La directive adopte une approche "opt-in" à l'égard des communications électroniques à caractère commercial non sollicitées, c'est-à-dire que les utilisateurs devront donner leur accord préalable avant de recevoir ces messages. Ce système d'opt-in couvre également les messages par SMS et les autres messages électroniques reçus sur n'importe quel terminal.

Témoins de connexion (ou cookies)

Les témoins de connexion ou cookies sont des informations cachées échangées entre un utilisateur Internet et un serveur web et sauvegardées dans un fichier sur le disque dur de l'utilisateur. Ces informations permettent initialement la persistance d'informations entre deux connexions mais elles s'avèrent aussi un outil de contrôle de l'activité de l'internaute.

À ce sujet, la directive prévoit que les utilisateurs doivent avoir la possibilité de refuser qu'un témoin de connexion ou qu'un dispositif similaire soit placé sur leur équipement terminal. Pour ce faire, les utilisateurs doivent également recevoir des informations claires et précises sur la finalité et le rôle des cookies.

Annuaire publics

Selon la directive, les citoyens européens devront donner leur accord préalable afin que leurs numéros de téléphone (fixe ou mobile), leur adresse e-mail et leur adresse physique puissent figurer dans les annuaires publics.

La sécurité et la confidentialité des données

Ces deux aspects constituent l'une des raisons principales qui ont justifiées la reformulation de la directive 1997/66/CE. Le principe de sécurité est inscrit dans la directive 1995/46/CE, obligeant le responsable du traitement à mettre les mesures nécessaires en place afin de protéger les données personnelles contre la destruction, la perte, la falsification et la publication ou l'accès non-autorisé. La même obligation est appliquée sur les communications électroniques dans l'article 4 de la directive 2002/58/CE.

Les « *mesures d'ordre technique et organisationnel appropriées* » doivent être prises par le prestataire d'un service de communications électroniques accessible au public afin de garantir la sécurité des services. Les mesures doivent garantir un degré de sécurité qui est adapté au risque existant, compte tenu des possibilités techniques les plus récentes et du coût de leur mise en oeuvre.

En cas de risque particulier de violation de la sécurité du réseau, le prestataire (même s'il n'exploite pas ce réseau lui-même) est également obligé d'informer ses abonnés de ce risque, ainsi que des mesures qui peuvent être prises afin de diminuer ce risque. Ainsi, le prestataire est assujéti à une obligation de responsabilisation quant à la sécurité des données dont il a la charge.

L'obligation de garantir la confidentialité des données personnelles est exposé dans l'article 5 de la directive. Le premier point de cette article oblige les États membres à assurer le caractère confidentiel de la communication. En particulier, les États membres doivent interdire à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, à moins que les utilisateurs aient donné leur consentement à tel traitement, ou à moins qu'il existe une exception légale (telle que la sécurité nationale, ou la prévention, la recherche et la poursuite de faits et actes pénalement punissables). Le stockage simplement technique, qui est requis afin de transmettre des informations sur le réseau est exclu du champ d'application de l'article 5. Le premier point de l'article 5 n'est pas d'application sur l'enregistrement légalement autorisé de communications et des données relatives au trafic lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale (comme un achat sur Internet par exemple).

L'article 5 dispose aussi que les réseaux de communications électroniques ne peuvent être utilisés afin d'obtenir des informations sur l'équipement d'un utilisateur du réseau, à moins que ce dernier ne soit informé de façon complète et claire des objectifs d'une telle utilisation, et à moins qu'il ait le droit de refuser. Cette disposition s'oppose à l'utilisation du spyware, un software qui rassemble des données sur l'utilisation d'un ordinateur spécifique et qui transmet cette information sans l'autorisation de l'utilisateur. Les cookies sont également concernés par cette disposition.

Chapitre 3 : L'application internationale des principes de la sphère de sécurité (safe harbor)

Exemple éclairant de l'harmonisation des institutions communautaires en matière de sécurité des systèmes d'information, la politique de protection des données prend une dimension politique significative sur la scène internationale. En effet, l'article 25 de la directive 1995/46/CE et l'application qui en a été faite dans les négociations entre l'Union européenne et les États-Unis sont des éléments incontournables de l'existence d'une vision européenne de la sécurité des systèmes d'information.

L'article 25 de la directive 95/46

Depuis son invention, Internet de même que le monde des communications électroniques est largement dominé par la suprématie américaine, que ce soit en terme d'avancées technologiques ou bien en considérant le nombre d'utilisateurs des réseaux.

Or le cadre juridique européen repose sur l'idée de la nécessité d'une protection forte des données personnelles et de la vie privée. Le principe du « safe harbour » est le lieu idéal de la confrontation entre une vision protectrice des droits attachés à la personne et le principe de la liberté d'expression et une attitude libertaire des États-Unis en terme de marketing électronique et de profiling. À tel point que certains auteurs, tels Yves Pouillet voit dans la réglementation européenne en matière de protection des données une politique active des institutions européennes visant à l'affirmation d'une souveraineté européenne dans le cyber espace. Le problème réside dans la juste définition d'une approche conciliant la protection adéquate des libertés et des valeurs inscrites dans le cadre réglementaire européen et le respect des systèmes des pays tiers rendu nécessaire par le caractère éminemment transnational d'Internet.

L'article 25.1 de la directive aborde ce problème de la manière suivante:

« Les États membres prévoient que le transfert vers un pays tiers des données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales, prises en application des autres dispositions de la présente directive, le pays tiers, en question offre un niveau de protection adéquate. »

La directive précise dans son article 25.2, que l'appréciation du caractère adéquat de la protection du pays doit tenir compte de « toutes les circonstances relatives à un transfert ou à une catégorie de transferts » et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et d'autres concernent le niveau de protection dans le pays tiers, comme « les règles de droit générales ou sectorielles en vigueur ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».

Le texte de l'article 25 suppose donc une approche fonctionnelle, la protection s'évaluant tant par rapport aux risques de d'atteinte à la protection des données générés par le flux en question que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques. La notion de « protection adéquate » implique de comparer les exigences de protection de la directive avec les réponses qui leurs sont apportées hors de l'Union européenne. Il faut tenter de découvrir une certaine « similarité fonctionnelle », c'est-à-dire non pas la transposition intégrale des principes européen mais l'existence de systèmes pourvoyant à cette fonction, ces systèmes pouvant être d'une nature différente. C'est en terme d'équivalence du résultant que l'adéquation de la protection est évaluée dans ce secteur et non pas dans le respect de la forme de celle-ci.

Cette approche permet de respecter les caractéristiques juridiques locales tout en garantissant les résultats d'une protection jugée nécessaire par l'Union européenne. Concernant les instruments de protection mis en place dans le pays tiers, l'article 25 comprend donc non seulement les normes juridiques nationales mais aussi d'autres types de réglementations tels les codes de conduites des secteurs d'activité ou encore les règlements de politiques de protection des données des entreprises.

Le point sur lequel doit se concentrer l'évaluation de la protection est donc son effectivité et la possibilité de recours pour les particuliers de pouvoir en cas d'atteinte à l'encontre de ces principes.

Les principes de la sphère de sécurité (safe harbour)

La négociation entre l'Union européenne et les Etats Unis porte sur la mise en place d'un cadre réglementaire auquel les entreprises américaines peuvent adhérer volontairement. Dès lors que ces entreprises seront considérées comme respectant les normes imposées par la législation européenne en terme de protection des données personnelles, elles peuvent recevoir et traiter des données provenant de l'Union européenne. Les États-Unis étant l'un des premiers partenaires commerciaux de l'Union européenne cette exigence est primordiale.

Or, les approches américaines et européenne de la protection de la vie privée sont diamétralement opposées. Le régime européen, est fondé sur une approche uniforme et centralisée pour tous les États membres, puisque soumise à l'harmonisation communautaire. Le régime américain lui au contraire est diffus et décentralisé, fondé sur une approche sectorielle avec des codes de conduite fondés sur l'auto-régulation des secteurs concernés. La protection des données n'est donc pas soumise à un pouvoir central uniformisant. Cette non homogénéité de la politique de protection des données a comme conséquence que suivant les États où sont installées les entreprises ou encore les secteurs concernés, la politique de protection des données peut être considérée comme tout à fait adéquate au regard de la directive européenne ou pas du tout.

Le 26 juillet 2000, la Commission européenne reconnaît les principes de la sphère de sécurité négociés avec le ministère du commerce extérieur américain. Les principes apportent une solution à ce problème en énumérant les conditions auxquelles une entreprise doit répondre pour être considérée comme adéquatement protégée. L'accord final comporte une liste de sept principes très proches des principes généraux de la directive européenne qui sont ici énumérés :

1. **Notification:** Ce principe correspond aux articles 10 et 11 de la Directive qui définissent le droit à l'information des personnes concernées. La notification contraint les entreprises à informer les personnes concernées de la finalité du traitement réservé à leurs données personnelles ainsi que de leur destination. Un point de contact et une possibilité de s'informer et de s'opposer à ce traitement doit aussi être mis en place.
2. **Liberté de choix:** Ce principe fait référence au droit d'opposition de l'article 14 de la directive. Les Etats Unis ont fait le choix de l'opt-out, ce qui implique que le transfert et l'utilisation des données pour une finalité incompatible avec les finalités initialement déclarées sont possibles si la personne concernée ne s'y oppose pas. Il s'agit certainement d'une garantie plus limitée que l'opt-in imposé dans l'Union européenne.
3. **Transfert subséquent:** Afin que le transfert des données d'une entreprise américaine respectant ces principes vers une autre entreprise américaine qui ne le ferait pas, ne viennent pas ruiner l'efficacité de l'application de ces principes, le transfert est soumis à un régime explicite. En effet, le transfert vers un tiers n'est possible que si celui-ci est déjà soumis aux règles des principes ou lorsqu'une convention écrite engage le tiers à respecter au moins le même niveau

de protection.

4. **Protection des données:** Ce principe fait référence à l'article 16 de la Directive et impose aux entreprises de protéger les données dont elles sont détentrices contre la perte, l'accès illicite, la publication, la modification, l'abus et la destruction.
5. **Intégrité des données:** Afin d'être en conformité avec ce principe, les données à caractère personnel doivent être pertinentes pour les finalités poursuivies par le traitement, un traitement incompatible est dès lors illicite. Les données doivent être fiables, précises, complètes et à jour.
6. **Accès aux données:** Il s'agit en conformité avec l'article 12 de la directive de donner non seulement un droit d'accès à la personne concernée mais aussi un droit de rectification à l'égard de l'inexactitude des données la concernant.
7. **Application:** Ce principe impose aux organisations la mise en oeuvre d'un mécanisme d'application effectif permettant aux personnes concernées d'entreprendre des démarches éventuelles et entraînant des conséquences graves pour une organisation ayant enfreint les principes.

En plus de ces principes une liste de 15 questions-réponses est adjointe. Celle-ci a pour objectif de guider les entreprises voulant adopter les principes. Ces questions abordent de nombreux sujets, tels que les données sensibles, l'auto-certification ou encore les informations publiquement accessibles.

L'Union européenne a reconnu la compétence de deux organismes américains pour le traitement des plaintes relativement à des violations des principes : le Federal Trade Commission et le Department of Transportation. Les principes de la sphère de sécurité laissent une grande autonomie aux organisations adhérentes, en leur permettant de régler elles-mêmes les modalités précises via la procédure d'auto-certification. C'est pourquoi l'Union européenne a obtenu à minima la garantie du contrôle par les deux organismes américains.

Finalement si les principes de la sphère de sécurité apparaissent ambitieux quant à leur objectif, on peut néanmoins émettre quelques réserves quant à leur effectivité. En effet, si la conclusion de ces principes indique une volonté de l'Union européenne de s'engager à faire respecter un modèle alternatif à celui des États Unis, ils sont parfois considérés comme trop peu contraignants, c'est l'avis notamment du groupe de travail article 29.

Le groupe de travail article 29 et les réserves concernant l'application des principes

Pour assurer l'application de la directive 1995/46/CE un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dit "groupe de travail article 29", a été institué⁹³. Ce groupe de travail a pour mission d'examiner toute question relative à l'application des dispositions nationales qui ont été prises en exécution de la directive. Dès 1999, le groupe de travail s'est intéressé aux négociations engagées entre la Commission européenne et les États-Unis, qui ont abouti aux principes sur la sphère de sécurité (safe harbour). Dans son avis sur la question, le groupe de travail article 29⁹⁴ émet quelques réserves. Ces réserves concernent essentiellement les garanties offertes par les principes de la sphère de sécurité et leur application, notamment en ce qui concerne les inspections quelque peu vaguement formulées. Un autre point d'inquiétude est l'effectivité de la possibilité d'obtenir un dédommagement en cas d'infractions éventuelles.

Plus critique Yves Poulet⁹⁵ relève que les principes de la sphère de sécurité méconnaissent le principe de la finalité déterminée et légitime. Par ailleurs, en accord avec l'avis du groupe de travail article 29, il relève que l'effectivité des principes reposent sur des mécanismes compliqués et peu susceptibles d'être respectés. Mais surtout, le plus grand travers de cette accord est que c'est à la personne concernée de s'assurer de la conformité ou non de l'organisme américain. C'est à elle de saisir l'autorité de contrôle. L'intégralité du processus est donc laissé à la sphère privée, ce qui laisse penser que ces principes puissent rester lettre morte.

Cependant, malgré les craintes exprimées quant à l'application effective des principes de sécurité, il faut saluer la mise en place d'un instrument, certes globalement moins protecteur que la directive européenne, mais permettant néanmoins un contrôle des données à caractère personnel transitant outre-atlantique. Tout au moins, sur le plan politique cet accord montre la volonté de l'Union européenne d'assurer le respect des dispositions communautaires dans les pays tiers. Cet accord indique en outre une ouverture des institutions européennes à d'autres formes de régulation laissant une large place aux acteurs économiques par le biais notamment des codes de conduite et de la co-régulation. Ce sont ces autres formes de régulation qui sont abordées dans la section suivante.

93Ce groupe de travail est un comité consultatif indépendant chargé d'analyser la mise en oeuvre de la directive 1995/46/EC. Il se compose de représentants des autorités indépendantes compétentes des États membres comme la CNIL en France et est présidé par un représentant de la Commission européenne. L'article 30 de la Directive lui confie aussi la tâche d'informer la Commission de toute différence entre la réglementation des États membres et les dispositions de la Directive. Le groupe de travail article 29 rédige un rapport annuel sur la situation du traitement des données à caractère personnel dans l'Union européenne et dans les pays-tiers et formule des avis et recommandations.

L'intégralité des travaux du groupe de travail sont accessibles à l'adresse suivante:

http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2004/wpdocs04_fr.htm

94Avis 4/2000 du 16 mai 2000 du groupe de travail article 29

95POULLET Yves , « Les Safe Harbor Pinciples – Une protection adéquate ? », www.juriscom.net, 10 juillet 2000

Section 2 : La co-régulation une approche complémentaire à la réglementation communautaire

La co-régulation, est définie dans l'Accord interinstitutionnel « Mieux légiférer » comme :

« le mécanisme par lequel un acte communautaire confère la réalisation des objectifs définis par l'autorité législative aux parties concernées reconnues dans le domaine (notamment les opérateurs économiques, les partenaires sociaux, les organisations non gouvernementales ou les associations). »⁹⁶

Ce moyen est une sorte de troisième voie pour reprendre l'expression de Timothy Fenoulhet⁹⁷ entre l'approche traditionnelle de la réglementation publique et de l'interventionnisme étatique et l'approche libérale de l'auto-régulation par les acteurs privés. La co-régulation est un concept à géométrie variable qui regroupe des réalités différentes. Si on s'en tient à la vision européenne de la co-régulation, on peut dégager une réelle spécificité européenne dans la régulation de la société de l'information et de la sécurité des réseaux: la co-régulation n'est donc pas un substitut à la régulation publique, bien au contraire, elle en est une forme modernisée. En effet, la co-régulation doit comme le souligne Yves Poulet⁹⁸ :

« [...] non plus être vue comme une discussion préliminaire à la réglementation, discussion entre tous les acteurs publics et privés intéressés, mais davantage comme un mécanisme de répartition des rôles réglementaires. »

Ce mode de régulation est particulièrement adapté à un domaine régi par l'immédiateté, l'ubiquité et la transnationalité. La co-régulation confère à l'ensemble des acteurs le rôle de mettre en oeuvre les objectifs fixés par les voies classiques de la législation communautaire. L'approche communautaire de la co-régulation conserve la hiérarchie entre les interventions publiques et privées. L'intervention privée reste, en effet, investie par et sous le strict contrôle de la réglementation publique. De ce fait, la co-régulation est une méthode à la fois légitime et efficace, conforme aux normes issues du processus législatif traditionnel.

Dans le domaine de la sécurité des réseaux et des systèmes d'information, la co-régulation est promue dans le plan d'action visant à promouvoir une utilisation sûre d'Internet. Elle vise tout particulièrement à soulager la Commission des missions jugées trop techniques en y impliquant largement le secteur privé. La création d'une agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) illustre le développement de la co-régulation.

⁹⁶Définition donnée dans l'Accord interinstitutionnel « Mieux légiférer », 2003/C 321/01. [JOUE n° C. 321 du 31.12.2003]

⁹⁷FENOULHET Timothy, « la co-régulation : une piste pour la régulation de la société de l'information ? », www.droit-technologie.org, 25 juillet 2002

⁹⁸POULLET Yves, « Technologies de l'information et de la communication et « Co-régulation » : une nouvelle approche ? », www.droit-technologie.org, 27 mai 2004, p.6

Chapitre 1 : Le plan d'action visant à promouvoir une utilisation sûre d'Internet

La mise en oeuvre de la sécurité européenne des systèmes d'information passe par l'instauration et le maintien d'un cadre réglementaire favorable à la concurrence. La protection des données est un des aspects privilégié de cette réglementation fondée sur l'harmonisation des législations nationales. Les institutions européennes disposent d'autres instruments qu'elles utilisent pour garantir et favoriser la sécurité des réseaux. Notamment, dans le domaine de la sécurité, la promotion de la recherche concernant le développement et la diffusion de nouvelles technologies nécessaires à garantir la sécurité des internautes aussi bien que les données et les infrastructures qui les transportent. Les programmes de recherche ont permis la mise au point d'applications et de contenus novateurs.

Le plan d'action visant à promouvoir une utilisation sûre d'Internet est adopté le 25 janvier 1999⁹⁹. Son objectif général est d'encourager un environnement favorable au développement de l'industrie liée à Internet en promouvant une utilisation sûre d'Internet et en luttant contre le contenu illégal et préjudiciable. Le programme s'articule autour des trois axes suivants: la création d'un environnement plus sûr par la mise en place d'un réseau européen de lignes directes; l'encouragement à l'auto-réglementation et à l'élaboration de codes de conduites et le développement de systèmes de filtrage et les actions de sensibilisation.

Ce plan d'action envisage le financement d'initiatives publiques ou privées. Par le financement de programmes de recherche par exemple, la Commission tente de faire émerger des projets communs, des standards et des produits qui répondent aux exigences juridiques de l'Union européenne. Le plan d'action, initialement prévu pour la période 1999-2002, a été prolongé jusqu'au 31 décembre 2004.

Contenu du plan d'action

Le plan d'action prévoit une enveloppe financière de 25 millions d'euros¹⁰⁰, vise à inciter les acteurs (industrie, utilisateurs) à développer et à mettre en oeuvre les systèmes adéquats d'auto-réglementation. Il est intéressant de noter que la participation à ce plan d'action peut être ouverte aux entités juridiques établies dans les pays AELE qui sont membres de l'Espace Economique Européen et à d'autres organisations européennes et de pays tiers.

L'objectif du plan d'action peut être résumé de la manière suivante: soutien aux démonstrations et application de solutions techniques; alerte et information des parents et enseignants; encouragement à la coopération et l'échange des expériences et des meilleures pratiques; coordination et coopération entre les acteurs concernés; ou encore compatibilité entre les approches adoptées en Europe et ailleurs.

99Décision [276/99/CE](#) du Parlement européen et du Conseil, du 25 janvier 1999, adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux, entrée en vigueur le 26 février 1999, [JOUE n° L. 33 du 06.02.1999]

100 Le plan d'action est doté d'une rallonge budgétaire de 13,3 millions d'euros pour les deux années supplémentaires (2002 à 2004).

Le plan d'action comprend quatre lignes d'action:

1. création d'un environnement sûr par le biais d'un réseau de lignes directes ("hot lines") et en encourageant l'auto-réglementation et les codes de conduite;
2. développement des systèmes de filtrage et de classification en rendant plus facile l'identification du contenu;
3. promotion d'actions de sensibilisation à tous les échelons pour mieux informer les parents et toutes les personnes s'occupant d'enfants (enseignants, travailleurs sociaux, etc.) sur la meilleure manière de protéger les mineurs contre l'exposition à un contenu qui pourrait être préjudiciable à leur développement;
4. actions de soutien en évaluant les implications juridiques, en les coordonnant avec les initiatives internationales similaires et en évaluant l'impact des mesures communautaires.

La Commission s'engage, entre autres, à entreprendre les actions suivantes :

- promotion de l'auto-réglementation de l'industrie et des systèmes de suivi du contenu des informations diffusées par Internet. Le plan d'action procède à la distinction entre contenu illégal et contenu préjudiciable dont le traitement par les autorités de police est différent.
- encouragement de l'industrie à fournir des outils de filtrage et des mécanismes de classification qui permettent aux parents ou aux enseignants de sélectionner un contenu convenant aux enfants dont ils ont la garde tout en permettant aux adultes de choisir le contenu licite auquel ils souhaitent accéder;
- accroissement de la sensibilisation sur les services offerts par l'industrie auprès des utilisateurs en particulier les parents, les enseignants et les enfants, afin qu'ils comprennent mieux les opportunités d'Internet et en tirent avantage;
- évaluation des implications juridiques;
- activités favorisant la coopération internationale.

Concernant la définition du contenu, la Commission distingue entre contenu préjudiciable et illégal:

- **Le contenu préjudiciable** est à la fois un contenu autorisé mais dont la distribution est restreinte (réservée aux adultes, par exemple) et un contenu qui peut offenser certains utilisateurs, même si la publication n'est pas restreinte en raison du principe de liberté d'expression. Les utilisateurs doivent avoir la possibilité de refuser le contenu préjudiciable. Ceci nécessite le développement de solutions technologiques (systèmes de filtrage et de classification), la sensibilisation des parents et le développement de l'auto-réglementation qui peut fournir un cadre adéquat, en particulier pour la protection des mineurs.
- **Le contenu illégal** est celui dont la diffusion n'est pas autorisé. Il doit être traité à la source par les autorités de police et judiciaires selon les règles des lois nationales et les accords de coopération judiciaire applicables. L'industrie peut cependant apporter une aide importante pour limiter la circulation du contenu illégal (en particulier dans les cas de pornographie juvénile, de racisme et d'antisémitisme) par des mécanismes d'auto-réglementation efficaces (tels que les codes de conduite et l'établissement de lignes directes) régis et étayés par des dispositions juridiques.

La Commission est responsable de la mise en oeuvre du plan d'action et, à cette fin, est assistée par un comité consultatif composé des représentants des États membres et présidé par le représentant de la Commission.

L'évaluation du plan d'action

Comme tous les plans d'actions, le plan d'action visant à promouvoir une utilisation sûre d'Internet est soumis à évaluation régulière. Cette évaluation est ensuite communiquée par la Commission. La dernière évaluation à laquelle a été soumis le plan d'action est celle communiquée dans un rapport daté du 3 novembre 2003¹⁰¹ par la Commission.

Le rapport souligne l'impact positif du plan d'action, notamment dans la promotion de la mise en réseau et la mise à disposition d'une quantité importante d'informations sur les problèmes de sécurité dans l'utilisation d'Internet. L'extension du plan d'action aux technologies de communications naissantes (comme la téléphonie mobile de troisième génération) est prévue dans la seconde phase du programme en 2003-2004. En particulier, le rapport conclut que:

- Le programme a permis d'élaborer plusieurs logiciels de filtrage, ce qui constitue une avancée notable. Néanmoins, l'adoption du classement n'est pas totalement satisfaisante. En outre, certaines parties intéressées estiment que le filtrage n'est pas la meilleure approche pour la protection des enfants. Au niveau politique, le programme a permis de mieux ancrer la place des questions liées au développement d'un Internet plus sûr dans les actions de l'Union européenne et des États membres;
- Concernant les lignes d'action, la Commission a suscité la constitution d'un réseau de lignes directes en Europe, incluant des membres associés non européens (aux États-Unis et en Australie). Elle a financé des recherches sur la sensibilisation des utilisateurs, stimulé le développement du filtrage et soutenu l'élaboration d'un système international de classement;
- une des réussites du programme réside dans la mise en relation des parties intéressées pour aboutir à la constitution d'une "communauté d'acteurs". Toutefois, la Commission regrette une trop faible participation de l'industrie, des organismes d'auto-réglementation et des groupements de consommateurs.

Ce dernier point de l'évaluation de la Commission démontre l'importance qu'elle accorde à la nécessité d'un véritable partenariat entre les différents acteurs de la sécurité des réseaux et des systèmes d'information. En effet, en se plaçant comme arbitre et catalyseur d'une coopération entre les organismes publiques et les acteurs privés, la Commission illustre la volonté des institutions communautaires de mettre en place un nouveau type de réglementation, la co-régulation, qui associe l'ensemble des

¹⁰¹Communication de la Commission, du 3 novembre 2003, concernant l'évaluation du plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet et des nouvelles technologies en ligne par la lutte contre les messages à contenu illicite et préjudiciable, principalement en relation avec la protection des mineurs [[COM\(2003\) 653](#) final - Non publié au JOUE].

acteurs de la société de l'information à la mise en oeuvre des règles qui garantissent une sécurité européenne des réseaux et des systèmes d'information.

Chapitre 2 : Les autres mécanismes de réglementation

L'évolution rapide des technologies et des marchés qui en résulte dépasse largement la vitesse du processus législatif. L'adoption et la transposition d'une directive prennent au minimum trois ans. Durant ce laps de temps, le contexte économique et technologique peut évoluer de telles sortes que la législation devienne obsolète avant même son entrée en vigueur. C'est pourquoi, en complément de l'établissement de normes juridiques strictes au moyen de l'harmonisation communautaire, d'autres mécanismes sont utilisés dans le domaine de la sécurité européenne des systèmes d'information. Ces mécanismes participent, de même que les directives à l'élaboration d'une approche européenne de la sécurité des systèmes d'information, c'est pourquoi il convient d'en étudier la teneur.

Le contrôle des réglementations nationales

En plus des directives, l'Europe met en place des mécanismes visant à prévenir la divergence des systèmes juridiques lors de l'adoption de nouvelles réglementations dans les pays membres. Il s'agit à la fois de prévenir des actions réglementaires nationales mettant en cause une approche cohérente européenne et le cas échéant de détecter des zones d'ombre juridiques nécessitant une harmonisation.

Le principal mécanisme de cette sorte de veille juridique est mis en oeuvre par la Directive 98/48/CE sur la transparence qui fixe une procédure pour la fourniture d'informations dans le domaine des standards techniques et de la réglementation. En effet, les institutions européennes ont conscience qu'en terme de sécurité un cadre juridique stricte et cohérent est nécessaire. Mais une législation trop lourde peut devenir un handicap et freiner le développement de la société de l'information. Un contrôle a priori et une coordination communautaire de toute initiative nationale en la matière est nécessaire pour éviter la fragmentation du marché interne, les inconsistances réglementaires ou encore le risque de suractivité réglementaire.

La directive impose donc aux États membre de notifier à la Commission tout projet de réglementation nationale relative à un service de la société de l'information. Cette notification suspend pendant trois mois la procédure nationale. Cette période autorise la Commission et les autres États membres à émettre des commentaires voire des « opinions détaillées » qui ont force obligatoires vis-à-vis de l'Etat membre ayant pris l'initiative. Ces commentaires ne concernent que les aspects de l'initiative qui pourraient avoir un effet sur la libre circulation des services ou le libre établissement des opérateurs de tels services. Néanmoins, on connaît l'inventivité des institutions européennes pour se servir de ces objectifs en les interprétant très largement afin de mettre en place un espace juridique européen unifié.

La Commission européenne uniformise les règles mais, peu à peu, par ces mécanismes de notification obligatoire par les États membres de leur projets réglementaires et se réserve le droit d'intervenir si elle constate qu'une réglementation existante ou en projet dans un État membre fait obstacle à l'émergence d'une approche uniforme européenne.

La promotion de la coopération des administrations nationales

De nombreux textes européens insistent sur la nécessité d'une coopération renforcée entre les administrations des États membres afin qu'une meilleure coordination de leurs actions se mette en place. Cette coopération passe par l'établissement de systèmes d'échanges d'information, de relais de plaintes ou encore par l'élaboration de codes de conduite communs. La sécurité des systèmes d'information en ce qu'elle implique fortement les administrations nationales n'échappe pas, bien au contraire à cette nécessité de coopération administrative.

Là encore l'objectif de cette coopération est de conduire à une application plus uniforme des textes nationaux pris en application d'une directive communautaire. La coordination de ces administrations s'opère sous l'égide de la Commission ce qui contribue à accentuer son rôle dans le développement d'une politique proprement européenne.

L'article 24 de la directive Commerce électronique¹⁰² impose la coopération entre États membres et la Commission par la mise sur pied de points de contacts administratifs destinés à informer les destinataires des services sur leurs droits et sur les obligations des prestataires de ces services. Une initiative identique a été prise en matière de lutte contre la fraude et la contrefaçon des paiements non liquides¹⁰³: la coopération administrative par l'intermédiaire de points de contact nationaux pour la lutte contre les fraudeurs ou contrefacteurs a été activée¹⁰⁴.

La création d'un comité signature électronique composé des représentants des États Membres est aussi prévu dans la directive sur la signature électronique¹⁰⁵. Ce comité soutient la Commission dans la définition des standards et des critères de conformité applicables. Enfin, dans la Communication du 6 juin 2001 sur la «Sécurité de l'Information et des Réseaux – Proposition d'une approche politique européenne » la Commission envisage la mise en place d'un système européen d'information et d'alertes, fondé sur des relais nationaux. La création d'une agence européenne, étudiée ci après, chargée de la sécurité des réseaux et de l'information répond à cette demande.

102 Directive [2000/31/CE](#) du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques du commerce électronique dans le marché intérieur (« directive sur le commerce électronique ») [JOUE L 178 du 17.07.2000]

103 Règlement (CE) 2560/2001 Règlement du Parlement européen et du Conseil du 19 décembre 2001 concernant les paiements transfrontaliers en euros [JOUE L 344 du 28/12/2001]

104 Recommandation de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire [JOUE L 208 du 02/08/1997]

105 Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, relative à la signature électronique [JOUE L 013 du 19/01/2000]

La promotion de l'auto-régulation

L'auto-régulation est selon Bertrand du Marais:

« l'élaboration et le respect par les acteurs eux-mêmes de règles qu'ils ont formulé sous la forme, par exemple, de règles de bonne conduite et dont ils assurent eux-même l'application¹⁰⁶. »

Ce système peut être considéré comme une forme de régulation décentralisée et non hiérarchique. Les tenants de l'auto-régulation dans le secteur des télécommunications mettent en avant sa plus grande efficacité. En effet l'auto-régulation permet une meilleure adéquation entre le champ de la régulation et le champ géographique du réseau puisque les opérateurs sont eux-mêmes transnationaux. De plus, le respect des normes d'auto-régulation est facilité par le fait qu'elles sont négociées entre les acteurs privés qui doivent les appliquer. En outre, le caractère informel de leur mode d'adoption et de révision en font des procédés plus rapide, plus souple que les normes législatives. L'auto-régulation paraît donc être plus adaptée à encadrer les évolutions technologiques de la société de l'information. C'est pourquoi, les textes européens promeuvent très fréquemment l'auto-régulation. Un exemple fréquemment cité de l'auto-régulation est la netiquette, ensemble de règles de bonne conduite, guidant les internautes dans une utilisation civique d'Internet.

En matière de protection des données personnelles, l'article 25-1 de la directive 95/46 indique que les États Membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer en fonction de la spécificité des secteurs à la bonne application des dispositions communautaires. Ces codes de conduite doivent être soumis aux autorités publiques de contrôle nationales et communautaires qui en garantissent la conformité au regard de la réglementation. L'auto-régulation est encadrée par un ensemble de règles et de normes juridiques découlant de l'harmonisation, communautaire. Loin d'être un substitut à la régulation normative, elle en est le complément. Elle est une réponse adéquate aux aspects techniques d'Internet du fait de sa souplesse et ne peut être efficace qu'encadrée par la législation communautaire.

L'objectif de tels codes de conduite est d'accroître la confiance de l'internaute et d'améliorer l'image de marque des acteurs privés qui s'y soumettent. Cette promotion de l'auto-régulation ne s'arrête pas à la possibilité pour le secteur privé de définir des contenus réglementaires. La Commission européenne encourage également la solution des litiges par des systèmes de médiation ou d'arbitrage en dehors des cours et tribunaux officiels. Ainsi, les acteurs du commerce électronique sont-ils, dans la directive commerce électronique¹⁰⁷ encouragés à faciliter le recours à des systèmes alternatifs de règlements des litiges transfrontaliers.

106 DU MARAIS Bertrand, « auto-régulation, régulation et co-régulation des réseaux », in *Le droit international de l'Internet*, G.Chatillon (ed.), Actes du Colloque de Paris, 19-20 novembre 2001, Bruxelles, Bruylant, 2002, P.296

107 Directive [2000/31/CE](#) du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques du commerce électronique dans le marché intérieur (« directive sur le commerce électronique ») [JOUE L 178 du 17.07.2000]

L'auto-régulation est avant tout une forme de mobilisation conjointe des acteurs du secteur public et privé. À cet égard, dans le domaine de la sécurité des réseaux et de l'information, la Communication de la Commission du 6 juin 2001¹⁰⁸ suggère une approche commune au niveau communautaire¹⁰⁹. Elle propose en particulier de soutenir les projets de normalisation et de certification orientés vers les besoins du marché, et d'investir dans les programmes de recherche et de développement pour rendre les systèmes d'information plus sûrs.

La mise en place d'une stratégie européenne en la matière implique une coopération étroite entre les pouvoirs publics et les entreprises. Ces dernières contribuent en effet directement au développement des réseaux d'information et à leur sécurisation, notamment par le développement de logiciels de protection tels que les programme anti-virus ou les firewalls¹¹⁰.

La Commission a mis en place un forum européen destiné à améliorer la compréhension et la collaboration mutuelle entre les secteurs public et privé. Il rassemble différents acteurs dont les services de police, les fournisseurs d'accès à l'Internet, les entreprises de télécommunications et les association de défense des droits de l'homme ou des consommateurs. Ce forum a pour but de sensibiliser le public à la menace criminelle sur internet par:

- la promotion des meilleures pratiques pour la combattre;
- le développement d'un mécanisme d'alerte précoce et d'un système de gestion de crise
- et l'amélioration de l'échange de connaissance dans ce domaine.

En outre, le plan d'action visant à promouvoir une utilisation plus sûre de Internet , évoqué plus haut, a notamment pour but d'encourager l'auto réglementation de l'industrie pour empêcher la diffusion de messages à contenu illicite et la fourniture d'outils de filtrage sur le contenu des sites Internet. La promotion de l'auto-régulation est donc un complément apporté à la production des normes juridiques qui encadre la politique européenne de la société de l'information et de la sécurité des systèmes d'information. Il n'est pas question pour les autorités européennes de laisser intégralement aux acteurs privés le soin de décider des règles à suivre mais de les associer à la réalisation des objectifs fixés dans par le processus législatif. En ce sens la promotion de l'auto-régulation participe de cette forme de régulation qu'affectionne les institutions européennes lorsqu'il s'agit de réguler la société de l'information, la co-régulation.

108Communication de la Commission au Conseil, au Parlement européen, au Comité économique et Social et au Comité des régions du 6 juin 2001, « La sécurité des réseaux et de l'information : Proposition pour une approche politique européenne », COM(2001)298 final

109Approche entérinée par une résolution du Conseil du 28 janvier 2002 relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information (Résolution 2002/C 43/02)

110 Un pare-feu (appelé aussi coupe-feu ou firewall en anglais), est un système permettant de protéger un ordinateur des intrusions provenant du réseau (ou bien protégeant un réseau local des attaques provenant d'Internet).D'autre part un firewall permet également de contrôler l'accès au réseau des applications installées sur la machine. Le firewall permet d'une part de repérer les connexions suspectes de la machine, mais il permet également de les empêcher.

Chapitre 3 : L'agence européenne de la sécurité des réseaux (ENISA)

La mise en place d'une agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ayant pour fonction de conseiller et coordonner les mesures prises par les États membres pour sécuriser leurs réseaux et systèmes d'informations illustre cette approche novatrice de la co-régulation. L'objectif de cette agence est de renforcer la coopération entre les différents acteurs opérant dans le domaine et, en particulier, entre la Commission, les États membres et les acteurs du secteur privé afin de prévenir les risques et de gérer en commun les problèmes de sécurité.

Tenant compte des insuffisances de l'approche réglementaire, cette agence a aussi pour objectif de promouvoir l'auto-régulation des secteurs en question et de développer une culture de co-régulation entre secteur privé et autorités publiques. C'est bien ce que souligne Erkki Liikanen Commissaire en charge de la société de l'information, dans un discours prononcé le 18 mars 2004¹¹¹ :

« The Commission sees the establishment of ENISA as an important driver for enhanced co-operation across sectors and among countries. I hope that we can find more ways for governments and industry to co-operate on these issues. We share the same goal, and should make security an example of successful public/private partnership. » 112

Enjeux de la création de l'ENISA

Les agences relèvent de la nouvelle gouvernance publique prônée par les institutions européennes¹¹³ qui sépare la conception des politiques de leur mise en oeuvre.

La création de l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) marque la volonté européenne de réguler le monde des réseaux de communication et des systèmes d'information. Les préoccupations de lutte contre la cybercriminalité sont évidemment présentes dans les raisons qui motivent l'Union dans la création de cette nouvelle agence. Des violations répétées de la sécurité des réseaux provoquent des dommages financiers considérables et ébranlent la confiance des utilisateurs.

Les particuliers, les administrations publiques et les entreprises réagissent en faisant appel à des mesures technologiques de sécurité et à des procédures de gestion de la sécurité. Toutefois, les réactions des États membres sont disparates et insuffisamment

111 LIIKANEN, Erkki, Commissaire européen en charge des DG Société de l'Information et Entreprise, « European Network Security » allocution du 18 mars 2004 faite à Hannover, référence: SPEECH/04/148.

112 « *La Commission considère que la mise en place de l'ENISA va développer une coopération renforcée entre les secteurs et parmi les pays. J'espère que nous pourrions trouver encore plus de moyens pour que les gouvernements et l'industrie travaillent ensemble sur ces enjeux. Nous partageons le même objectif, et la sécurité devrait être un exemple de partenariat réussi entre le privé et le public* », traduction non officielle.

113 COMMISSION EUROPEENNE, Livre Blanc sur la gouvernance européenne du 25 juillet 2001, COM(2001) 428

coordonnées.

En dehors de certains réseaux administratifs, il n'existe pas de coopération transfrontalière systématique entre les États membres de l'Union européenne. Enfin, la coordination et l'organisation européenne de la lutte contre la criminalité informatique sont devenues une des priorités de l'Union européenne comme la première partie de ce mémoire l'analyse.

La plupart des États membres ont déjà mis en place des organismes qui interviennent lorsque se pose un risque accru pour la sécurité des données. À cet égard, on peut évoquer la création d'équipes en charge de répondre rapidement à des situations de crise organisées dans toute l'Europe, en complément des départements des services de recherche nationaux spécialisés dans la criminalité informatique ainsi que les campagnes de sensibilisation et l'organisation de formations spécifiques.

Ces constatations et l'urgence de réponses adéquates à ces menaces conduisent à la création d'une Agence chargée de la sécurité des réseaux et de l'information (ENISA) qui entre en fonction en mars 2004¹¹⁴. Cette création s'intègre dans le cadre du plan d'action e-Europe 2005.

Objectifs et fonctionnement d'ENISA

Objectifs

L'ENISA est avant tout chargé de coordonner les politiques nationales et de définir une politique européenne commune en matière de sécurité des réseaux. Ainsi, l'ENISA doit fonctionner comme une organisation de coordination veillant à ce que tous les États membres reconnaissent les mêmes priorités, soient dotés d'une législation similaire, s'échangent des informations et disposent de moyens similaires (campagnes de sensibilisation nécessaires par exemple). L'objectif est également de prêter assistance et fournir des conseils à la Commission et aux États membres dans le cadre de la préparation et du développement de la législation communautaire dans ce domaine. Enfin, l'agence est chargé de faciliter la coopération entre les acteurs des secteurs public et privé¹¹⁵.

114 L'agence a été instituée par le règlement du Parlement européen du 10 mars 2004. Elle est entrée officiellement en fonction le 14 mars 2004. Le Conseil européen a chargé le gouvernement grec d'installer le siège de l'ENISA sur son territoire qui est provisoirement installé à Bruxelles. Pour l'exécution de ses tâches, elle dispose initialement d'un budget de 24,3 millions d'euros par an, révisable à l'expiration du premier terme de fonctionnement de 4 ans.

115 L'article 2 du règlement fondateur de l'ENISA stipule que l'agence renforce « *la capacité de la Communauté, des États membres et, de ce fait, du secteur des entreprises, de prévenir les problèmes de sécurité des réseaux et de l'information, de les gérer et d'y faire face. (...) L'Agence prête assistance et fournit des conseils à la Commission et aux États membres sur les questions liées à la sécurité des réseaux et de l'information relevant de ses compétences telles que définies par le présent règlement. (...) S'appuyant sur les initiatives prises aux niveaux national et communautaire, l'Agence acquiert un niveau élevé de compétences spécialisées. Elle met à profit ces compétences pour encourager une vaste coopération entre les acteurs des secteurs public et privé.(...). Lorsqu'elle y est invitée, l'Agence aide la Commission à mener les travaux techniques préparatoires en vue de la mise à jour et du développement de la législation communautaire dans le domaine de la sécurité des réseaux et de l'information.* »

Définitions

Le règlement fondateur d'ENISA¹¹⁶ étend sa compétence à la sécurité des réseaux et de l'information. Les définitions suivantes permettent de mieux saisir la définition exacte de ce champs de compétence:

- "réseau": désigne les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes et mobiles, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision;
- "système d'information": entendu comme les ordinateurs et réseaux de communications électroniques, ainsi que les données électroniques stockées, traitées, récupérées ou transmises par eux en vue de leur fonctionnement, utilisation, protection et maintenance;
- "sécurité des réseaux et de l'information": définie comme la capacité d'un réseau ou d'un système d'information de résister aux événements accidentels ou aux actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données stockées ou transmises et des services connexes que ces réseaux et systèmes peuvent offrir.

Missions de l'ENISA

Les missions de l'Enisa ont été listées dans le règlement du Parlement et du Conseil l'instituant et peuvent être résumées comme suit:

Mission d'information: collecte des informations nécessaires à l'analyse des risques actuels et émergents pour la sécurité des réseaux et des systèmes d'information, analyse et rapport à communiquer aux États membres et à la Commission;

Mission de conseil: élaboration de conseil destinés aux institutions européennes (Parlement européen, Commission, Conseil, autres organes compétents) ainsi que, le cas échéant, d'une assistance entrant dans le cadre de ses objectifs;

Promotion de la coopération: entre les différents acteurs du secteur (organisation de consultations avec les entreprises et les universités, par exemple) et entre la Commission et les États membres dans l'élaboration de méthodologies communes pour prévenir les problèmes de sécurité;

Actions de sensibilisation et d'avertissement du public: mise à disposition rapide, pour tous les utilisateurs, d'informations objectives et complètes sur la sécurité des réseaux et de l'information. Cette mission nécessite la promotion des échanges des meilleures pratiques actuelles, y compris les méthodes d'alerte des utilisateurs du risque d'attaques informatiques ou de virus particulièrement agressifs;

¹¹⁶Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information [JOUE L 077 du 13/03/2004]

Point de contact entre instances nationales et communautaires: mission d'assistance de la Commission et des États membres dans le dialogue qu'ils entretiennent avec les entreprises privées en vue de gérer les problèmes de sécurité que posent les matériels et les logiciels informatiques;

Suivi de l'élaboration de normes: évaluation, sur le plan scientifique des normes pour les produits et services en matière de sécurité et promotion et développement d'outils d'évaluation des risques. En fonctionnant dans ce cadre comme interlocuteur pour les organismes de normalisation internationaux (comme le W3C), l'ENISA peut exercer une influence importante;

Coopération avec les pays tiers: contribution aux initiatives communautaires visant à coopérer avec les pays tiers et les organisations internationales en vue d'élaborer une approche globale commune sur la problématique de la sécurité. Liaison avec des organisations et groupes internationaux en charge des mêmes questions.

En résumé, l'ENISA doit fonctionner comme centre d'expertise européen centralisé, qui collecte et analyse les données sur les risques existants et nouveaux liés à la sécurité des réseaux et des systèmes d'information. En plus de ces missions d'information, de conseil et d'expertise, l'agence possède des compétences en matière d'assistance nécessaires à la préparation et à la mise en place de la législation communautaire. Enfin, la Commission a la possibilité d'attribuer des tâches supplémentaires à l'ENISA dans les limites de ses objectifs.

Organisation et fonctionnement de l'ENISA¹¹⁷

L'organisation d'une agence communautaire comme l'ENISA est une matière relativement complexe. En effet, l'ENISA doit pouvoir fonctionner de manière suffisamment indépendante pour pouvoir donner un avis objectif à toutes les parties prenantes. À cet égard, la transparence de son administration et des modes de prise de décision doit être suffisamment garantie pour que ses décisions et avis soient empreints d'une légitimité démocratique suffisante.

C'est une des raisons pour lesquelles l'ENISA a été créée sur la base juridique spécifique à la politique de la société de l'information par un règlement communautaire et non pas sur le fondement de l'article 308 CE (ex article 235)¹¹⁸. Ceci permet d'augmenter la légitimité de l'agence, puisque le Parlement européen, élu au suffrage universel est intégré au processus de décision qui abouti à sa création du

¹¹⁷Pour des informations complémentaires, consulter le site Internet de l'Agence européenne pour la sécurité des réseaux (l'ENISA) sous: <http://www.enisa.eu.int>

¹¹⁸Cet article relève que « Une action de la Communauté apparaît nécessaire pour réaliser, dans le fonctionnement du marché commun, l'un des objets de la Communauté, sans que le présent traité ait prévu les pouvoirs d'action requis à cet effet, le Conseil, statuant à l'unanimité sur proposition de la Commission et après consultation du Parlement européen, prend les dispositions appropriées ».

fait de la co-décision¹¹⁹.

¹¹⁹Dans le cadre de l'article 308 CE, le Parlement européen n'a qu'un rôle consultatif

La direction de l'ENISA est confiée à un conseil d'administration, placé sous l'autorité d'un directeur exécutif. Le conseil d'administration établit le règlement intérieur et est responsable du bon fonctionnement de l'ENISA.

Le directeur exécutif est à la tête de l'ENISA et est nommé par le conseil d'administration sur la base d'une liste de candidats présentée par la Commission. Il est responsable du fonctionnement interne de l'Agence, ce qui implique notamment qu'il établit chaque année le programme de travail de l'ENISA qui dresse les objectifs de l'agence.

Il est également institué un groupe permanent des parties prenantes avec pour tâche de conseiller et d'assister le directeur exécutif dans l'exécution de ses tâches. Ce conseil consultatif assiste le directeur exécutif dans l'élaboration d'activité et dans l'entretien de la collaboration étroite entre l'Agence et les institutions et organes compétents dans les Etats membres. L'ENISA peut enfin instituer, en complément des organes permanents, des groupes de travail d'experts sur proposition du conseil consultatif.

Comme pour les autres agences communautaires, des garanties sont mises en place pour assurer la neutralité de l'agence. Les membres du conseil d'administration, le directeur exécutif et le conseil consultatif sont tenus d'agir de manière indépendante dans l'intérêt général. Les experts externes qui participent aux groupes de travail doivent signaler à l'avance tous les intérêts qui peuvent entrer en conflit avec leur indépendance présumée. Pour satisfaire aux exigences de transparence, l'Agence doit veiller à ce que le public et toutes les parties prenantes aient accès à des informations objectives, fiables et facilement accessibles, exception faite des seules informations confidentielles.

Pour élargir également la coopération internationale en dehors de l'Union, l'Agence est également ouverte à certains pays tiers. Il s'agit de pays qui ont conclu, avec la Communauté européenne, des conventions les engageant à reprendre et à appliquer la législation communautaire dans le domaine de la sécurité des réseaux et de l'information. Les modalités concrètes de cette coopération doivent être élaborées au cas par cas.

Pour que les conseils et avis formulés par l'Agence soient acceptés par les particuliers, par les administrations publiques et les entreprises, l'indépendance de l'Agence doit être garantie et reconnue. À cette fin, les membres du conseil d'administration, le directeur exécutif et les experts externes participant aux groupes de travail ad hoc seront tenus de faire une déclaration concernant l'absence d'intérêt susceptible de remettre leur indépendance en question. De plus, l'Agence doit veiller à ce que le public et toute partie intéressée reçoivent une information objective, fiable et facilement accessible, notamment en ce qui concerne le résultat de ses travaux .

L'article 25 du règlement fondateur de l'ENISA prévoit une évaluation du fonctionnement de l'Agence à l'expiration d'un délai de trois ans après la date de son début d'activité. À cette occasion, des adaptations éventuelles seront envisagées pour mieux répondre aux objectifs de l'ENISA. L'existence même de l'Agence sera évaluée. En effet, l'article 27 du règlement stipule expressément que l'ENISA ne fonctionne en

principe que pour une période de 5 ans (à compter du 14 mars 2004).

L'ENISA apparaît donc bien comme le lieu de l'établissement de la politique européenne de la sécurité des réseaux. Néanmoins, il faut souligner que les activités de l'agence sont limitées à un rôle consultatif. Elle n'a pour l'instant aucune latitude en ce qui concerne la production de normes¹²⁰. On peut considérer qu'il s'agit là d'une lacune importante. En effet, la sécurité des réseaux est de part son aspect extrêmement technique un domaine où la certification notamment est très importante et il est à regretter que l'Agence n'est pas le pouvoir de réellement coordonner cette certification au niveau européen et donc d'imposer des standards homogènes. Pour l'instant donc, il ne s'agit que d'un centre d'expertise destinée à assister la Commission dans la mise en oeuvre de la politique européenne de la sécurité des réseaux. Mais il y a fort à parier que son mandat va évoluer vers une participation plus active dans la régulation de la sécurité, comme le lui permet le règlement de création de l'Agence, qui stipule:

« De nouveaux points faibles et de nouvelles menaces apparaissent constamment dans le secteur des réseaux et des systèmes d'information. Il faut que la Commission puisse assigner des tâches supplémentaires à cette Agence afin de rester en prise avec l'évolution actuelle de la technique et de la société... ». 121

En effet, les décideurs politiques commencent d'ores et déjà à prendre conscience que l'harmonisation de la sécurité, en cette époque où la protection contre les risques mobilise les opinions publiques, nécessite de réelles délégations de pouvoirs et surtout une coopération accrue entre les différents acteurs de la société de l'information. Aussi l'ENISA est-elle destinée à prendre en charge de nouvelles responsabilités, comme l'exprime Christian Stoffaës dans un rapport remis au Ministre délégué aux Affaires européennes en 2003¹²²:

« S'il existe donc un « sens de l'histoire » européen, l'étape suivante des démarches [...] sur la coordination de la régulation des réseaux et sur le développement des agences est celle de la mise en place d'une véritable fonction de régulation des réseaux à l'échelle européenne et d'autorités communautaires appropriées. »

120 Ce qui est le cas pour l'agence chargée de la sécurité aérienne, par exemple, qui elle dispose de pouvoirs nettement plus importants, et notamment des pouvoirs de décision contraignants, à portée individuelle et quasi-réglementaire. De plus elle joue en grand rôle en terme de certification.

121 Art. 3.3.2 du Règlement du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information [JOUE L 077 du 13/03/2004]

122 STOFFAËS Christian, « Vers une régulation européenne des réseaux », rapport remis au Ministre délégué aux Affaires européennes, Paris : La Documentation française, 2003, p.24

CONCLUSION

L'émergence d'une politique européenne de la sécurité des réseaux et des systèmes d'information se perçoit timidement dans la coopération intergouvernementale organisée dans la lutte contre la cybercriminalité et la fraude informatique. En effet, ce domaine reste encore très marqué par une approche classique du droit international fondée sur la coopération des forces de police et la mise en place d'une convention internationale.

Il n'existe pas encore de véritable cadre juridique commun à l'ensemble des Etats membres de l'Union européenne dans la lutte contre la criminalité informatique. Ceci s'explique notamment par la réticence des Etats de laisser au processus communautaire un domaine aussi sensible touchant à l'expression de la souveraineté nationale. Les Etats membres de l'Union européenne ont institué des modes de coopération dans le cadre du 3ème pilier communautaire et préfèrent aborder ces questions dans des enceintes plus larges et strictement intergouvernementales comme le Conseil de l'Europe.

Cependant, compte tenu de l'omniprésence de l'informatique et des environnements en réseaux et face à une dépendance croissante de la société vis-à-vis de ces nouvelles technologies, une politique communautaire commence à s'esquisser. L'adoption de la Décision-cadre du Conseil des Ministres de l'Union européenne relative aux attaques visant les systèmes d'information en témoigne.

C'est davantage dans le domaine de la protection du contenu, des données et de la sphère privée, que dans celui de la protection des infrastructures, qu'on observe la mise en place d'un réel cadre réglementaire communautaire traitant de la politique européenne de la sécurité des réseaux et des systèmes d'information. Ce cadre prend la forme d'un appareil législatif destiné à harmoniser les règles juridiques nationales au moyen de l'adoption de directives, comme c'est le cas notamment pour la protection des données et de la vie privée. Il vise à développer la confiance des utilisateurs et à assurer le respect des principes fondamentaux de respect de la vie privée tout en interdisant les pratiques illicites.

On peut interpréter ainsi la négociation sur les « principes de la sphère de sécurité » comme l'affirmation d'une véritable tradition juridique spécifique à l'Union européenne concurrençant la vision américaine des principes régissant la protection des données. Cette affirmation participe à l'émergence d'un cadre spécifiquement européen de la sécurité des réseaux et des systèmes d'information sur la scène

internationale.

Par ailleurs, les institutions européennes ne se contentent pas de produire des textes législatifs, elles promeuvent des enceintes encadrant les initiatives des acteurs privés qui sont invités à participer au dialogue normatif, notamment pour l'élaboration de normes et standards techniques concernant la protection des réseaux. C'est dans la coexistence ou plutôt dans l'articulation de l'action réglementaire communautaire classique avec la promotion des initiatives privées que les institutions européennes se montrent les plus novatrices.

Si aujourd'hui le mandat de la toute nouvelle agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) paraît peu audacieux au regard des enjeux qu'elle aborde et la confine dans un rôle strictement consultatif, la porte ouverte laissée lors de sa création, permettra de faire évoluer son mandat et peut-être d'en faire le lieu de l'épanouissement d'un cadre normatif européen de la sécurité des réseaux et des systèmes d'information.

BIBLIOGRAPHIE

1. Ouvrages

BEN ACHOUR Rafea, LAGHMANI Slim. Le droit international face aux nouvelles technologies : colloque des 11, 12 et 13 avril 2002 (5ème rencontre). Paris : Editions A. Pedone, 2002, 283 p.

BENSOUSSAN, Alain, Le Multimédia et le droit, Paris : Hermès (Mémento Guide), 1996.

BENSOUSSAN, Alain, Internet, aspects juridiques, Paris : Hermès, 1998.

BERGER Michel. Le droit communautaire des télécommunications. Paris : PUF (Que sais-je ?) 1999, 128 p.

BLANDIN-OBERNESSER, Annie, L'Union européenne et Internet, Travaux de la Commission pour l'étude des Communautés européennes (CEDECE). Rennes : Editions Apogée, Publication du Pôle Universitaire Jean Monnet de l'Université de Rennes I, 2001, 189p.

BOURCIER Danièle, dir., HASSETT Patricia, dir., ROQUILLY Christophe, dir. Droit et intelligence artificielle : une révolution de la connaissance juridique. Paris : Romillat (Droit et technologies), 2000, 303 p.

CHATILLON Georges, dir. Droit européen comparé d'Internet. XVe congrès international de droit comparé : Bristol, 1998. Bruxelles : Bruylant (Académie internationale de droit comparé), 2000, 542 p.

CHATILLON, Georges - Le droit international de l'Internet : actes du Colloque organisé à Paris les 19 et 20 novembre 2001. Bruxelles : Bruylant, 2002, cop. 2003 - 693 p.

DECOCQ André, DECOCQ Georges. Droit de la concurrence interne et communautaire. Paris : LGDJ, 2002, 578 p.

M.P FENOLL- TROUSSEAU et G. HAAS, Internet et protection des données personnelles, Paris : Litec 2000.

FÉRAL-SCHUHL, Christiane, Cyberdroit - Le droit à l'épreuve de Internet, 3ème édition, Paris : Dunod 2002.

ITEANU, Olivier, Internet et le droit, Aspects juridiques du commerce électronique, Paris : Eyrolles, 1996.

KRIEG Jean-François, BARELLA Dominique « Espace Pénal commun en Europe : Quelles perspectives ? », Notes de la fondation Robert Schuman, N°16, Fondation Robert Schuman, Paris, Mai 2003, 89 p.

LAMY, Droit de l'informatique et des réseaux , 2000

LAMY, Droit des médias et de la communication, 2000

PANSIER Frédéric-Jérôme. La criminalité sur Internet. Paris : PUF (Que sais-je ? 3546), 2e éd., 2001, 128 p.

THOUMYRE, Lionel « Une Europe unie face à la réglementation de l'Internet ? Etat des lieux », www.droit-technologie.org, 23 octobre 2003.

TRUDEL Pierre et alii. Droit du cyberspace. Montréal (Canada) : Thémis, 1997, n.p.

UNESCO. Les dimensions internationales du droit du cyberspace. Paris : UNESCO, Economica (Droit du cyberspace), 2000, 284 p.

Articles

Cour d'Appel de Paris 11è ch. Corr. Sect. A., 5 avril 1994, « Assistance Génie Logiciel et Geste c/Niel et autres ». Dossier Télécommunications, Les Petites Affiches, n°80, du 5 juillet 1995 (chronique sous la direction du professeur J.Huet).

DU MARAIS, Bertrand « Réglementation ou autodiscipline: quelle régulation pour l'Internet ? », Les cahiers Français, N° 295, La Documentation Française, Paris, mars-avril 2000, p.65-73

FENOULHET Timothy, « la co-régulation : une piste pour la régulation de la société de l'information ? », www.droit-technologie.org, 25 juillet 2002

JOUGLEUX, Philippe « De la négligence dans la protection d'un système de traitement informatisé d'informations », Expertises, juillet 2000, p.220 s.

LE CERF, Xavier « Lutte contre la cybercriminalité : le Projet de convention du Conseil de l'Europe sur la cybercriminalité », www.juriscom.net, 19 avril 2001

PADOVA, Yann « Un aperçu de la lutte contre la cybercriminalité en France », revue de Sciences Criminelles (4), Oct-déc, 2002, p.765 et s.

POULLET, Yves « Les Safe Harbor Pinciples – Une protection adéquate ? », www.juriscom.net, 10 juillet 2000

POULLET, Yves « Internet et vie privée : entre risques et espoirs », Journal des Tribunaux, N°6000 ,Larcier, Bruxelles, 17 février 2001, p. 155 à 164

POULLET, Yves « Vers la confiance : Vues de Bruxelles: un droit européen de l'internet ? », dans CHATILLON, Georges - Le droit international de l'Internet : actes du colloque organisé à Paris les 19 et 20 novembre 2001. Bruxelles : Bruylant, 2002, cop. 2003 - 693 p.

POULLET Yves, « Technologies de l'information et de la communication et « Co-régulation » : une nouvelle approche ? », www.droit-technologie.org, 27 mai 2004

SEDALLIAN, Valérie « Légiférer sur la sécurité informatique : la quadrature du cercle ? », www.juriscom.net, 5 décembre 2003

2. Rapports et documents officiels

2.1. Sources françaises

BRAIBANT, Guy, « Données personnelles et société de l'information, Rapport au

Premier Ministre sur la transposition en droit français de la directive 95/46/CE ». Paris : La Documentation française, 1998, 292 p.

CONSEIL D'ETAT , Section des rapports et études, Internet et les réseaux numériques. Paris : La Documentation française, Coll. Etudes du Conseil d'Etat, 1998, 286 p.

MARTIN-LALANDE, Patrice « Internet : un vrai défi pour la France », rapport présenté au Premier Ministre, Paris: La Documentation française, 1998.

PAUL, Christian « Du droit et des libertés sur Internet », rapport remis au Premier ministre le 19 juin 2000, Paris : La Documentation française, 2000, 200 p.

STOFFAËS Christian, « Vers une régulation européenne des réseaux », rapport remis au Ministre délégué aux Affaires européennes, Paris : La Documentation française, 2003, 153 p.

2.2. Sources européennes et internationales

COMMISSION EUROPEENNE, « Croissance, compétitivité, emploi - Les défis et les pistes pour entrer dans le XXI ème siècle », livre blanc de la Commission européenne, Office des Publications Officielles des Communautés européennes (OPOCE), supplément 6/93, 1993, p. 183.

COMMISSION EUROPEENNE, « Vers une approche pour la société de l'information », livre vert sur la convergence des secteurs des télécommunications, des médias et des technologies de l'information et les implications pour la réglementation, COM(97) 623 final, Non publié au Journal Officiel de l'Union Européenne (JOUE).

COMMISSION EUROPEENNE, « Sécurité des réseaux de l'information : Proposition pour une approche politique européenne », Communication de la Commission européenne du 6 juin 2001 COM(2001) 298 final.

COMMISSION EUROPEENNE, « La gouvernance européenne », Livre blanc de la Commission européenne du 25 juillet 2001, COM(2001) 428

COMMISSION EUROPEENNE, « eEurope 2005 : une société de l'information pour tous », Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions présentée en vue du Conseil européen de Séville des 21 et 22 juin 2002, COM(2002) 263 final.

LIIKANEN, Erkki, Commissaire européen en charge de la Direction-Générale Société de l'Information, « European Network Security », allocution du 18 mars 2004 faite à Hannovre, référence SPEECH/04/148 sur le site www.europa.eu.int

OCDE, « Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité », Recommandation du Conseil de l'OCDE lors de la 1037ème session du 25 juillet 2002, 29 p.

OCDE, Direction de la Science, de la Technologie et de l'Industrie, Comité de la politique de l'information, de l'informatique et des communication, Groupe de travail sur la sécurité de l'information et la vie privée, « Synthèse des réponses à l'enquête sur la mise en oeuvre des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité », référence DSTI/ICPP/REG(2003)8/FINAL, document non classifié du 29 juin 2004, 26 p.

UNESCO. Les dimensions internationales du droit du cyberspace. Paris : UNESCO, Economica (Droit du cyberspace), 2000, 284 p.

3. Sites de Référence

<http://www.legifrance.gouv.fr>

Base de données des textes législatifs français

<http://europa.eu.int/eur-lex>

Le portail d'accès au droit de l'Union européenne

<http://www.db.europarl.eu.int/dors/oeil>

L'Observatoire législatif du Parlement européen

<http://conventions.coe.int/Treaty>

Traités et textes du Conseil de l'Europe

<http://www.ssi.gouv.fr/fr/dcssi>

Direction centrale de la sécurité des systèmes d'information

<http://www.assemblée-nationale.fr>

Site de l'Assemblée nationale

<http://www.senat.fr>

Site du Sénat

<http://www.ladocumentationfrancaise.fr>

Site de la documentation française

<http://www.cnil.fr>

Site de la Commission Nationale Informatique et Libertés

<http://www.commentcamarche.net>

Encyclopédie informatique libre