# Internet et la sécurité des Etats

Bérangère Taxil

# INTERNET ET LA SECURITE DES ETATS

par

Bérangère Taxil (*)

A nouvelles technologies, nouvelles menaces pour les Etats ? Avec l'arrivée de la technique du numérique, de nouveaux moyens de communication et d'information sont nés. Or, la libre circulation de toutes sortes d'informations, quel que soit leur support, peut représenter un danger pour la sécurité des Etats. Pour autant, ceux-ci peuvent-ils (et doivent-ils) contrôler toutes ces informations ?

Internet est le plus récent et le plus vaste système de communication qui ait jamais existé. C'est un outil de dialogue, par le biais des forums de discussion et du courrier électronique. C'est aussi un formidable moyen d'information, avec le World Wide Web (la "toile") : la profusion extraordinaire de sites, qu'ils soient officiels, publicitaires, ou encore personnels, le démontre. Enfin, de façon plus récente, le commerce électronique se développe rapidement, grâce aux nouveaux moyens de paiement virtuel.

Internet est un espace de liberté, mais dans lequel tous les excès sont possibles, de la propagande à la fraude fiscale, en passant notamment par le piratage électronique. Les Etats doivent faire face à cette nouvelle "cybercriminalité", difficile à contrôler. Par leur dimension totalement transnationale, les "autoroutes de l'information" cristallisent l'ensemble des problèmes existants dans les autres secteurs de communication (audiovisuel, télécommunications).

---

* Allocataire – moniteur à l'Université de Paris I Panthéon-Sorbonne, membre du CEDIN (centre de droit international)- Paris I.

Ces nouveaux moyens de communication sont caractérisés par leur relative indifférence à la notion de frontières, de territoire. Le problème s'est posé par exemple avec la télévision directe par satellite : elle fut saluée comme un progrès pour la communication. "*Mais c'était sans compter avec l'hostilité de la majorité des gouvernements, pour lesquels l'audiovisuel relève de la compétence intérieure de l'Etat, et demeure intimement lié à l'exercice de la souveraineté. Ces mêmes Etats craignaient que la télé internationale non contrôlée mette en péril leurs valeurs culturelles, sociales, économiques ou politiques*" (1).

Le problème se pose également pour Internet. Ce réseau permet de véhiculer des valeurs, et certains Etats luttent contre ce qu'ils considèrent être de la propagande, voire de l'ingérence. Ils cherchent ainsi, par le biais d'un arsenal législatif ou technique permettant de restreindre l'usage d'Internet, à protéger leur sécurité ou leur souveraineté. On peut parfois confondre ces deux termes proches aux contours flous, qui recouvrent des aspects différents. La sécurité est une notion qui semble plus restrictive que celle de souveraineté ; toutefois, bien que difficiles à identifier dans leur contenu, ces notions impliquent toutes deux les fondements même de l'Etat.

Les exemples et hypothèses de menaces qui pèsent sur sa sécurité sont innombrables ; elles peuvent être notamment stratégiques, terroristes, idéologiques, économiques, et constituent toujours une atteinte contre les fonctions régaliennes de l'Etat. "*Internet est aujourd'hui utilisé par les plus grands délinquants du monde en raison de sa capillarité qui permet la liaison d'un point à l'autre du globe. Ainsi, la mafia y blanchit l'argent de la drogue en utilisant des systèmes de cryptage ultra perfectionnés. Se réalisent alors, en temps réel, des opérations financières douteuses dans des paradis fiscaux sans que les Etats ne puissent déceler ni identifier les fraudes ou les délinquants… Par ailleurs, l'Internet abrite également les terroristes du monde entier. La sécurité d'un Etat peut également être mise à mal de façon directe par une attaque logique du système de tel ou tel service administratif*" (2).

Face à ces menaces diverses, l'Etat tente de protéger sa sécurité. Mais à ces exigences sécuritaires, on peut opposer, de manière classique, le respect des libertés individuelles. Internet n'échappe pas à cette problématique : il faut concilier protection de l'ordre public et liberté de communication, d'expression.

---

(1) Achilleas P., *La télévision par satellite, aspects juridiques internationaux*, Montchrestien, 1995, p.18.
(2) Bitan H., "L'Internet représente-t-il une menace pour l'ordre public ?", *Expertises des systèmes d'information*, no 196, juillet-août 1996, p.266.

Ces libertés sont consacrées en droit international dans de nombreux instruments conventionnels, que ce soit par la Déclaration universelle des droits de l'homme, le Pacte relatif aux droits civils et politiques, ou encore la Convention européenne des droits de l'homme (3). Mais des limites peuvent y être apportées. Ainsi, la CEDH, dans son article 10§2, encadre ces exceptions : L'Etat peut effectuer des restrictions à la liberté d'expression, à condition qu'elles soient prévues par la loi, qu'elles soient proportionnées, et surtout qu'elles visent un but légitime de "sécurité nationale, protection morale, prévention du crime" (4). Mais cette notion de sécurité nationale peut être interprétée de façon fort variable par les Etats, qui s'abritent parfois derrière cet argument pour ne pas avoir à justifier une atteinte à des libertés fondamentales. Comment identifier et sanctionner une atteinte à la sécurité, si celle-ci n'est pas définie et restreinte à l'essentiel ?

Les Etats ont un intérêt sécuritaire en la matière ; mais ils ne sont pas les seuls. De façon générale, tous les acteurs présents sur Internet (particuliers, entreprises, scientifiques…) ont intérêt à ce qu'une réglementation cohérente soit appliquée à ces réseaux de communication. Or, il est parfois avancé qu'Internet est un espace de non-droit, que les législations nationales ne sont pas adaptées à ce nouveau phénomène, voire même qu'il n'en existe pas en la matière. La réglementation d'Internet existe pourtant sous de nombreuses formes : le réseau peut ainsi être soumis aux lois sur l'audiovisuel, sur les systèmes automatisés, sur l'informatique et les libertés ; enfin, des législations spécifiques au réseau apparaissent également. "*La difficulté propre à Internet ne réside pas dans un prétendu vide juridique, mais dans la mondialisation des échanges. En effet, le cloisonnement des législations nationales conduit inévitablement à des disparités dans la notion d'atteinte à l'ordre public*" (5). C'est donc avant tout la conception qu'ont les Etats de la notion de sécurité nationale (en ce qu'elle est liée à celle de souveraineté) qui va induire des comportements différents face à des menaces identiques.

De nombreuses branches du droit sont impliquées dans la réglementation d'Internet. Ainsi, le droit pénal tente d'identifier, de responsabiliser et de punir les auteurs d'un "cybercrime". Le droit fiscal, le droit de l'audiovisuel, contiennent des dispositions applicables au réseau. Mais

---

(3) Article 19 de la DUDH du 10 décembre 1948 : "*tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions, et celui de chercher, de recevoir et de répandre, **sans considération de frontières**, les informations et les idées par quelque moyen d'expression que ce soit*", in Dupuy P.M., *Grands textes de droit international*, Dalloz 1995, p.131-136.

(4) *ibid*., p.184-200. Pour plus de détails sur ce sujet, voir Slozzi G., "Liberté de l'information et droit international", *RGDIP* 1990/4, p.947s.

(5) Feral-Schuhl, "Contrôle du contenu d'Internet : amorce d'une réglementation", *Les Echos*, 11 juin 1996.

les Etats ne réglementent pas de façon identique. En l'absence d'une convention internationale générale, de nombreuses lois peuvent être utilisées concomitamment pour un même fait, et c'est alors le droit international privé qui peut résoudre ces conflits de lois (6). Le droit international public a également un rôle à jouer dans le développement des communications virtuelles : "*le droit international a toujours été un droit des communications. Dès lors que l'immatériel est un vecteur privilégié ou une des formes privilégiées de communication, il relève d'abord du droit international*" (7)

Internet n'est donc pas un espace hors du droit. Les législations nationales en la matière existent. La terminologie employée (cyberespace, espace virtuel, etc.) ne doit pas faire oublier qu'il s'agit avant tout d'un lieu de communication entre des individus liés à un territoire et à une nationalité. Néanmoins, il est vrai que ces législations, pour cohérentes et complètes qu'elles soient, ne règlent pas certaines difficultés tenant au caractère transnational du réseau.

Face à l'internationalisation de ces supports de communication, comment les Etats peuvent-ils lutter contre la criminalité informatique ? Quelles sont les approches, qu'elles soient juridiques ou techniques, nationales ou internationales, qui permettront d'assurer leur sécurité ?

Les atteintes à la sécurité des Etats doivent être identifiées, pour être sanctionnées, en tenant compte des diverses appréciations de la notion. Mais pour réglementer le réseau, les Etats se heurtent à des problèmes relativement nouveaux. La difficulté d'appréhender ce phénomène tient en effet à son caractère immatériel, et à une certaine inefficacité du droit existant : le droit international reste fondé sur une approche territoriale de la souveraineté, alors qu'Internet est par nature un phénomène empreint d'extraterritorialité et d'internationalité. Les Etats luttent donc par divers moyens contre cette cybercriminalité, que ce soit de façon nationale, ou par le biais d'une coopération régionale et internationale. Le droit international, encore balbutiant en la matière, est ainsi appelé à se développer dans ce domaine, grâce à un intérêt croissant des organisations internationales pour le sujet.

(6) Sur la question, voir Bariatti S., "Internet : aspects relatifs aux conflits de lois", in *Le droit au défi d'Internet, colloque de Lausanne*, Librairie Droz, Genève, 1997, p.65.
(7) Ruiz-Fabri H., "Immatériel, territorialité et droit", *Archives de philosophie du droit*, 1999, volume 43, p.191.

# I. Les atteintes à la sécurité des Etats par le biais d'Internet

## A. Une conception variable de la notion de sécurité

Internet est perçu plus ou moins comme une menace pour la sécurité, selon le degré de contrôle que l'Etat entend exercer sur les informations qui circulent sur son territoire. La notion de sécurité d'un Etat peut ainsi être confondue avec celle d'ordre public, ou encore de souveraineté. Une atteinte à la sécurité, en tant qu'atteinte contre la substance même de l'Etat, peut revêtir de nombreuses formes. Trois exemples marquants peuvent être relevés : ainsi, la situation d'Internet en Chine, aux USA et en France illustre bien ces divergences.

### 1. Une conception maximale de la sécurité : l'exemple chinois.

Fin 1996, on recensait en Chine 200000 propriétaires d'un ordinateur, dont 10% seulement étaient abonnés à l'Internet chinois, "Chinanet". Cet abonnement est conditionné à l'obtention d'une autorisation spéciale de la police, qui limite l'accès à Internet en opérant une sélection des sites accessibles. Dans la majorité des pays de l'ASEAN (Singapour, Vietnam, Philippines, Brunei, Malaisie, Indonésie, Thaïlande), "*les fournisseurs d'accès doivent être agréés, dans chacun de ces pays, par les autorités gouvernementales. Ils sont tenus pour responsables et doivent par conséquent interdire la circulation, par leur intermédiaire, de toute information "contaminatrice", susceptible de nuire à la stabilité politique ou à l'harmonie religieuse*"(8).

Les usagers d'Internet doivent donc se déclarer à la police et remplir une déclaration de responsabilité les engageant à ne pas porter atteinte à la sécurité de l'Etat.

La communication, l'information, sont ainsi considérées en Chine comme des éléments essentiels que l'Etat doit contrôler. La sécurité de l'Etat englobe ici des aspects économiques, politiques, idéologiques, culturels, religieux, etc. On peut estimer que, dans ce cas, il n'est fait aucune différence entre la notion de sécurité et celle de souveraineté, déjà prise dans son acception la plus large.

---

(8) Balle Francis, *Médias et société, de Gutenberg à Internet*, Montchrestien 1997, p.681. Voir également "Une grande muraille contre Internet", *le Figaro* du 14/9/96.

Depuis peu, la Chine semble s'ouvrir quelque peu : en septembre 1998, un "programme d'action franco-chinois sur les nouvelles technologies de l'information" a lancé un dialogue sur les enjeux et sur l'utilisation de ces technologies. Son objectif est "*d'entamer un dialogue approfondi sur la responsabilité des gouvernements et les limites de leur action, la fiscalité et la lutte contre l'évasion fiscale sur Internet, lutte contre la cybercriminalité et la sécurisation des transactions dans le respect de la sécurité et des objectifs d'intérêt public*"(9).

A l'opposé de cette conception extrême de la communication comme danger pour la sécurité nationale, on trouve une conception très libérale d'Internet dans son berceau même, aux Etats-Unis.

**2. Une conception minimale de la sécurité : l'exemple américain.**

Internet, aux Etats-Unis comme ailleurs, s'inscrit dans la problématique relative à la liberté d'expression : à quel équilibre peut-on parvenir, entre ordre public et liberté d'expression ? Dans ce pays, celle-ci est quasiment totale. On sait que le premier amendement de la Constitution américaine fait de cette liberté un principe fondateur de la nation. Par conséquent, l'accès à Internet est totalement libre, et l'Etat est un des principaux usagers de ce moyen de communication. Ainsi, les fichiers informatiques des administrations fédérales et locales américaines sont disponibles sur Internet : "*on peut accéder aujourd'hui directement aux registres d'Etat civil complets de la plupart des Etats de l'Union, aux fichiers publics des agences fédérales, y compris le fisc, ainsi qu'aux listes électorales de 24 Etats. La police et les tribunaux de nombreux Etats affichent sur Internet des renseignements sur les affaires en cours, et les listes de toutes les personnes impliquées dans des procès. Certaines prisons ont désormais des sites Web, avec la liste des prisonniers, leur âge, leur race, la durée de leur peine, leur numéro d'écrou et de dossier…*"(10).

Par rapport à la précédente conception de la sécurité de l'Etat, Internet n'est plus perçu comme une menace. Au contraire, le réseau est utilisé comme instrument de cette sécurité, en tant que protection de l'ordre public.

Il ne s'agit pas de soutenir que la notion de sécurité n'existe pas aux Etats-Unis ; mais elle n'inclut pas les mêmes aspects économiques ou culturels, ou encore religieux, que précédemment. L'ordre public est une

(9) "Programme d'action franco-chinois sur les nouvelles technologies de l'information" du 24/9/98, *Documents d'actualité internationale*, no23, 1/12/98, p.902-903.
(10) Mallet-Poujol, *Nouvelles technologies de l'information et libertés individuelles*, La Documentation Française, 1998, p.44.

chose, la sécurité nationale en est une autre. Elle est pour ainsi dire assimilée à la notion de défense nationale. Les actes commis sur Internet et réprimés en tant qu'atteintes à la sécurité nationale sont alors beaucoup plus restreints qu'ailleurs, ce qui mène aussi à des disparités entre les législations : ainsi, les thèses révisionnistes et négationnistes qui sont admises aux Etats-Unis au titre du droit fondamental de chacun à la liberté d'expression, ne le sont pas en France, où leurs auteurs s'exposent à de lourdes sanctions. Aux Etats-Unis, la crainte principale demeure celle de l'espionnage militaire ou de services tels que FBI, CIA ou NSA (National Security Agency).

### 3. L'exemple français : un équilibre relatif entre liberté d'expression et sécurité nationale

Face à Internet, la France est dans une position intermédiaire, en "voie de développement". L'utilisation du réseau, notamment pour le commerce électronique, est loin d'être courante. Les différentes législations sur la communication, ou encore sur les moyens de cryptage des données circulant sur Internet, illustrent bien la recherche d'un équilibre entre liberté individuelle et protection de la sécurité, comprise ici au sens plus large d'ordre public. La situation d'Internet fait encore l'objet d'un "*bras de fer entre les tenants d'une libéralisation totale et les partisans d'un maintien du contrôle étatique sur une technologie qui relève encore pour partie de l'arme de guerre*" (11). Ainsi, la libéralisation de l'accès à Internet est effectuée de manière progressive.

Les principales actions que l'on tente de sanctionner sur le réseau sont ainsi relatives à l'espionnage, au terrorisme, à la fraude fiscale, ou encore à la pédophilie. Plus que la "simple" sécurité-défense, et moins que la surveillance des communications privées, la notion de sécurité en France s'apparente à la notion d'ordre public, comprenant des aspects tant militaires que moraux (12).

Il n'y a donc pas de définition stricte de ce qu'est la sécurité d'un Etat, ni d'identification précise de ce que sont les atteintes à cette sécurité. On peut toutefois considérer qu'il s'agit de tenter de déstabiliser (voire de détruire) une partie de ce qui symbolise l'Etat : son système militaire, politique, économique, ou social.

La notion de sécurité peut donc s'entendre de façon très large selon ce que l'Etat inclut dans ses fonctions ; en d'autres termes, ce qui constitue sa

(11) Mallet-Poujol, *Nouvelles technologies de l'information et libertés individuelles*, *op. cit*., p.71.
(12) Par exemple, le site Internet de l'école Polytechnique, lequel dépend du ministère de la défense, a été fermé en 1996 à la suite d'intrusions : le mot de passe d'un chercheur français résidant en Israël avait été piégé, ce qui donnait au pirate un accès à tous les ordinateurs reliés au même réseau : voir Inciyan, Kahn, *le Monde* du 4 juin 1996.

souveraineté (13). Néanmoins, laisser cette appréciation aux seuls Etats peut s'avérer dangereux, car cela ouvre la porte à des excès de réglementation, d'interdictions, de sanctions. Cela entraîne également des disparités importantes entre les réglementations nationales. Quels sont vraiment les dangers d'Internet pour la sécurité des Etats ? On peut tenter, de façon pragmatique, d'établir une liste des "cybercrimes" existant à l'heure actuelle et considérés comme tels par la majorité des Etats concernés.

## B. Les dangers d'Internet pour la sécurité des Etats

Dans un ouvrage intitulé "la criminalité informatique", un auteur identifie trois vagues successives de criminalité, dans lesquelles Internet joue un rôle croissant. La première phase concernait uniquement le piratage informatique, sans l'aide des réseaux, Internet n'étant pas encore public. Il s'agissait d'une menace surtout interne, nationale. Ainsi, au milieu des années 1980, le crime informatique consistait à pirater des logiciels, en raison du coût et de la rareté de l'offre. Puis, à la fin des années 1980, une seconde forme apparaît avec, cette fois-ci, l'émergence des réseaux : il s'agit alors de pénétration des systèmes des entreprises et d'attaques de symboles politiques. "*La troisième vague correspond à une sorte d'externalisation du crime informatique. La conjugaison d'une concurrence effrénée entre entreprises et nations, de la reconversion des services de renseignements, de mafias virulentes et l'apparition de terrorismes variés caractérisent une situation où l'information ouverte est privilégiée*" (14).

A l'heure actuelle, les principales menaces pesant sur les Etats sont liées à cette mondialisation, doublée de la libéralisation des moyens de communication. En effet, cette libéralisation entraîne une perte de contrôle des Etats en la matière, et donc un accroissement réel des dangers pour leur sécurité.

Il existe certains délits ou crimes commis par le biais d'Internet mais qui ne concernent pas directement la sécurité d'un Etat. Tel est le cas, par exemple, des atteintes à la vie privée, du viol de droits d'auteurs, des

(13) La résolution 2625 de décembre 1970, prise par l'Assemblée générale de l'ONU affirme ainsi clairement que tout Etat souverain "*a le droit inaliénable de choisir son système politique, économique, social et culturel, sans aucune forme d'ingérence de la part d'un autre Etat* ", in Dupuy P.M., *Grands textes de droit international, op. cit*., p.82.

(14) Martin D., *La criminalité informatique*, PUF, Collection criminalité internationale, 1997, p.25.

contrefaçons, du trafic de médicaments etc. (15). Ce sont les plus faciles à identifier et à sanctionner.

Deux types de menaces visant directement l'Etat peuvent être distingués. Certaines font partie d'une sorte de dénominateur commun aux Etats : elles sont systématiquement sanctionnées. On les regroupe souvent dans le terme "d'infoguerre", de "cyberguerre" ou encore de "cyberconflits" (16). D'autres, en revanche, sont réglementées et sanctionnées de façon différente selon les législations nationales, ce qui conduit à une grande difficulté d'élaboration d'une législation internationale.

### 1. La cyberguerre : une atteinte universellement réprimée

Lors du piratage des sites militaires américains (attaques organisées avec autorisation hiérarchique), les chiffres furent concluant : 88% de succès, 4% des sites repèrant le piratage. "*L'infoguerre est presque à la portée de tout le monde et les technologies utilisées sont développées en toute liberté sur les marchés commerciaux. (...) Toutes les recherches militaires, médicales, économiques ou scientifiques se trouvent dans des ordinateurs vulnérables connus pour être la cible potentielle de gouvernements étrangers*" (17).

Que peut-on inclure dans cette criminalité ? Outre le piratage militaire, le blanchiment d'argent et la fraude fiscale sont aussi communément sanctionnés (18) . La cyberguerre est également un des aspects modernes du terrorisme. Toutefois, si les actes terroristes sont condamnés, il existe déjà une limite en la matière : la simple incitation au terrorisme (comme la publication d'une méthode de fabrication d'une bombe) n'est pas sanctionnée aux Etats-Unis, au nom de la liberté d'expression, mais l'est dans les pays européens.

Globalement, "*la suprématie ne passant plus par la conquête territoriale mais par le contrôle de "l'infosphère", c'est au moyen de virus, de*

---

(15) Pour ce qui est des atteintes à la vie privée, on peut prendre l'exemple récent et désormais célèbre dans le monde des internautes de l'affaire Altern : certaines photos impudiques d'un célèbre mannequin ayant été dévoilées sur un site, www.altern.org, c'est l'hébergeur de ces pages Web, Valentin Lacambre, qui fut condamné, bien que n'ayant matériellement pas la possibilité de contrôler toutes les informations circulant sur son site. Ce type de problèmes a fait l'objet d'une étude approfondie du Conseil d'Etat : *Internet et les réseaux numériques*, collection les études du CE, la Documentation française, 1998, 266 p.

(16) Voir par exemple Guisnel J., *Guerre dans le cyberespace : services secrets et Internet*, La Découverte, 2ème édition, 1997, 320 p. Egalement Wautelet M., *Cyberconflits : Internet, autoroutes de l'information et cyberespace, quelles menaces ?*, Editions Complexe, 1998, 102 p.

(17) Martin D., *La criminalité informatique, op. cit*, p.34-35.

(18) Il suffit de créer un serveur, puis des sociétés clientes fictives de ce serveur, qui l'appellent en permanence : l'opérateur (par exemple France Télécom) facture les clients fictifs, garde 1/3 du prix des consommations téléphoniques et reverse les 2/3 restant au serveur, 2/3 d'argent blanchi. Martin D., *op. cit.*, p.37-38. Pour les questions de fiscalité, voir Le Gall J.P., "Internet : cyberfiscalité ou cyber-paradis fiscal ?", *Revue de droit des affaires internationales (RDAI/IBLJ)*, 1998-3, p.357-372.

*bombes logiques détruisant les ordinateurs de l'adversaire – et désorganisant les communications, le trafic aérien, routier, ferroviaire, les circuits bancaires – que se déroulera ce que l'on appelle aujourd'hui la cyberguerre*" (19).

Parallèlement à ces menaces que l'on peut qualifier de matérielles, il existe également des atteintes aux valeurs morales que véhicule un Etat, qui sont sanctionnées de façon variable.

**2. L'atteinte à l'ordre public : une sanction variable**

Il s'agit ici de menaces qui ne concernent plus la structure de l'Etat, mais l'ordre public (notion plus large que celle de sécurité), dont les Etats ont des conceptions différentes.

Ainsi, les pays européens ont en commun la condamnation de la pornographie impliquant des enfants, la traite d'êtres humains, la diffusion de documents racistes, l'incitation à la haine raciale (20). Les institutions de l'Union européenne ont élaboré une liste du contenu illicite d'Internet, en le distinguant du contenu préjudiciable. Le contenu illicite sera strictement interdit et sanctionné ; il concerne les atteintes à des valeurs fondamentales des Etats européens : la lutte contre la pédophilie, la pornographie, le révisionnisme, en font partie. En revanche, le contenu considéré comme préjudiciable n'est pas sanctionné mais surveillé : les appréciations de ces actes "préjudiciables" varient selon les opinions politiques ou religieuses.

D'autres pays n'effectuent pas cette distinction. Ainsi le révisionnisme diffusé par Internet n'est pas condamnable aux Etats-Unis, en raison du premier amendement de la Constitution. En revanche, la pornographie est plus lourdement sanctionnée.

Il existe enfin une catégorie d'actes qu'il est difficile d'inclure dans les dangers pour la sécurité d'un Etat (bien que certains les considèrent comme tels). Ils sont essentiellement relatifs à des valeurs politiques et religieuses. Ainsi, certains Etats pratiquent une religion d'Etat, ou ont une idéologie nationale exacerbée. La liberté d'expression y est en général assez réduite. Ce n'est que pour ces Etats qu'Internet représente un danger quant à la diffusion de ce qu'ils estiment être de la propagande, et qui est ailleurs libre expression. La limite entre religion et intégrisme religieux peut être parfois floue, tout comme entre opinion politique et propagande. Toutefois, il ne s'agit pas

(19) Lavenue J.J., "Cyberespace et droit international : pour un nouveau jus communicationis", *Revue de la recherche juridique*, 1996-3, p.823.

(20) Voir une résolution du Conseil de l'Union européenne sur les "messages à contenu illicite et préjudiciable diffusés sur Internet" du 17 février 1997, *Documents d'actualité internationale*, no5, mars 1997, p.207-208.

d'éléments appartenant au standard minimum des actes dangereux pour les Etats, devant être systématiquement sanctionnés.

Dans cette notion de sécurité des Etats, tout comme dans l'identification des dangers pour cette sécurité, on ne peut laisser une totale appréciation discrétionnaire aux Etats, car les normes juridiques dépendent aussi de valeurs morales. Cela entraîne trop de disparités entre les législations nationales, avec comme conséquence de nombreux conflits de lois pour un même fait.

Ces cybercrimes posent ainsi un problème essentiel : il existe dans tous les Etats un arsenal juridique suffisant pour les sanctionner ; mais encore faut-il parvenir à les localiser. Si les faits ont lieu sur le territoire, c'est *a priori* relativement simple. Mais souvent ces cybercrimes impliquent des faits plurilocalisés : intervient alors fortement la notion d'immatérialité de ces communications, qui conduit les Etats à produire des législations extraterritoriales. Le droit international, balbutiant en la matière, tente d'appréhender le phénomène, avec comme objectif une réglementation internationale des problèmes relatifs à Internet.

## II. L'appréhension du phénomène des réseaux : le rôle du droit international

Les actes criminels commis par le biais d'Internet peuvent se dérouler sur un seul territoire, auquel cas il est relativement facile de localiser et de sanctionner les responsables. Mais le plus souvent, les fait envisagés sont plurilocalisés, c'est-à-dire que leurs éléments constitutifs prennent place dans plusieurs territoires. Cela pose un double problème : d'une part, celui de l'immatérialité des communications sur le réseau, et par conséquent leur indifférence aux législations nationales ayant une assise territoriale ; d'autre part, celui de l'application extraterritoriale de certaines normes par les Etats, dans un souci d'efficacité certes, mais parfois en contradiction avec le droit international.

### A. La question de l'immatérialité

Il a toujours existé des flux transfrontières, et le droit international connaît déjà ce phénomène : notamment en droit économique, il s'agit fréquemment de réglementer des comportements tenus par des sujets qui se

trouvent dans différents Etats. De plus, la nature immatérielle des communications sur le réseau renforce cette problématique : Internet est non seulement transfrontières, mais aussi (et surtout) indifférent à la notion de territoire. Comment réglementer au niveau national de tels mouvements ? Ainsi, "*parce qu'ils sont organisés en réseaux et parce qu'ils ignorent les frontières, les systèmes d'information posent un difficile problème de contrôle et de surveillance aux autorités. Problèmes techniques mais aussi problèmes juridiques et politiques complexes puisque sur les autoroutes de l'information, il n'existe aucune frontière ni aucun douanier*" (21).

**1. L'absence de rattachement d'Internet au territoire**

Le premier titre de compétence normative des Etats repose sur le principe de territorialité : celui-ci peut être défini comme "*le principe majeur énonçant la maîtrise de l'Etat sur son territoire et le champ d'application spatial normal de ses normes, et qui, à ce titre, cadre les compétences normatives qui s'y déploient. Il exprime ou fonde la compétence de l'Etat pour régir de façon unilatérale et exclusive les mouvements intra-étatiques*" (22). Outre une compétence territoriale, l'Etat possède également une compétence personnelle, fondée essentiellement (mais non exclusivement) sur la nationalité des individus qui forment sa population. Ce sont les deux principaux titres de compétences qui lui sont reconnus. Or, les communications immatérielles sur Internet ont un lien très diffus, pour ne pas dire parfois inexistant, avec un territoire ou une nationalité. Il ne s'agit que rarement de mouvements uniquement intra-étatiques.

Cela ne signifie pas qu'on ne puisse réglementer ce "cyberespace": "*le fait que des zones non susceptibles d'appropriation territoriale puissent faire l'objet d'une réglementation juridique a été établi depuis de nombreuses années au plan international. A cet égard, les problèmes posés par Internet s'inscrivent dans une même évolution tout à fait identifiable d'un droit international passant de l'établissement du statut de certains espaces à la prise en compte, au niveau transnational, de l'organisation du régime de certaines activités*" (23).

La compétence de l'Etat pour réglementer le statut et les activités d'Internet ne peut donc que difficilement reposer sur ces deux titres traditionnels que sont le lien territorial et personnel. Par conséquent, "*le*

(21) Martin D., *La criminalité informatique, op. cit.*, p.64.
(22) Ruiz-Fabri H., "Immatériel, territorialité et droit", *op. cit*., p.190.
(23) Lavenue J.J., "Cyberespace et droit international : pour un nouveau jus communicationis", *op. cit*., p.831.

*développement de communications immatérielles et la porosité du territoire de l'Etat à leurs mouvements posent la question de la maîtrise par l'Etat d'un espace normatif national normalement calqué sur le territoire et exprimé dans le principe de territorialité*" (24).

**2. La remise en cause du principe de territorialité**

De nombreux auteurs s'interrogent sur "*la remise en cause par l'Internet du principe de territorialité des lois. Ainsi, dans un contexte universel où l'information traverse plusieurs ordres juridiques différents à la vitesse de la lumière, comment tenir pour effectives des règles qui ne s'appliquent que sur un seul territoire ?*" (25).

La nature immatérielle d'Internet pose plusieurs sortes de problèmes. D'une part, celui de l'inefficacité des lois pour identifier et sanctionner les responsables d'une atteinte à la sécurité de l'Etat provenant d'un ou plusieurs autres Etats. Par exemple, le code pénal français retient le principe de territorialité dans son article 113-2, qui dispose que "*l'infraction est réputée commise dès lors qu'un des faits constitutifs a eu lieu sur ce territoire*". Or, un crime ou délit commis par le biais d'Internet implique une série d'acteurs (fournisseur d'accès, hébergeur, auteurs des messages illicites, simples utilisateurs etc.), qui peuvent être tous situés en des lieux différents. Un exemple classique est celui de l'affaire Compuserve : un tribunal de Munich a condamné la filiale allemande du groupe américain Compuserve, le plus important fournisseur d'accès à Internet, pour diffusion de messages pornographiques. La société a été sommée de fermer l'accès à 200 serveurs consultables sur Internet. Comme il ne lui était pas possible de paralyser l'accès à ces serveurs dans la seule Allemagne, Compuserve en a bloqué l'accès pour ses quatre millions d'utilisateurs dans le monde entier. Dans ce cas, les lois nationales sont parfaitement applicables, à condition de savoir qui est considéré comme responsable de la diffusion de messages illicites. Ces lois condamnent ainsi souvent la personne qui se situe sur le territoire, c'est-à-dire le fournisseur d'accès, alors que l'auteur de l'infraction se situe dans un autre Etat.

D'autre part, un second problème est celui des conflits de lois, problème classique mais exacerbé en la matière : dans le cas de faits plurilocalisés, plusieurs lois, de plusieurs Etats, peuvent être utilisées de façon parallèle. Il faut donc rechercher quelle seront les lois les plus adéquates et les tribunaux compétents pour une situation donnée. Les principes généraux en la

(24) Ruiz-Fabri H., "Immatériel, territorialité et droit", *op. cit.*, p.187.
(25) Bitan H., "L'Internet représente-t-il une menace pour l'ordre public ?", *op. cit.*, p.268.

matière, au niveau européen, sont contenus dans la Convention de Bruxelles du 27 septembre 1968 concernant la "*compétence judiciaire et l'exécution des décisions en matière civile et commerciale*" (26). Bien qu'elle ait fait l'objet de nombreuses adaptations au fil du temps, elle n'est pas forcément utilisable pour Internet. En effet, elle exclut les matières fiscale, administrative et pénale : "*en conséquence, les différends entre les fournisseurs d'accès et les utilisateurs d'Internet, d'une part, et les autorités publiques d'autre part, en matière fiscale ou concernant la cryptographie ou la censure…ne relèvent pas de la convention de Bruxelles*" (27).

Il reste donc de nombreuses questions sans réponse, qu'elles soient juridiques ou techniques : qui rendre responsable d'un "cybercrime" ? Quelle loi utiliser, sachant que plusieurs seront compétentes et qu'un comportement peut être condamnable dans un pays et pas dans un autre ? Comment localiser l'origine d'un délit commis par le biais d'une communication immatérielle ?

Les législations nationales existant sont applicables aux crimes informatiques. Néanmoins, en pratique, elles sont relativement inefficaces, car fondées sur une compétence étatique territoriale. Internet remet donc en cause le principe de territorialité, voire même de souveraineté territoriale. Il semble donc nécessaire de fonder la compétence normative des Etats sur d'autres titres, exceptions ou aménagements du principe de territorialité.

## B. La question de l'extraterritorialité

La territorialité n'est pas le seul fondement de compétence de l'Etat. Depuis longtemps, le droit international reconnaît aux Etats d'autres compétences, notamment extraterritoriales, pour plusieurs raisons. Compte tenu de ces possibilités, certains vont jusqu'à remettre en cause la validité de la notion de souveraineté territoriale pour la réglementation d'Internet.

(26) Cette convention retient la compétence générale du tribunal du domicile du défendeur. Quant à la loi applicable, il s'agit en général de celle qui a un lien avec un des éléments constitutifs du délit. Certains remarquent qu'en " *l'état actuel de notre monde et de l'Internet, cela voudrait dire déjà que la loi américaine serait compétente dans l'immense majorité des situations*". Voir Lamy *Droit de l'informatique et des réseaux*, 1999, no 2319, p.1317.

(27) Van Overstraeten T., "Droit applicable et juridiction compétente sur Internet", *RDAI / IBLJ*, 1998-3, p.376.

### 1. L'extraterritorialité en droit international : application à Internet

Il y a extraterritorialité dans l'hypothèse où une compétence exercée par un Etat en dehors de son territoire entend se fonder sur un autre titre que la souveraineté territoriale. Elle est admise en droit international, dès lors qu'il existe un lien de rattachement "raisonnable" entre l'Etat et la situation qu'il veut appréhender. En la matière, on cite traditionnellement l'affaire du Lotus, arrêt rendu par la CPJI en 1927, qui affirme que "*la limitation primordiale qu'impose le droit international à l'Etat est celle d'exclure- sauf existence d'une règle permissive contraire- tout exercice de sa puissance sur le territoire d'un autre Etat…Mais il ne s'ensuit pas que le droit international défende à un Etat d'exercer dans son propre territoire sa juridiction sur toute affaire où il s'agit de faits qui se sont passés à l'étranger…*" (28). Cette compétence extraterritoriale n'est pas absolue, et deux distinctions importantes sont à effectuer.

D'une part, il faut différencier compétence normative et compétence d'exécution : la première peut être extraterritoriale, mais pas la seconde. On entend par compétence normative le pouvoir qu'a l'Etat d'édicter des règles à travers ses organes législatifs, exécutifs ou juridictionnels. La compétence d'exécution est le pouvoir de mettre en œuvre une règle générale ou une décision individuelle par des actes matériels d'exécution pouvant aller jusqu'à la mise en œuvre de la contrainte étatique.

D'autre part, un Etat peut édicter des normes extraterritoriales, s'appliquant donc à des situations se déroulant en dehors de son territoire. Il peut également effectuer une application extraterritoriale directe d'une norme qu'il a lui-même édictée, c'est-à-dire prétendre entraîner des effets juridiques directs à l'extérieur de son territoire. On distingue ici le fait d'édicter une norme extraterritoriale du fait d'appliquer une norme territoriale, avec la volonté de donner à cette dernière un effet extraterritorial. Pour ce qui est de la réglementation d'Internet, c'est la seconde hypothèse qui se réalise le plus souvent et qui est fortement contestée. En effet, il n'existe que peu de législations propres à Internet : le réseau est soumis aux lois relatives à la communication ou à l'audiovisuel, lois de nature territoriale. C'est la façon dont elles sont appliquées (comme le montre le cas Compuserve) qui va poser problème.

"*Le seul enseignement que l'on puisse donc tirer d'une analyse rigoureuse de l'arrêt du Lotus est que le droit international n'interdit pas*

(28) Arrêt Lotus du 7 septembre 1927, Recueil CPJI série A no 10.

*l'exercice d'une compétence normative extraterritoriale à l'égard de certaines personnes, de certains biens et actes hors du territoire*" (29).

Cette compétence est d'ailleurs limitée par certains critères : l'extraterritorialité se justifie dès lors qu'il y a un lien de "rattachement raisonnable" entre l'Etat et la situation qu'il veut appréhender. Il s'agit d'une notion qui est encore peu reconnue par le droit positif (exception faite des Etats-Unis), et c'est la doctrine qui tente d'identifier ces critères de rattachement. Internet est le domaine de l'extraterritorialité par excellence, et certains de ces critères peuvent être considérés comme pertinents pour appréhender ce phénomène de réseau mondial.

**2. Quelle compétence étatique pour réglementer Internet ?**

On peut étudier, d'une part, la théorie des effets ou de l'ubiquité, extension fictive du principe de territorialité. Selon cette théorie, "*une infraction est considérée comme ayant été commise sur le territoire d'un Etat si l'un des actes matériels constitutifs de l'infraction y a été commis* ***ou*** *si les effets de l'infraction s'y sont manifestés*" (30). Il s'agit bien dans ce second cas d'une hypothèse réelle d'extraterritorialité. En matière de cybercriminalité, on constate que le lieu du fait générateur, s'il est localisable, est en général différent de celui où il produit ses effets. Cette théorie pourrait alors permettre aux tribunaux de l'Etat victime d'une atteinte à sa sécurité de juger les responsables, bien qu'ils n'aient aucun contact direct avec son territoire. Il s'agit d'un titre de compétence contestable mais utile, "*notamment dans les cas où il est très difficile de déterminer le lieu où l'infraction proprement dite a été commise, par exemple parce que celle-ci suppose le recours à des communications*" (31).Dans la mesure où il s'agit d'une fiction juridique qui assimile un acte commis hors du territoire à un acte commis sur ce territoire, la théorie des effets peut entraîner certains excès, si le lien de rattachement est trop ténu, voire inexistant. Toutefois, elle est très peu reconnue par la jurisprudence (32).

D'autre part, certains auteurs reconnaissent aux Etats une compétence extraterritoriale pour la protection des intérêts nationaux fondamentaux et de la sécurité. Ainsi, pour certains, il s'agit d'une compétence fondée sur la

(29) Stern B., "Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit", *AFDI* 1986, p.19.
(30) Conseil de l'Europe, *Compétence extraterritoriale en matière pénale*, Strasbourg, 1990, p.25.
(31) *ibid*., p.26.
(32) Elle n'a été utilisée qu'indirectement par la CJCE dans l'affaire Pâte de bois du 27 septembre 1988. Voir Stern B., "l'extraterritorialité revisitée, où il est question des affaires Alvarez-Machain, Pâte de bois et de quelques autres…", *AFDI* 1992, p.239-312.

souveraineté, et "*le droit international public reconnaît ainsi à tout Etat la possibilité d'exercer une compétence normative extraterritoriale à l'égard de tous faits menaçant son existence ou sa sécurité*" (33).On utilise dans ce cas le terme de "principe de protection". Consciente que ce critère peut être source d'abus, que la notion "d'intérêts" n'est pas une notion juridique et peut difficilement servir de fondement à une réclamation internationale, la doctrine tente de déterminer, en fonction de la pratique des Etats, ce qui peut constituer un intérêt essentiel de la nation. "*On peut se demander s'il est vraiment possible, voire sage, d'essayer de les énumérer. Pour que l'application de ce principe de compétence soit en conformité avec les objectifs généraux du droit international public, il devrait être limité aux intérêts considérés comme vitaux pour l'existence de l'Etat, de ses institutions et de son ordre constitutionnel et social*" (34). La sécurité nationale en fait nul doute partie, et ce principe de compétence, s'il était reconnu par le droit positif, pourrait être directement applicable au réseau Internet. Ce n'est pas encore véritablement le cas, et seuls les américains usent (et abusent ?) de ce critère pour justifier leur législation extraterritoriale (35).

En l'état actuel du droit, les Etats ne peuvent encore pas, de façon générale, édicter de telles normes ou en effectuer une application extraterritoriale. Est-ce d'ailleurs souhaitable ? Pour ce qui est de leur comportement vis-à-vis d'Internet, ils demeurent largement limités par le cadre territorial de leurs compétences. Cela conduit certains à proposer une remise en cause du fondement même du droit international : la souveraineté territoriale.

Dès 1959, lors d'un cours relatif au droit de l'espace professé à l'Académie de la Haye, Rolando Quadri affirmait déjà qu'on ne pouvait plus parler de souveraineté en terme territoriaux, en raison du caractère "spatialement incoercible" de certaines activités (36). Selon lui, il était plus approprié de traiter la souveraineté en termes fonctionnels : au niveau international, il s'agit non plus de réglementer les espaces mais les activités. Certains appliquent désormais ce raisonnement à Internet.

Ainsi, un auteur estime que "*si la notion de souveraineté territoriale paraît désormais difficile à retenir, on peut s'interroger sur le caractère d'une*

(33) Stern B., "Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit", *op. cit*., p.25.
(34) Conseil de l'Europe, *Compétence extraterritoriale en matière pénale, op. cit.*, p.31.
(35) Ainsi en est-il, notamment, pour la loi Helms-Burton. Le titre de compétence fondé sur la sécurité nationale fait d'ailleurs partie du §402 du 3ème restatement américain, leur accordant ainsi une faculté générale d'édiction de normes extraterritoriales. Ce même §402 constitue également une application de la théorie des effets.
(36) Rolando Quadri, "Droit de l'espace", *RCADI* 1959-3.

*autre conception de la souveraineté : la souveraineté « informationnelle » par exemple*" (37). Un article paru dans le Monde traite ainsi de cette "souveraineté informationnelle" (38). "*Constatant à son tour l'inanité de l'approche territoriale, l'auteur définira la souveraineté comme une capacité à déterminer le régime des activités en cause…Entendue jadis en termes géographiques et territoriaux, elle consiste aujourd'hui à assurer le contrôle du patrimoine informationnel. De sorte que la maîtrise de l'information constitue désormais un nouvel attribut du pouvoir souverain…La souveraineté informationnelle comprend le droit de restreindre ou de soumettre à certaines conditions l'accès à l'information et sa communication à des pays étrangers*" (39).

Ce raisonnement peut paraître un peu excessif. En effet, s'il est vrai que le principe de territorialité doit être relativisé, modéré par d'autres types de compétence étatique, cela ne signifie pas pour autant qu'il faille le nier. Il demeure la base du droit international public. Si le contrôle étatique sur certains domaines semble disparaître, cela peut aussi être du à une volonté des Etats eux-mêmes : ainsi, "*l'exemple des autoroutes de l'information montre un retrait volontaire des Etats : l'initiative privée est considérée comme le moteur du développement de la société de l'information*" (40). Ainsi, ce sont les Etats qui esquissent un mouvement de désengagement, ce qui va à l'encontre de la notion de "souveraineté informationnelle". L'information semble au contraire échapper de plus en plus au domaine réservé étatique.

Pour autant, les Etats ont toujours un rôle essentiel à jouer dans la lutte contre la cybercriminalité. Mais les solutions envisageables sont multiples, et ne passent pas nécessairement par des approches nationales, aux tendances extraterritoriales. Il faut distinguer extraterritorialité et internationalité : "*on peut considérer l'extraterritorialité comme signifiant que l'Etat projette sa compétence normative unilatéralement à l'extérieur de son territoire*", ce qui peut être source de nombreux conflits. En revanche, "*l'internationalité apparaît lorsque deux ou plusieurs Etats se coordonnent de façon plus ou moins formelle pour réguler en commun une situation qui les concerne tous*" (41). C'est peut-être effectivement par une approche coordonnée que les

(37) Lavenue J.J., "Cyberespace et droit international : pour un nouveau jus communicationis", *op. cit*., p.831-832.
(38) Leîla Bouachera, "La souveraineté informationnelle entre utopie et projet", *Le Monde* du 1er décembre 1996.
(39) Lavenue J.J., "Cyberespace et droit international : pour un nouveau jus communicationis", *op. cit*., p.833.
(40) Ruiz-Fabri H., "Immatériel, territorialité et droit", *op. cit*., p.204.
(41) Ruiz-Fabri H., "Immatériel, territorialité et droit", *op. cit*., p.197-198.

solutions seront les plus adaptées aux problèmes spécifiques posés par Internet.

## III. Les solutions pour lutter contre la cybercriminalité

Les solutions actuelles aux problèmes de sécurité posés par Internet sont de deux types. Il existe ainsi des solutions purement techniques qui permettent aux Etats d'obtenir un contrôle plus large des données circulant sur Internet : il s'agit des méthodes de cryptologie. Toutefois, cette seule approche ne suffit pas et est aujourd'hui en passe d'être abandonnée. On privilégie donc désormais des solutions juridiques, impliquant une coopération internationale.

### A. Les solutions techniques : la question de la cryptologie

La cryptologie (ou cryptographie) est le "*procédé qui permet de rendre une donnée, un texte, une image ou un son illisible sauf pour son destinataire*" (42). Elle permet le chiffrement des données, à l'aide de "clés". Plus la taille de la clé (exprimée en nombre de bits) est importante, plus le chiffrement est complexe et difficile à pirater. Un débat existe autour de cette méthode, qui peut être utilisée par l'Etat mais aussi contre lui. Les Etats hésitent donc de plus en plus à s'en servir uniquement comme outil de sécurité : on assiste à un mouvement de libéralisation de cette technologie, désormais accessible aux personnes privées.

#### 1. Débat autour de la cryptologie

Elle était autrefois réservée à l'Etat et classée matériel de guerre jusqu'au début des années 1990 : "*l'Etat doit, pour les intérêts essentiels de sa sécurité, éviter que des exportations de technologie de haut niveau ne renforcent le potentiel militaire de pays susceptibles de recourir à des actions armées. Au rang de ces technologies figurent celles relatives à la sécurité des systèmes d'information*" (43). Aujourd'hui, les logiciels de cryptage sont, dans une certaine mesure, accessibles aux "civils". Ceux-ci ont alors la possibilité

(42) Balle F., *Médias et société, de Gutenberg à Internet, op. cit.*, p.686. Pour une réflexion sur la problématique et les perspectives historiques de la cryptologie, Stern J., *La science du secret*, Editions Odile Jacob, Paris, 1998, 203p. "*Les termes cryptologie et cryptographie sont restés longtemps synonymes et recouvrent encore aujourd'hui un contenu sémantique proche, même si l'on a eu progressivement tendance à utiliser le mot cryptologie pour désigner la science des messages secrets, réservant l'autre substantif à l'ensemble des méthodes mises en œuvre pour assurer ce secret*", p.10.
(43) Martin D., *La criminalité informatique, op. cit.*, p.102-103.

de crypter leur communications privées, ou d'effectuer des transactions commerciales sécurisées. Un premier problème se pose alors : si la cryptologie permet aux Etats de contrôler ce qui se passe sur Internet, elle n'empêche pas les fraudes, car les criminels peuvent également disposer d'instruments de cryptage, parfois plus puissants.

La cryptologie étatique représente également un inconvénient pour les individus, qui peuvent voir leurs communications privées déchiffrées par l'Etat. Cela peut ainsi être un frein pour certaines activités. Il faut donc trouver un équilibre entre deux types d'intérêts sécuritaires : celui des Etats et celui des particuliers. Ainsi, "*la crainte de l'espionnage et les activités menées par les services de renseignements pour des raisons de sécurité nationale sont des facteurs de complication dans le débat concernant la cryptographie. Si les divers pays décident que cet intérêt doit prévaloir, il est probable que le développement du commerce sur Internet sera considérablement ralenti…*" (44).

Un débat s'élève donc depuis quelques années : faut-il libéraliser la cryptologie ? En effet, les Etats souhaitent utiliser la cryptologie pour se protéger, en contrôlant son accès aux particuliers comme aux entreprises. Les particuliers et les entreprises souhaitent également s'en servir, pour assurer la sécurité de leurs communications, de leurs transactions etc. La question tourne ainsi autour du monopole de son utilisation et de son contrôle par l'Etat, ou de sa libéralisation. Les Etats souhaitent conserver la mainmise sur cette technologie. Or, "*personne ne peut être empêché efficacement de chiffrer des données (les criminels ou les terroristes peuvent également utiliser le chiffrement pour leurs activités), par exemple en chargeant simplement un logiciel de chiffrement puissant à partir d'Internet. Le résultat en est que restreindre l'usage de la cryptologie pourrait bien empêcher les entreprises et les citoyens respectueux des lois de se protéger contre les atteintes criminelles. Cependant, cela n'empêcherait pas totalement les criminels d'utiliser ces technologies*" (45).

Par conséquent, on assiste à un mouvement de libéralisation de la cryptologie dans certains pays, notamment en France.

### 2. Vers la libéralisation de la cryptologie ?

C'est aux Etats-Unis que la cryptologie a d'abord été libéralisée, au début des années 90. Les clés des logiciels tolérés pour une utilisation civile ne pouvaient pas dépasser 40 bits. Cela permettait à l'Etat de pouvoir les

(44) Bernhard S., "How to secure the network : mutual trust and encryption", *RDAI/IBLJ*, 1998-3, p.326.
(45) Mallet-Poujol, *Nouvelles technologies de l'information et libertés individuelles, op. cit*., p.76.

décrypter, et ainsi de limiter les risques pour sa sécurité. Or, en 1991, un logiciel extrêmement perfectionné, PGP (Pretty Good Privacy), fut diffusé gratuitement sur Internet par son créateur, Philip Zimmermann. Il s'agissait pour lui d'un moyen de protection de la vie privée face à un Etat soupçonné de vouloir espionner la correspondance électronique des citoyens. "*Son système réputé 300 millions de milliards plus puissant que les moyens de cryptage habituels offrait la possibilité d'échanger données et correspondances sur Internet sans que FBI, CIA ou NSA puissent y avoir accès…. En rendant le logiciel accessible, il venait de s'attaquer à un dogme issu de la guerre froide : l'export de logiciels, considérés comme des armes de guerre, n'était autorisé que lorsque les clés de chiffrement ne dépassaient pas 40 bits. Or, les clés de PGP en comptaient 128. Les poursuites engagées par un juge fédéral de San José n'ont cessé qu'en janvier 1996, sans que Zimmermann soit condamné (...). C'est que les préoccupations des champions de l'intimité et les intérêts de l'industrie électronique convergent : le développement du commerce en ligne ne peut se passer de moyens de cryptage sûrs*" (46).

Entre 1996 et 1997, l'usage de PGP a été toléré, mais restreint aux entreprises américaines, et interdit d'exportation. Depuis juin 1997, la cryptologie est largement libéralisée et des logiciels comme Netscape et Microsoft Explorer utilisent des clés à 128 bits. Les Etats-Unis ont ainsi quasiment abandonné la cryptologie comme moyen d'assurer leur sécurité nationale.

L'évolution en France est beaucoup moins rapide (47). Elle a toujours été très restrictive sur le sujet : une loi de 1990 soumettait la cryptologie à un régime d'autorisation préalable. En 1996, une première évolution se dessine, et instaure un système unique au monde : celui du tiers de confiance. La loi de 1996 instaure plusieurs régimes ; elle distingue notamment les clés inférieures à 40 bits (d'utilisation libre) et supérieures à 40 bits : celles-ci sont autorisées, à condition de déposer les clés chez un tiers de confiance agréé par l'Etat, le principal étant le SCSSI (Service central de la sécurité des systèmes d'information), service du Premier Ministre. Ce système a largement échoué, les entreprises refusant de confier leurs clés à des organismes proches de l'Etat.

---

(46) *ibid*, p.70.

(47) Pour la situation de la cryptologie en France, voir le rapport Francis Lorentz au ministère des finances, du 7 janvier 1998, intitulé "*le commerce électronique : une nouvelle donne pour les consommateurs, les entreprises, les citoyens et les pouvoirs publics*", notamment sa partie III : "La sécurité et la confidentialité des échanges", disponible sur www.internet.gouv.fr.
Voir également sur www.legifrance.gouv.fr , la loi no 96-659 du 26 juillet 1996 sur la réglementation des télécoms, publiée au JO du 27 juillet 1996 et ses décrets d'application no 98-206 et 98-207 du 23 mars 1998.

C'est pourquoi, depuis janvier 1999, la France a décidé de s'aligner sur la plupart des pays dans lesquels Internet est utilisé, et de libéraliser totalement la cryptologie. Une réforme législative sera effectuée, autour des orientations suivantes : liberté totale d'utilisation (niveau relevé de 40 à 128 bits), sous réserve du maintien des contrôles à l'exportation, et suppression du recours aux tiers de confiance (48).

### 3. Une harmonisation envisageable du régime de la cryptologie

Les Etats semblent ainsi s'aligner sur un standard de libéralisation maximum de la cryptologie à 128 bits. Par ailleurs, au niveau international, c'est l'OCDE qui est chargée de la question. Elle a ainsi élaboré, en 1992, des "lignes directrices sur la sécurité des systèmes d'information". Celles-ci avaient pour objet d'établir les liens entre cette sécurité, la cryptologie, et la protection de la vie privée. Elles ont mené aux "lignes directrices pour une politique de la cryptologie" du 27 mars 1997 (49). Ce texte constitue un compromis entre les intérêts des Etats et des entreprises, et va moins loin que la solution choisie par la France. En effet, l'OCDE prône simplement une harmonisation du régime de la cryptologie entre les Etats membres, tout en posant comme principe le libre choix d'une méthode de cryptologie. Il s'agit d'une reconnaissance du rôle fondamental de la cryptologie comme moyen de protection de la vie privée, mais l'organisation ne préconise pas expressément la libéralisation. "*La principale avancée se matérialise en fait par la reconnaissance de la solution de l'accès légal au texte clair ou aux clés de cryptologie par l'intermédiaire d'un tiers de confiance, de façon à permettre l'utilisation du chiffrement tout en sauvegardant les intérêts des Etats*" (50).

La cryptologie était utilisée par les Etats principalement pour lutter contre l'espionnage électronique, le terrorisme et autres manifestations de "cyberguerre". Le choix de la libéralisation indique clairement que ce n'est désormais plus le cas.

Cette technique de sécurisation est peut-être en passe de servir uniquement pour le commerce et ne présentera plus guère d'utilité pour les Etats, qui doivent se tourner vers des solutions juridiques.

---

(48) "La France renonce à contrôler les communications sur Internet", *Le Monde*, 21 janvier 1999, p.10.
(49) "Guidelines for cryptography policy", OCDE/GD(97)204, disponible sur www.oecd.org
(50) "Cryptologie, les lignes directrices de l'OCDE", *SILEX (revue internationale du droit de l'informatique et des systèmes d'information)*, no 97-2, p.5.

## B. Les solutions juridiques : le développement de règles internationales

On peut aisément constater les inconvénients des approches uniquement nationales : en raison du cloisonnement des législations, de leur diversité, et des conflits juridiques que cela engendre, il semble qu'une coopération internationale soit souhaitable. Les organisations internationales commencent à se pencher sur les différents problèmes juridiques que pose Internet. Toutefois, elles adoptent pour l'heure une approche extrêmement sectorisée ; il n'existe pas encore de véritable droit international qui constituerait une réglementation globale d'Internet. Des solutions diverses sont d'ores et déjà proposées, qui mêlent solutions nationales, internationales, publiques et privées.

### 1. L'ébauche d'une coopération juridique internationale : le rôle des organisations internationales

Depuis le milieu des années 90, les organisations internationales tentent d'élaborer une réglementation internationale d'Internet. Une coopération internationale en matière de lutte contre la cybercriminalité est ébauchée. Toutefois, la compétence d'une organisation internationale est restreinte par le principe de spécialité de sa mission. Ce sont donc des approches sectorielles, compartimentées selon les domaines, qui sont adoptées.

Ainsi, l'OCDE, qui dispose d'un comité de la politique de l'information, de l'informatique et des communications, tente de résoudre les problèmes de criminalité en matière de commerce. Outre les lignes directrices sur les questions de cryptologie, elle travaille, par le biais du GAFI (Groupe d'action financière internationale), sur le blanchiment d'argent et le trafic de drogue. Le conseil de l'Europe, quant à lui, effectue des recommandations sur les problèmes de droit pénal et de procédure pénale liée à la criminalité informatique.

L'Union européenne travaille également sur certains aspects particuliers de cette criminalité : il s'agit essentiellement d'une approche qui porte sur les questions de pornographie, de pédophilie, de racisme, et de terrorisme. Le Conseil de l'Union a pris le 17 février 1997 une résolution qui fixe un objectif général : celui "*d'établir un résumé des problèmes que pose le développement rapide d'Internet et d'évaluer, en particulier, l'opportunité d'une réglementation communautaire ou internationale*" (51).

(51) Conseil de l'UE, "Résolution sur les messages à contenu illicite et préjudiciables diffusés sur Internet", *op. cit.*, p.207.

L'ONU, quant à elle, ne semble pas envisager une approche générale du sujet. Seule la CNUDCI (Commission des Nations Unies pour le droit commercial international) a jusqu'à présent élaboré un texte, sur un sujet très particulier : celui du commerce électronique. Elle a ainsi rédigé une "loi-modèle" sur la question, adoptée par l'Assemblée générale en juin 1996 (52).

Ces approches limitées illustrent la difficulté de lancer une réflexion générale sur la criminalité informatique. Les intérêts des Etats divergent, notamment en raison de leurs approches différentes de la criminalité : il en découle, pour l'instant, une impossibilité d'élaborer une réglementation universelle. Toutefois, des solutions sont proposées, compromis entre réglementations nationales, internationales, et auto-régulation du réseau.

**2. Une réglementation internationale pour Internet ?**

Sachant qu'un comportement peut être condamnable dans un pays mais pas dans un autre, il paraît impossible d'élaborer un droit universel. Est-il d'ailleurs souhaitable de tenter une uniformisation des valeurs politiques ? Ceci est un autre débat. Toutefois, le droit international doit jouer un rôle, pour pallier les insuffisances des législations nationales. Certains problèmes sont difficiles à traiter au seul plan national. Ainsi, certains prônent une réflexion internationale sur les questions suivantes : "*la criminalité informatique transportée en ligne ; la diffusion de messages racistes, xénophobes ou plus largement discriminatoires dans les réseaux (et peut-être la diffusion de messages pédophiles dans la mesure où de rares Etats manifestent une étonnante complaisance à cet égard) ; l'utilisation des œuvres protégées à travers le réseau ; ou encore le recours à la cryptologie*" (53). Pour un droit véritablement international en la matière, plusieurs techniques juridiques peuvent être employées. Il est d'abord possible d'élaborer des traités internationaux ; c'est l'option choisie notamment par le Conseil de l'Europe, qui a mis en place en 1997 un "comité sur la criminalité dans le cyberespace", chargé de proposer un projet de traité sous trois ans. Toutefois, il faut souligner que, pour être efficace, cette approche conventionnelle ne semble possible qu'à un échelon régional, compte tenu du poids des différences de valeurs politiques et culturelles en la matière. Ce qui est applicable aux membres du Conseil de l'Europe ne l'est pas nécessairement ailleurs. C'est

(52) Pour une analyse de ce texte, voir Caprioli E., Sorieul R., "Le commerce international électronique : vers l'émergence de règles juridiques transnationales", *JDI* 1997-2, p.323-401.

(53) "Dimension internationale des réseaux et de l'Internet : les solutions", Lamy *Droit de l'informatique et des réseaux*, 1999, no 2341, p.1326.

pourquoi le rôle d'une organisation universelle de l'ONU ne peut être actuellement que limité.

Certains proposent la création d'une unique organisation internationale pour réguler Internet. Prenant exemple sur les réalisations en matière de droit de la haute mer, ils suggèrent la création d'une "Autorité internationale du cyberespace", dont la réglementation serait basée sur trois points : le cyberespace est un patrimoine commun de l'humanité ; seules les activités pacifiques y sont autorisées ; toute appropriation nationale de cet espace est interdite (54).

Toutefois, dans les faits, la tendance n'est pas à la réglementation par le droit international, ni à l'institutionnalisation. En effet, on insiste plutôt sur l'efficacité d'une auto-régulation du réseau par ses propres usagers. Les codes de conduite du type "Nétiquette" et les organisations d'internautes sont déjà extrêmement développés.

Ainsi, sur la question de la naissance d'un "tiers droit" en la matière, entre solutions nationales et internationales, on peut noter que "*le débat ressurgit périodiquement. Ainsi, à propos du développement de l'Internet, on évoque une lex electronica, par analogie avec la lex mercatoria. On emploie aussi l'idée d'autorégulation, d'un droit spontané. Face à la relative abstention des Etats, quelle qu'en soit la cause, on redécouvre la solution normative de la transnationalité*" (55). Le problème posé par ces normes d'origine privée est celui de leur statut, de leur reconnaissance et de leur application par les Etats : "*en d'autres termes, les règles ainsi créées sont-elles du droit international, ce qui renvoie à la question très classique de la subjectivité internationale des personnes privées et de leur capacité à participer à l'élaboration de règles de droit international*" (56).

Entre traités contraignants et une lex electronica basée sur les usages déontologiques, avec les inconvénients inhérents à la *soft law*, un équilibre doit être recherché. La solution pour une réglementation adéquate et efficace d'Internet passe probablement par un compromis entre les sources d'origine étatique (et le droit international public reste essentiellement d'origine étatique) et les sources privées.

(54) Lavenue J.J., "Cyberespace et droit international : pour un nouveau jus communicationis", *op. cit*., p.834s.
(55) Ruiz-Fabri H., "Immatériel, territorialité et droit", *op. cit*., p.201.
(56) *ibid*., p.202.

*"La régulation du net par les intéressés ne justifie nullement l'exclusion des Etats qui restent tout de même les premiers, sinon les seuls, à avoir l'investiture démocratique (dans les systèmes démocratiques, il est vrai) pour intervenir. Les expressions de « souveraineté des usagers » ou de « souveraineté des réseaux », pour brillantes qu'elles soient, ne sont pas recevables et recèlent même bien des dangers si elles devaient signifier qu'aucune instance ne serait fondée à imposer le respect de certaines valeurs…"* (57).

(57) "Dimension internationale des réseaux et de l'Internet : les solutions", *op. cit*., no 2351.