INSTITUT D'ETUDES POLITIQUES DE STRASBOURG

# Mémoire de recherche Diplôme Universitaire Sécurité intérieure/extérieure dans l'Union Européenne

## Les moyens juridiques et institutionnels nationaux et européens de lutte contre la cybercriminalité dans le cyberespace

**Clément ENDERLIN**

**[Année universitaire 2010/2011]**

*Je dédicace ce mémoire universitaire à Messieurs R. Doare Directeur du Centre de Recherche des Écoles de Saint-Cyr Coëtquidan, D. Danet directeur du pôle « Action globale et forces terrestres », et G. de Boisboissel ingénieur de recherche au Centre de Recherche des Écoles de Saint-Cyr Coëtquidan. Que ce mémoire puisse contribuer à élaborer une réflexion sur les enjeux de la cyberdéfense.*

La paternité du mot « cybernétique » revient à un professeur du Massachusetts Institute of Technology, Norbert Wiener, qui dans son ouvrage éponyme désigna sous ce vocable le « *champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal* ». Il l'a construit à partir du grec *Kuberneïn*, qui signifie « diriger ».

Peu à peu, le préfixe *cyber* va participer à la construction de nouveaux substantifs relatifs à cette société de l'information qui a vu le jour à la fin du XX$^{ième}$ siècle. La cybersécurité va donc concerner les usages défensifs et offensifs de ces systèmes d'informations qui irriguent nos organisations modernes. Elle prend en compte tant les contenants, c'est-à-dire les moyens techniques (réseaux informatiques, satellitaires, téléphoniques…) qui peuvent faire l'objet d'opérations d'infiltration, d'altération, de suspension voire d'interruption, que les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (sites internet, base de données, transactions dématérialisées…).

La cybersécurité porte aussi bien sur la protection de l'attaque d'équipements informatiques, afin de les surveiller ou d'en prendre le contrôle, que sur les renseignements disponibles sur la toile, avec de possibles atteintes à la réputation, le vol de données sensibles, des actions de piratage numérique…[1]

La difficulté à lutter contre la cybercriminalité tient dans un paradoxe : la mise en avant de la liberté d'expression et de circulation de l'information sur Internet et la nécessaire restriction de l'accès à Internet pour permettre une lutte efficace contre les cybermenaces. Par ailleurs, une autre difficulté réside dans la multiplicité des définitions du concept de cybercriminalité. Pour l'OCDE, la cybercriminalité consiste en tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique des données et/ou la transmission de données. Néanmoins, cette définition n'est pas pertinente, car l'approche morale de la lutte contre la fraude informatique comme constitutive d'un mode alternatif de règlement des conflits reste limitée. Selon le ministère Intérieur français, la cybercriminalité

[1] Arpagian N (2010) La cybersécurité, Paris, PUF, coll. Que sais-je ?

concerne « *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication en général, et en particulier sur les réseaux utilisant le protocole TCP-IP appelés communément l'Internet* ». Mais il n'est ici pas question des infractions commises sur les systèmes informatiques ni des infractions générées par le fonctionnement des réseaux informatiques. Pour sa part, l'ONU concerne comme cybercriminel, « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent* » ; et de manière générale « *tout fait illégal commis au moyen d'un système, d'un réseau informatique ou en relation avec un système informatique* ». Ici, l'ONU se réfère à la notion de « *comportement illégal* » pour définir la cybercriminalité, or chaque État défini différemment ce qu'est un comportement illégal[2].

Une difficulté supplémentaire tient dans la diversité des profils de cybercriminels. En effet, le cybercriminel ne constitue pas une catégorie d'individus clairement définie, et les motifs d'une attaque informatique sont aussi variés qu'il existe de types de cybercriminels. Par conséquent, l'image sociale du cybercriminel représenté et réduit à un expert en informatique travaillant seul depuis son ordinateur, vivant à l'écart de la société est partiellement fausse. Dans cette perspective la notion et le rôle de la représentation du cybercriminel est essentielle afin de mieux en cerner le phénomène et les moyens de lutter contre les attaques informatiques.

Une représentation sociale est un univers d'opinions propres à une culture, une classe sociale, ou un groupe et relatifs à des objets de l'environnement social. Une représentation sociale se présente comme un ensemble d'éléments cognitifs (opinions, informations, croyances…) relatifs à un objet social[3].

La première caractéristique de cet ensemble est d'être organisée. C'est-à-dire que les éléments qui constituent une représentation sociale entretiennent entre eux des relations. Plus exactement, les individus s'accordent à établir des liens entre ces divers éléments. La seconde est d'être partagée par les individus d'un même groupe

[2] Chawki M., Essai sur la notion de cybercriminalité, IEHEI, juillet 2006
[3] Moscovici (1961) La psychanalyse, son image et son public, Paris, PUF, coll. Bibliothèque de psychanalyse

social. La troisième est d'être un mode de construction : elle est collectivement produite à l'occasion d'un processus global de communication. Les échanges individuels et l'exposition aux communications de masse permettent aux membres d'un même groupe de mettre en commun les éléments qui constituent la représentation sociale. La quatrième et dernière caractéristique est sa finalité : elle est socialement utile. D'abord pour appréhender l'objet auquel elle se rapporte mais aussi pour intervenir dans les relations entre groupes.

Le cerveau humain est organisé pour traiter des informations absentes qui ne correspondent à aucune perception, ceci grâce à sa fonction anticipatrice. Par sa mémoire, l'homme peut revivre, à travers le récit, des événements anciens. Par conséquent hors du contexte social de la cyberdélinquance, un individu peut s'approprier n'importe quelle image du pirate informatique. Ces représentations mentales sont chez l'homme soit des images chargées émotionnellement puisqu'il se « re-présente » à d'autres intentionnellement dans la perspective d'une communication d'informations intellectuelles et/ou affectives qui ont une valeur dans l'échange social humain. Les représentations sociales telles que les préjugés, les stéréotypes, les idées reçues, sont des éléments constitutifs de la pensée commune qui participent au système de représentation avec lequel ils entretiennent des rapports de coexistence. Les images sont le résultat d'un processus de constructions mentales diverses de la représentation de l'objet[4].

Le concept de monde social renvoi à un réseau d'acteurs en interaction pour la construction d'un objet partagé. Chaque monde participe à la construction de l'image sociale du pirate informatique selon des codes, coutumes et besoin qui lui sont propres. On peut décrire trois mondes majeurs de la cyberdélinquance : le monde de la sécurité des systèmes informatiques, le monde des pirates informatiques, le monde médiatique. Ces trois mondes mobilisent de nombreux acteurs sociaux, qui coopèrent ou non, utilisent ou non des procédures conventionnelles au sein d'un ensemble de réseaux, constitutifs des mondes de la cyberdélinquance. Ces mondes génèrent des significations spécifiques formalisant une image singulière du pirate informatique, chaque monde forgeant une catégorisation particulière de ces acteurs

[4] Mannoni P (2010) Les représentations sociales, PUF Que sais-je ?

sociaux. Dans cette perspective, les événements de type « underground » permettent de rencontrer des personnages actifs « on-line ». L'absence de rencontre et d'amplifications au cœur du monde « underground » peut permettre l'émergence de la pensée vulgaire, entraînant la formalisation d'une image du cyber crime et de ses acteurs principaux en décalage avec la réalité des faits et des significations du monde concerné. Par conséquent, ce qu'on appelle le cybercrime ne peut être résumé à une perception subjective objectivée, cette notion posant la question de la connaissance.

La construction sociale du cybercrime est aussi le fait de la construction d'une image par un individu dans un champ donné (un monde social donné). La connaissance du cybercrime découlera de la prise en compte de plusieurs images, *via* l'ensemble des mondes sociaux de la cyberdélinquance concernés. La cyberdélinquance est un objet social construit qui apparaît comme structurant pour la formalisation des images sociales de la cyberdélinquance. L'absence de mise en relation directe du citoyen avec le pirate informatique va engendrer la production d'une image sociale relative à ce dernier ; avec l'association de valeurs particulières, cela en interdépendance avec l'objet social représenté de la cyberdélinquance. L'objet social « pirate informatique » n'existe pas mais plutôt des images de celui-ci.

Par conséquent, la définition du « pirate informatique » dépend donc de la représentation sociale de la cyberdélinquance qui est à la base de la production d'images sociales de ce dernier ; elle dépend également du contexte social associé alimentant la production même de ces images sociales. La construction de cet objet de recherche est en interdépendance avec ces deux éléments structurants[5].

Dès lors, nous pouvons affirmer qu'il n'existe pas un type de cybercriminels mais une pluralité de profils. Une première typologie[6] permet de différencier les cybercriminels selon qu'ils souhaitent obtenir un capital financier, détruire l'infrastructure d'une entreprise ou d'une organisation, ou recherche l'aspect ludique, le défi technique.

[5] Breton P (2004) L'interactionnisme symbolique, Paris, PUF, coll. Manuel
[6] Rosé P La criminalité informatique, Paris, QSJ ?, PUF

Une seconde typologie[7] permet de répartir les cybercriminels selon qu'ils recherchent une reconnaissance sociale, un gain financier, un sens à la réalité vécue, la défense d'une idéologie.

En conclusion, face à la difficulté d'appréhender la notion de cybercriminalité et de cybercriminel nous nous référerons à la définition posée par la **convention internationale de la cybercriminalité** adoptée par le Conseil de l'Europe à Bucarest le **23 novembre 2001**, qui constitue aujourd'hui le texte international le plus précis et le plus ambitieux en termes de répression des actes cybercriminels. La convention répertorie quatre catégories d'infractions : (i) les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes (accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs) ; (ii) les infractions informatiques (falsification et fraudes informatiques) ; (iii) les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. Un protocole additionnel du **7 novembre 2002** vise spécifiquement le racisme et la xénophobie sur Internet par la criminalisation de la diffusion de matériel raciste et xénophobe *via* les systèmes informatiques, ainsi que les menaces et insultes racistes, le négationnisme, le révisionnisme ou la justification des crimes contre l'humanité. La France a ratifié la convention de 2001 et son protocole additionnel par une loi promulguée le **19 mai 2005**[8]. C'est selon cette définition que seront abordés les dispositifs législatifs ainsi que les moyens de coopération en matière de lutte contre la cybercriminalité.

Si la répression de la fraude informatique a fait l'objet de nombreuses dispositions pénales en droit interne français et si de nombreux textes répriment la criminalité informatique, il n'en demeure pas moins que le nombre d'affaires qui y sont liées est en constante augmentation.

Le développement rapide de la criminalité informatique constitue un fait marquant qui s'explique, notamment, par la multiplication des systèmes informatiques connectés à des réseaux ouverts, tel l'Internet, et par la difficulté d'identification des auteurs

[7] Bologna G.-J An Organizationnal Perspective on Enhancing Computer Security, *in* Martin D (1997). La criminalité informatique, Paris, PUF, p. 68

[8] L. n°2005-493, 19 mai 2005, autorisant l'approbati on de la convention sur la cybercriminalité et du protocole additionnel à cette convention, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, *JO* 20 mai, p. 8729

d'infractions, compte tenu de la dimension mondiale du réseau dont l'une des caractéristiques les plus marquantes est d'être « déterritorialisée».

L'éclosion d'une cybercivilisation qui repousse les frontières de notre espace habituel pose de nouveaux problèmes d'une acuité particulière puisque les actes délictueux sont perpétrés par des individus qui résident dans un pays différent de celui où sont portées les atteintes aux systèmes informatiques. On assiste à l'émergence d'une criminalité planétaire.
En effet, la fluidité des systèmes d'information a aboli les frontières physiques et permet de mener des opérations criminelles à une échelle mondiale. Par exemple, le FBI a procédé le 16 octobre 2008, à la fermeture d'une plate-forme de recel de données informatiques volées. Baptisé « Dark market », ce forum mettait à la disposition de ses clients répartis sur toute la planète des informations bancaires captés frauduleusement via l'interface du web.

De même, au début du mois de mai 2000, le virus « I Love You» a été diffusé aux quatre coins de la planète et a provoqué, en quelques heures, des dégâts estimés à 4,7 milliards de dollars, selon le cabinet Computer Economics, sachant, qu'en 1999, le préjudice total lié à la cybercriminalité a été estimé par le Clusif à douze milliards de francs. Quant aux auteurs de cet acte de cyber terrorisme, les suspects arrêtés aux Philippines, peu après le début de l'attaque, devaient être relâchés, faute de preuve, alors que dans le même temps, de nouvelles variantes du célèbre virus apparaissaient aux quatre coins de la planète.

Qu'il s'agisse de fraude, de détournement de fonds ou d'extorsion, la difficulté ne réside pas tant dans la qualification de la faute que dans son caractère mondial qui rend toute opération de police particulièrement complexe. Ce n'est donc pas tant la règle de droit qui est défaillante que les moyens d'appréhender le coupable.

La criminalité informatique est, de par sa nature, fondée sur la technologie et, par conséquent, exige une compréhension et une maîtrise de celle-ci pour que les enquêtes et poursuites judiciaires soient efficaces. De plus, ce type de criminalité présente une menace « asymétrique » permettant aux criminels d'atteindre un

nombre de victimes importants et de causer des dégâts à grande échelle, avec un investissement modeste en termes de ressources et de savoir-faire.

Par ailleurs, la criminalité informatique n'a souvent pas de frontières juridiques : les attaques impliquent de nombreuses juridictions nationales et internationales. Cette absence de juridiction unique a des conséquences sur l'efficacité des enquêtes et des poursuites judiciaires. De surcroît, la nature transfrontalière de cette criminalité rend difficile la désignation d'un coupable en raison des difficultés techniques du traçage des manœuvres électroniques et du caractère éphémère des preuves électroniques.

Cette précision éclaire une préoccupation contemporaine parallèle à la hausse croissante de la cybercriminalité : le contrôle ou à défaut, la réglementation du cyberespace. Plusieurs gouvernements se sont préoccupés de la réalité du cyberespace en émergence, car ils la considèrent comme une menace pour leur souveraineté.

Le cyberespace est le terme forgé par le romancier William Gibson dans son ouvrage *Neuromancer* pour décrire un lieu dépourvu de murs au sens concret du terme, voir de dimensions physiques, où les données mondiales sont structurées sous la forme d'un support visuel et traversable. Ce type de cyberespace n'existe pas et ne peut exister actuellement. Dans le monde réel le cyberespace est l'endroit ou des conversations téléphoniques ordinaires ont lieu, où le courrier électronique vocal est les messages électroniques textes sont stockés et échangés…

Le cyberespace peut être défini comme l'espace où se produit l'interaction entre des entités électroniques. En d'autres termes, les acteurs du monde numérique ont besoin d'un espace électronique pour fonctionner[9].

« *Les espaces littéraires sont des espaces entièrement créés à l'aide de mots. Les débats publics sur l'Internet forment un genre d'espace car les conversations où*

[9] Balsano A. (2000) Un instrument juridique international pour le cyberespace ? Une analyse comparative avec le droit de l'espace *in* Les dimensions internationales du droit du cyberespace (2000), Economica, coll. Droit du cyberespace

*intervient un groupe de personnes ne pourraient autrement avoir lieu que dans une pièce réelle. Ce type d'espace littéraire est celui qui est le plus développé sur l'Internet. À l'autre extrême de l'espace littéraire, il y a l'espace architecturale, l'espace électronique perçu comme un véritable espace en quatre dimensions*[10] ». Il n'y a donc pas un seul cyberespace mais il y a beaucoup de cyberespaces avec un nombre quelconque de modèles tirés du monde réel et reproduits par le biais d'une communication informatisée. En outre, le nouveau monde de l'Internet offre de nouvelles cyber communautés qui tentent d'établir des cyber règles et une cyber éthique.

L'essor des réseaux informatiques mondiaux affaiblit le lien qui existe entre un lieu géographique donné, le pouvoir d'un gouvernement national d'exercer un contrôle sur les comportements en ligne et les conséquences qui en découlent pour des particuliers ou des entités. Il met également en évidence certaines questions touchant à la légitimité des efforts tentés par un État nation souverain pour faire respecter des règles applicables à un phénomène mondial et à la capacité d'une entité régulatrice à notifier l'ensemble des règles à appliquer.

En effet, l'incidence du cyberespace sur le pouvoir souverain des États revêt un intérêt particulier. En principe, les gouvernements ont le pouvoir d'exercer leur pouvoir normatif et de coercition sur les activités qui ont lieu dans les limites de leur territoire. L'exercice du pouvoir souverain d'un État dépend dans une certaine mesure de sa capacité à s'engager à l'intérieur de ses frontières. Or, le cyberespace remet en cause non seulement le concept de frontière, mais également la légitimité de l'adoption de règlements destinés à régir des relations à l'intérieur d'un espace numérique, et applicables sur la base de juridictions géographiquement définies[11].

Le cyberespace est essentiellement l'objet d'attentions en raison du potentiel de développement économique qu'il représente ainsi que pour les menaces qu'il recèle. Les dépendances et vulnérabilités développées vis-à-vis du cyberespace par

[10] Tribe L The Constitution in Cyberspace : Law and Liberty beyond the Electronic Frontier, Harvard University Press, Cambridge, MA, 1991
[11] Balsano A. (2000) Un instrument juridique international pour le cyberespace ? Une analyse comparative avec le droit de l'espace *in* Les dimensions internationales du droit du cyberespace (2000), Economica, coll. Droit du cyberespace pp. 159-185

nos sociétés contemporaines sont la cause de l'importance stratégique de cet espace pour la sécurité et la défense nationale. Ce dernier est d'ores et déjà considéré comme un espace d'opérations à part entière au même titre que l'air, la terre et la mer. Le cyberespace s'en distingue néanmoins, notamment, par l'impossibilité d'identifier incontestablement les acteurs sur les réseaux et de séparer activités économiques et de sécurité. Une approche globale doit donc être adoptée pour développer et sécuriser cet espace[12].

Le potentiel de développement du cyberespace est encore important : la convergence des services sur des supports mobiles et l'Internet des objets – qui permet par l'utilisation de systèmes d'identification électronique et des dispositifs sans fil de connecter tout objet à l'Internet et ainsi pouvoir en exploiter les données – augmenteront encore la dépendance vis-à-vis du cyberespace. Ce développement constitue à la fois un enjeu économique majeur et une vulnérabilité pour la sécurité nationale. Les infrastructures des secteurs d'activité d'importance vitale (énergie, eau, transport…) dépendent également du cyberespace. Celles-ci sont en effet surveillées et pilotées par des systèmes appelés *SCADA* (*Supervisory Control and Data Acquisition*) qui sont désormais de plus en plus connectés et utilisent des éléments informatiques du grand public. L'impact social du cyberespace est par ailleurs considérable, l'e-administration, les échanges de courriels et l'essor des réseaux sociaux le démontrent. Toute défaillance des systèmes ou réseaux qui soutiennent ces services provoque des perturbations majeures.

Plus déterminantes pour la prise de conscience de l'acuité des menaces et de l'importance stratégique du cyberespace furent les attaques en Estonie en avril 2007, puis en Géorgie en août 2008. Ces crises ont mis en évidence les effets perturbateurs majeurs causés par des cyberattaques dans une société fortement dépendante du cyberespace, ainsi que l'implication d'acteurs non étatiques dans ce nouveau type de conflit. Il est très difficile d'identifier avec exactitude le véritable auteur de l'attaque ou d'actes d'espionnage. Ce dernier parvient à se camoufler grâce à des techniques sophistiquées et, étant situé à grande distance de sa cible, peut bénéficier d'une protection de l'État depuis lequel il opère. L'implication des

[12] Maupeou S., Cybercriminalité, cyberconflits, Revue Défense nationale et sécurité collective, Mars 2009

services étatiques d'un pays, est très délicate à prouver. Il en résulte que toute approche de dissuasion classique par représailles est inadaptée.

Une autre caractéristique consiste en l'incertitude qui entoure les effets d'une cyberattaque. Les dommages collatéraux sont extrêmement probables Le virus *Stuxnet* a ainsi atteint en septembre 2010 plusieurs millions d'ordinateurs en Iran, en Chine, et aussi en Inde, au Pakistan et en Indonésie. La séparation entre cibles d'intérêts militaires et civils est donc particulièrement difficile. L'interconnexion des réseaux informatiques à l'échelle mondiale et l'interdépendance des économies des pays développés sont telles, qu'il est possible qu'un État soit un des premiers à souffrir d'une attaque qu'il à lui-même lancée[13].

Économie numérique et sécurité des systèmes d'information sont interdépendants. La première a besoin de la seconde pour être performante mais inversement, il est illusoire d'envisager de sécuriser ses systèmes d'information sans acquérir une position renforcée et stable dans les domaines de l'industrie du logiciel, des équipements réseaux ou des services en ligne qui représentent des sources importantes de failles de sécurité. Sécuriser le cyberespace signifie également pouvoir influer sur la définition des normes de l'Internet du futur et sur sa gouvernance. Il faut promouvoir la coopération internationale par le biais d'échanges de compétences et d'informations (failles de sécurité, techniques d'attaques utilisées…) par la mise en place de systèmes de détection et d'alerte interopérables ou encore par l'organisation d'exercices conjoints. L'OTAN propose de telles possibilités avec, par exemple, le centre d'excellence en matière de cyber défense créé à Tallin en 2008 (*Cooperative Cyber Defense Center of Excellence*), ou encore avec les exercices « Cyber coalition ». L'OTAN développe également une capacité d'assistance à un pays victime d'une attaque la mise d'équipes d'intervention rapide (*Rapid Reinforcement Teams*). L'Alliance prône néanmoins la mise en place d'un réseau de centres nationaux d'alerte et de réaction (*Computer Emergency Team-CERTI)* afin d'améliorer l'efficacité de la lutte contre les cybermenaces. Il est donc

[13] De Maupeou S., World War Web 3.0 : l'informatique dans les conflits, Revue Défense Nationale, Mars 2010

clair que la cyberdéfense de l'Alliance atlantique est largement tributaire de l'implication de chacun des États membres[14].
Pour conclure ce point consacré à la mise en perspective des enjeux liés à l'essor du cyberespace, il faut préciser que ce mémoire sera moins consacré à l'analyse du cyberespace en temps qu'environnement numérique à part entière, qu'à l'étude de la cybercriminalité à travers ses aspects juridiques et économiques et au regard de son potentiel de développement au sein du cyberespace.

Ce faisant, aujourd'hui est-ce que le cadre tant normatif que celui de la coopération institutionnelle national et européen est suffisant pour sanctionner les comportements cybercriminels, et agir efficacement dans le cyberespace ?

Cette étude suppose initialement de rappeler le cadre normatif national et européen de lutte contre la cybercriminalité (1) puis d'en envisager les instruments de coopération (2) avant d'analyser plus précisément les enjeux contemporains de maîtrise du cyberespace, et les actions prises par différents États en ce sens (3).

[14] Vincent S. Cyberespace : pour une stratégie globale, Revue Défense nationale, juin 2011

# LE CADRE NORMATIF NATIONAL ET EUROPEEN DE LUTTE CONTRE LA CYBERCRIMINALITE

## 1 La diversité des infractions cybercriminelles suppose un dispositif normatif diversifié et souple

### 1.1 La protection des données personnelles selon une perspective économique et juridique

#### 1.1.1 La protection des données personnelles selon une approche économique : une appréhension complexe et plurielle

##### *1.1.1.1 La définition économique des données personnelles*[15]

Dès lors qu'ils transitent ou utilisent un réseau numérique, les échanges marchands ou non marchand se doublent d'échanges d'informations personnelles, enregistrées par l'une des parties avec l'accord ou non de son émetteur. Les données personnelles constituent donc des données spécifiques enregistrées sur un support numérique combinées aux caractéristiques individuelles des personnes identifiées.
Le support des données personnelles est durable : une information ne se détruit pas par l'usage mais se reproduit à l'infini. Mais l'information est périssable : les caractéristiques d'une personne peuvent changer au cours du temps, sans que les supports de cette information soient actualisés.

La durabilité associée à la reproductibilité parfaite des supports des données personnelles fait qu'elles sont non rivales : les partager ne privent pas leur détenteur du bénéfice de leur utilisation, ni n'empêche un acquéreur de les vendre à son tour. Le caractère « excluable » vis-à-vis d'utilisateurs potentiels est coûteux à mettre en œuvre pour les personnes concernées par l'échange de leurs données. La

[15] Rochelandet F. (2010) Économie des données personnelles et de la vie privée, Paris, La découverte, coll. Repères

vérification des utilisations par les uns et leur certification par les autres sont des activités coûteuses aux effets incertains.

Par conséquent, l'utilisation des données personnelles est marquée par des asymétries informationnelles entre les individus et les exploitants. Dans certains cas, lorsqu'il divulgue ses données, l'intéressé est le seul à pouvoir certifier de la véracité des informations transmises, ainsi que leur évolution et leur qualité au cours du temps.

Par exemple, les consommateurs sont les seuls à connaître leur disposition à payer ; les assurés, leur niveau de précaution…de telles asymétries défavorables aux entreprises ont des incidences sur la qualité des données personnelles collectées et affectent le fonctionnement du marché. De plus, la valeur marchande d'une base de données recensant des données personnelles variera en fonction de la stratégie des individus lorsqu'ils divulgueront leurs informations, de l'acceptabilité du système de collecte…

Néanmoins, la situation d'asymétrie informationnelle joue fréquemment dans le sens inverse. Ce sont les consommateurs qui, le plus souvent, ne savent pas quelles sont les données qui sont collectées, leur usage, le niveau de protection qui est garanti…En outre, lorsqu'elles sont collectées à l'insu de son propriétaire (traces de navigation laissée sur le navigateur) ses données personnelles peuvent refléter plus ou moins fidèlement son comportement réel.

Ces asymétries sont d'autant plus fortes qu'elles se reproduisent à tous les stades de la chaîne d'exploitation : un individu a encore moins le contrôle sur les utilisations secondaires de ses données personnelles (suite à leur transfert d'un exploitant à l'autre) et, de ce fait, il peut subir des externalités négatives suite à chaque transaction portant sur ces informations. En parallèle, l'exploitant initial ne peut pas connaître le comportement des exploitants secondaires.

Enfin, si les techniques d'exclusion *ex ante* existent afin d'empêcher la collecte ou le transfert de données, elles ne permettent pas de contrôler *ex post* leur traitement.

Par ailleurs, les données personnelles présentent un coût de production supérieur à leur coût d'exploitation. La collecte des données primaires supposent la mise en place de système de collecte spécifiques : système de saisie des données, formulaires en ligne…tandis que le transfert de données est relativement aisé.
Or, ceci peut aboutir à leur exploitation excessive : la perspective de revenus supplémentaires obtenus avec le même niveau de coûts fixes de collecte crée une incitation excessive à la revente des données personnelles, au détriment des individus auprès de qui les données sont prélevées. Les revendeurs n'intériorisent *a priori* pas le coût externe lié à leur activité de revente : les exploitants subséquents peuvent en effet faire subir des nuisances aux personnes sans que les revendeurs en supportent les coûts eux-mêmes.

Stigler rejette l'éventualité d'une telle défaillance de marché car selon lui, la dissémination des données personnelles se heurterait en fait à des coûts spécifiques liés à leur traitement et notamment à la détermination des informations pertinentes au regard de l'utilisation prévue. Ces coûts conduiraient à une limitation naturelle de la demande d'informations qui se fixerait au minimum nécessaire pour protéger les intérêts de la partie sous-informée. Passé un seuil le coût marginal de collecte des données serait supérieur au bénéfice marginal de leur utilisation. De surcroît une demande excessive de données personnelles réduirait la disposition des individus à satisfaire à une telle demande. La demande de données personnelles se limiterait ainsi au niveau nécessaire pour satisfaire les intérêts de chacun.

Pour autant cet argument est tout relatif. La collecte de certaines données suppose un investissement spécifique lié soit à l'utilisation que l'on souhaite en faire (cas de la prospection directe) ou de la qualité des données qui suppose alors un coût supplémentaire pour les protéger contre la perte ou le vol.

Par conséquent et plus généralement, l'école de Chicago sous-estime les externalités directes engendrées par l'exploitation des données personnelles et néglige les externalités indirectes subies par les personnes. Or, ces deux types d'externalités peuvent justifier des solutions correctrices comme la protection légale des données personnelles.

#### 1.1.1.2 *L'analyse économique de l'exploitation des données personnelles au regard du concept d'externalité*

Le concept d'externalité permet de formaliser le cas où un agent voit son utilité diminuer du fait de l'abstention/l'action économique d'un autre agent, alors que cet effet n'est pas pris en compte par les mécanismes de marché. En l'occurrence, l'exploitation des données personnelles engendre des bénéfices pour la firme qui, en première analyse, ne supporte que les coûts privés de son activité et non les coûts reportés sur les individus à l'origine de ces ressources informationnelles.

Symétriquement, une autre manière d'envisager l'exploitation des données personnelles consiste à se placer du côté de l'exploitant. Les activités des individus à partir desquelles sont produites les données personnelles sont une source d'externalités positives pour la firme. La consommation d'un service par un agent lui procure du plaisir, mais également à l'agent qui exploite les données ainsi collectées. Ce bénéfice externe constitue une externalité positive lorsque l'exploitant des données personnelles tire des bénéfices nets de leur exploitation.

L'existence d'externalités positives peut inciter les consommateurs à limiter leurs activités dès lors qu'ils ont connaissance des bénéfices d'une telle collecte et qu'ils ne perçoivent aucune contrepartie. Si l'on retient une analyse en termes d'externalités négatives, l'exploitation des données personnelles peut affecter le bien-être des émetteurs de données personnelles en leur infligeant des nuisances (spamming). L'exploitant quant à lui ne supporte que des coûts privés liés à la collecte des données.

Il faut aussi préciser que l'incitation de l'entreprise à ne pas outrepasser ses engagements en termes d'exploitation des données personnelles est garantie par la dissuasion d'une sanction légale, mais également par un effet de réputation.

Aussi, toute mesure augmentant les coûts de marketing peut inciter les entreprises à cibler au mieux leur stratégie de marketing direct. La protection des données personnelles peut donc jouer un rôle équivalent à celui d'une taxe environnementale visant à limiter la surexploitation d'une ressource. En l'occurrence, un renforcement

de la *privacy* par l'établissement d'une taxe sur les sollicitations, en augmentant les coûts de la communication des messages et de la sollicitation, pourrait améliorer le bien-être des consommateurs et obliger les entreprises à spécialiser leur stratégie marketing en sélectionnant mieux leur cible et donc en augmentant l'efficacité des messages en termes de réception et de réactions aux messages par les consommateurs. À l'inverse, une restriction légale en matière de collecte des données personnelles limiterait la capacité des vendeurs à définir une stratégie efficace de prospection.

Ce faisant, la politique de protection des données personnelles présente un ensemble d'objectifs contradictoires. Pour réduire le coût externe lié à la collecte et à l'exploitation des données, les vendeurs devraient disposer d'un grand nombre d'informations personnelles afin de cibler au mieux leur message et leur public. En contrepartie, les individus devraient disposer d'un contrôle plus efficace sur leurs données personnelles pour être en mesure de décider ce qu'ils souhaitent diffuser ou non, c'est-à-dire leur permettre d'opérer le meilleur arbitrage possible.

#### *1.1.1.3 Règlementation, corégulation ou laissez-faire : une approche comparative des outils normatifs de protection des données personnelles*

L'exploitation des données personnelles peut être à la source d'externalités négatives, pour autant cela justifie-t'il une intervention publique correctrice, et le cas échéant, jusqu'à quel degré et sous quelles formes ?

La protection des données personnelles est une question complexe car, d'un côté les méthodes de collecte et d'exploitation des données personnelles sont polymorphes et évolutives et, de l'autre, les individus ont eux-mêmes des stratégies propres de protection de leurs données personnelles. Il apparaît alors complexe de parvenir à définir un cadre uniforme qui régule l'ensemble des situations dans lesquelles les données sont collectées et exploitées.

##### 1.1.1.3.1 Les solutions institutionnelles existantes

#### *1.1.1.3.1.1 Marché ou gouvernement : quelle solution optimale ?*

La régulation par le marché consiste à ne soumettre les entreprises à aucune contrainte légale, sinon le droit commun. Les incitations marchandes sont considérées comme suffisamment fortes pour empêcher les firmes d'exploiter les données personnelles d'une manière socialement inacceptable et à respecter leurs engagements en matière de vie privée.

La *privacy* devient un élément de marketing et de différenciation entre les firmes, ce qui peut enclencher un processus de concurrence vers le haut. À terme, toutes les entreprises s'engageraient dans une démarche de protection des données personnelles élevée. L'efficacité de cette pression dépend de la publicité qui est faite des entreprises vertueuses tant par les médias que par les consommateurs *via* les forums, réseaux sociaux…

Cependant, une régulation par le marché, souffre de défaillances majeures. En admettant que la pression du marché incite les entreprises à adopter des politiques pro-*privacy*, il n'en subsiste pas moins que des coûts d'information et de négociation. D'une part, l'entreprise bénéficie d'asymétries informationnelles *via* une meilleure connaissance juridique et technique, et d'autre part, les consommateurs subissent un coût d'information élevé à travers la lecture de charte de confidentialité complexe, ainsi que des coûts de surveillance du respect des engagements. Face à la faible probabilité d'être sanctionnée par le consommateur, les entreprises peuvent rédiger des chartes de confidentialité rigoureuses pour se différencier sur le marché et bénéficier ainsi d'une rente.

Se pose également le problème des entreprises pour lesquelles la dimension de réputation importe peu, comme les *spammer.* En effet, dans le cadre du spamming il suffit de 0, 001% de clients satisfaits pour rentabiliser l'activité.

À l'inverse, dans un environnement réglementé, l'État détermine les conditions de collecte et d'exploitation des données personnelles. Le coût de mise en œuvre

des dispositifs légaux est donc supporté par les firmes, et le niveau de protection est corrélé par le niveau de sanction.
L'effet dissuasif repose sur le pouvoir de coercition de l'État qui doit arbitrer entre le niveau de sanction et la probabilité de détection de l'acte illégal afin de minimiser le coût social de la protection et d'obtenir un niveau d'incitation optimal. Cependant, l'intervention publique souffre de plusieurs défaillances. D'abord, elle engendre des coûts administratifs de mise en œuvre et de contrôle de la norme. Ensuite, elle créé des coûts supplémentaires pour les entreprises qui doivent rédiger et afficher leur politique de confidentialité et assurer l'accès des citoyens à leurs droits en matière de collecte et de traitement de leurs données personnelles. Enfin, il existe un risque d'inadéquation entre la règlementation et les mesures prises pour la respecter.

#### 1.1.1.3.2 Les solutions intermédiaires

##### *1.1.1.3.2.1 L'autorégulation : la protection des données personnelles par les industriels*

Dans cette perspective, un label certifierait les entreprises qui s'engagent dans une démarche de protection des données personnelles. Une telle procédure permettrait d'instituer une relation de confiance entre les entreprises et les consommateurs.

La production en interne de normes de labellisation permettrait une plus grande adhésion des professionnels et une plus grande facilité d'application. De même, il serait plus aisé de standardiser ces règles et ainsi de réduire les coûts d'information supportés par les individus en cas de laissez-faire.

Cependant, l'autorégulation a des inconvénients majeurs. Elle repose sur la logique de l'action collective, donc plus la « communauté » de professionnels est importante plus le coût de la tricherie est réparti sur toute l'industrie, et plus les coûts de détection de la violation augmentent. Elles bénéficient ainsi autant de la réputation collective que du gain de la tricherie.

De plus, la rédaction des règles par des professionnels serait établit selon une logique de cartel. Dès lors que l'édiction de règles protectrices des données

personnelles augmente les coûts pour les entreprises, il n'y a pas forcément convergence entre les intérêts des consommateurs et des entreprises. De ce fait, une entente sur les règles aboutirait une protection sous-optimale du point de vue des individus, et ce d'autant plus que la société civile est exclue du processus de rédaction. Quant à la régulation publique, le *lobbying* des associations de protection des libertés individuelles influencera sur la rédaction des règles.

#### *1.1.1.3.2.2 Que l'acheteur soit vigilant*

Dans ce cas, les entreprises ne sont pas toutes obligées de définir les mêmes pratiques en matière de protection des données personnelles, mais elles doivent respecter les engagements prévus dans leur politique de confidentialité. La régulation publique intervient ici pour assurer le respect par les firmes de leurs engagements respectifs.

Ici, les consommateurs subissent des asymétries informationnelles importantes couplées à des coûts de recherche d'informations en raison de la diversité des politiques de confidentialité. Ces asymétries ne sont corrigées par aucun mécanisme contraignant les firmes à harmoniser leur politique. Toutes peuvent rédiger une charte de confidentialité mais, dans les faits, ne pas la respecter en bénéficiant de coûts élevés de détection.

#### *1.1.1.3.2.3 La labellisation*

L'adhésion à des labels permet de renforcer la confiance des consommateurs vis-à-vis des firmes car à chaque label correspond la garantie du respect d'un ensemble de règles relatives à la protection des données personnelles. Cette pratique vise également à réduire les coûts d'information des consommateurs en leur envoyant un signal crédible sur les coûts que les adhérents supportent pour protéger les données personnelles.

Toutefois, l'apposition d'un label ne garantit pas aux consommateurs du respect par l'entreprise de ses engagements. De ce fait, devant l'impossibilité pour les entreprises de diffuser la qualité de leur politique de confidentialité de manière

crédible, les entreprises n'ont pas d'incitation ni d'intérêt à respecter leur politique de confidentialité, au regard de celles qui violent les principes fixés par les labels tout en bénéficiant de ses avantages.

Les labels de certification peuvent également conduire à une forme de sélection adverse : les entreprises qui jouissent d'une bonne réputation en terme de protection de données personnelles n'ont pas besoin d'adhérer à un label ; alors que les entreprises les plus malveillantes ont intérêt à obtenir une certification.

Cette défaillance dans l'utilisation des labels pourrait justifier l'adjonction de mesures règlementaires tendant, par exemple, à diffuser sur le nombre de plaintes et de condamnations reçues par les sites audités par les entreprises de certification.

Pour autant dans ce cadre, qui contrôlerait le certificateur privé ? Plus il détecte de fraudes plus il acquiert de réputation auprès des consommateurs mais moins il a de clients. Ce faisant, cela plaiderait pour la mise en place d'un certificateur public.

#### 1.1.1.3.3 L'attribution de droits de propriété aux individus : une opportunité ?

Dans les différents scénarii envisagés il n'est pas prévu que le consommateur détienne un droit sur l'utilisation qui est faite de ses données. Certes, la règlementation nationale prévoit un ensemble de droits à destination des citoyens, mais dans la pratique ces droits sont soit méconnus soit pas/peu utilisés en raison de la complexité de leur mise en œuvre. En effet, les citoyens peuvent refuser de communiquer certaines données rendant ainsi impossible la collecte de données lorsqu'elle est autorisée, mais ils ne peuvent s'opposer à leur exploitation si celle-ci est légale.

Face à cette situation, faut-il préconiser l'octroi aux individus de droits de propriété sur leurs données personnelles pour leur permettre de les « gérer » comme tout élément de leur patrimoine, et notamment de percevoir une rémunération en contrepartie de leur exploitation marchande ?

#### *1.1.1.3.3.1 L'octroi de droits inaliénables fondés sur l'opt-in*

Une première approche considère les TIC comme particulièrement intrusifs justifiant une règlementation forte fondée sur l'*opt-in* : il faut obtenir le consentement des particuliers pour exploiter leurs données personnelles. Cela se justifierait d'autant que l'option inverse – l'*opt-out* (accord tacite) – entraîne des coûts de revirements élevés. Cependant, l'*opt-in* engage des coûts de négociation important liés à la nécessité d'obtenir l'accord de l'ensemble des personnes pour lesquelles ont souhaite exploiter les données.

#### *1.1.1.3.3.2 L'octroi de droits de propriété librement négociables*

Ici les droits de propriété sont accordés selon une logique marchande. En effet, si elles sont la plupart librement négociées, ces ressources sont sous-évaluées, ce qui expliquerait qu'elles soient surexploitées. Conférer des droits de propriété aux individus les inciterait à les valoriser en adoptant des protections techniques appropriées, et par ce biais, les mettrait en position de force sur le marché.
Des droits de propriété s'appuyant sur des moyens techniques facilitateurs de transactions permettraient aux individus d'être compensés, au moins partiellement, pour l'exploitation de leurs données personnelles.

Cependant, l'octroi automatique de droits de propriété aux individus ne résout toujours pas la question du coût de gestion et de surveillance des utilisations des données personnelles.

### 1.1.1.3.4 L'organisation d'un marché des données personnelles

Dans un monde d'information parfaite, la flexibilité dans la négociation et la contractualisation rendrait superflue la protection légale des données personnelles.
Ce qui suppose des conditions d'application restrictives, des droits de propriété clairement définis, une information mutuelle parfaite sur les intentions des autres et des coûts de transaction nuls.

Varian (1996) promeut l'échange marchand des données personnelles sous la forme d'un système de location/prêt pour certains types d'exploitation décidées et acceptées par l'individu « propriétaire » de ses données personnelles. Une telle solution serait en phase avec le comportement des individus qui préfèrent communiquer certaines données et garder le secret pour d'autres.

Par exemple :

Soit un vendeur de pommes de différentes variétés et un consommateur dont la disposition à payer maximale pour une variété est de 5€ et pour les autres de 0€. Le client est prêt à révéler sa préférence mais non sa disposition à payer pour conserver son surplus en cas d'achat. Le partage de données personnelles accroît l'efficience de l'échange en réduisant les coûts d'information : éviter au vendeur d'énumérer toutes les variétés et en proposer une qui ne correspond pas à la préférence de l'acheteur.

Laudron (1996) préconise un système où les données personnelles seraient agrégées en paquets loués sur un marché public, ouvert à tous les exploitants potentiels. Tout individu ayant des caractéristiques données pourrait ainsi fournir ces informations à un infomédiaire qui les agrégerait avec les données personnelles d'autres individus aux caractéristiques similaires. Chaque groupe obtenu serait alors associé à un descriptif précis. Les entreprises désirant proposer des offres au groupe défini selon tels ou tels critères achèteraient les droits d'utilisation des listes de contacts correspondantes pour une durée limitée. Les individus recevraient ensuite un pourcentage des revenus générés, une forme de dividende avec une option de sortie (*opt-out*) s'ils considèrent que la gêne occasionnée est insuffisamment compensée par le revenu perçu.

Cette solution agrégative présente l'avantage d'éviter les coûts de transaction prohibitifs tout en préservant les avantages – augmenter la quantité d'informations disponibles sur le marché et créer un gain mutuel – et en permettant aux individus d'arbitrer entre les bénéfices de divulguer leurs données personnelles et les coûts d'opportunité de les maintenir secrètes préservant ainsi leur anonymat.

#### 1.1.1.3.5 Les limites de l'approche par les droits de propriété

La reconnaissance de droits de propriété aux individus sur leurs données personnelles permettrait une allocation efficiente des ressources *via* la compensation ainsi obtenue et l'incitation à adopter des comportements socialement optimaux (éviter l'exploitation excessive et la divulgation d'informations erronées).

##### *1.1.1.3.5.1 La définition du « droit de propriété »*

Le principe des droits de propriété, au sens économique du terme, n'équivalent en rien à un droit de possession : il n'autorise pas les individus empêcher la collecte et l'exploitation licite de leurs données personnelles. D'où l'importance de préciser les prérogatives reconnues à travers l'appellation de « droit de propriété » :

- Un droit de possession classique ? La théorie des droits de propriété justifie l'octroi de droits clairement définis, exclusifs, et librement transférables afin de permettre l'allocation efficiente des ressources rares. Or l'octroi de tels droits pour les données personnelles reviendrait plutôt à octroyer une rareté artificielle. La ressource à préserver ici est la vie privée elle-même. Le marché des données personnelles serait alors à l'image des permis de pollution visant à créer de la rareté pour inciter les pollueurs à internaliser les coûts externes qu'ils infligent à la nature ;

- Un droit de propriété intellectuelle ? Le principe serait alors de permettre aux individus d'exclure quiconque d'utiliser leurs données personnelles sans autorisation. Mais à l'inverse de la production culturelle, la production des données personnelles ne coûte rien aux individus, mais est le résultat de l'activité d'autres agents. Dans une certaine mesure, de tels droits devraient échoir à ceux qui collectent ces ressources et les exploitent afin de protéger leurs investissements ;

- Un droit à compensation ? L'utilisateur pourrait exploiter les données d'une autre personne mais devrait lui verser une somme pour le dédommager. Mais qui serait chargé de fixer le tarif d'utilisation des données personnelles : l'entreprise gestionnaire, l'État, l'individu concerné… ? Et la valeur de

compensation, collectivement négociée, ne risquerait-elle pas d'être insuffisante pour compenser le dommage créé par l'exploitation des données ? Ou au contraire excessive, rendant ainsi impossible des utilisations innovantes ?

#### *1.1.1.3.5.2 L'évaluation des droits*

D'un côté les individus risquent de sous-évaluer la valeur de leurs données personnelles en n'incluant pas les bénéfices tirés de l'exploitation des données. De l'autre, les individus pourraient surévaluer la valeur de leurs données personnelles en exigeant un prix trop élevé pour céder leurs droits. Cela exclurait les entreprises pourtant prêtes à les acquérir à un prix socialement optimal et entraverait l'émergence d'un marché des données personnelles auquel participeraient les personnes.

### *1.1.1.4 Les coûts de mise en place du cadre institutionnel*

La transition vers un marché des données personnelles fondé sur des droits reconnus aux individus pourrait présenter des coûts majeurs. Une telle institutionnalisation créerait des coûts en matière de délimitation des droits octroyés, d'établissement des contrats, de procédure de surveillance… En outre, l'octroi de tels droits pourrait augmenter les coûts de production des firmes exploitant des données personnelles car elles devront payer leur usage. Elles reportaient alors ces coûts sur les prix, éliminant au niveau collectif tout ou partie des avantages économiques des droits de propriété.

Notons que la solution de Laudron répond, en partie à ces critiques :

- Réduction des coûts de transaction (guichet unique et mutualisation des moyens de gestion) ;
- Meilleur contrôle des exploitations secondaires (*via* l'anonymat des titulaires de droits) ;
- Meilleure évaluation des droits (mise en place du marché des infomédiaires, encadrement de leur activité par le droit de la concurrence et la CNIL)

#### *1.1.1.5 Concevoir une règlementation optimale à l'heure d'Internet*

##### 1.1.1.5.1 L'étendue optimale de la privacy

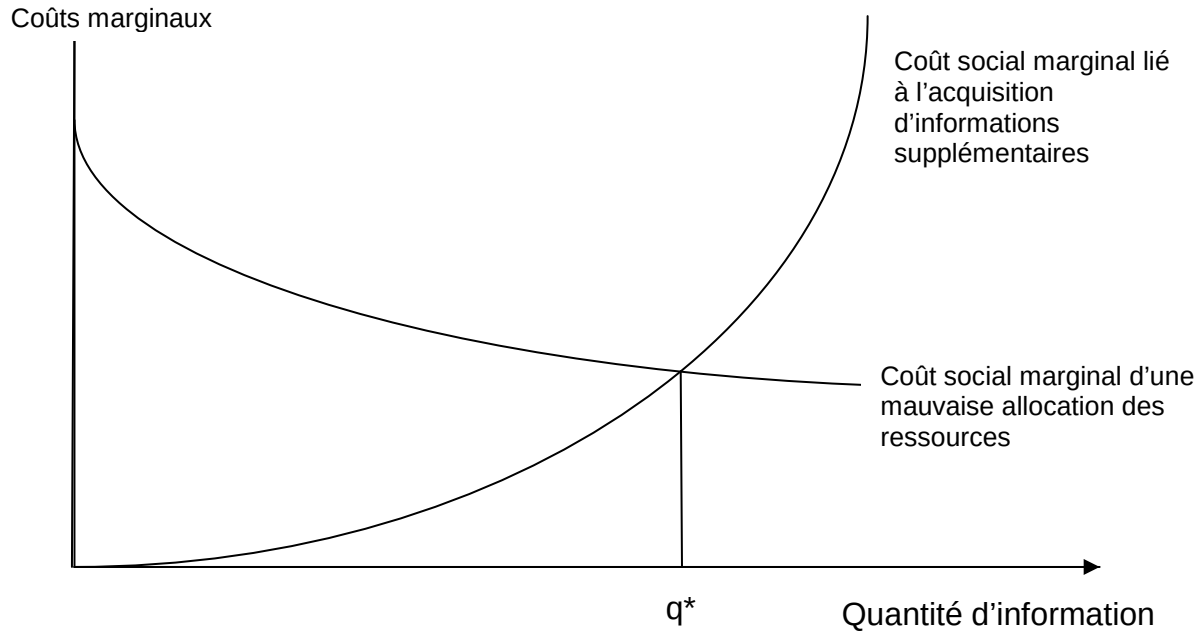
Théoriquement, le niveau optimal de protection légale de la vie privée revient à déterminer le volume de données personnelles accessibles aux organisations minimisant le coût social de leur exploitation. L'optimum est défini ici à partir des effets positifs et négatifs sur le bien-être d'une quantité additionnelle de données personnelles disponibles sur les individus en tant que consommateurs, emprunteurs, travailleurs…

D'un côté, cette quantité additionnelle peut améliorer l'appariement entre l'offre et la demande et engendrer un certain nombre de bénéfices. Ainsi, collecter suffisamment de données personnelles, permet de personnaliser l'offre ou de concevoir des services de mise en relation innovants sur Internet. Cet effet positif peut être conçu d'une certaine façon comme une diminution du coût social inhérent à une mauvaise allocation des ressources.

D'un autre côté, une quantité supplémentaire de données personnelles sur le marché peut diminuer le bien-être social en donnant lieu à des exploitations négatives ou dont les effets peuvent se révéler négatifs : pollutions numériques, contrainte sur l'autonomie individuelle,…Cet effet peut se traduire comme une augmentation du coût social marginal d'acquisition d'informations additionnelles.

Le graphique suivant illustre l'arbitrage entre deux objectifs contradictoires consistant à maximiser les bénéfices tirés de l'exploitation des données personnelles tout en maximisant le bien-être lié au respect de la vie privée. Définir une régulation optimale revient à déterminer la quantité d'informations qui minimise la somme des coûts sociaux liés à une mauvaise allocation des ressources et à l'acquisition d'informations supplémentaires, définie par l'intersection des courbes de coûts sociaux marginaux, soit $q^*$. Tout écart par rapport à cette quantité optimale augmente la somme des coûts sociaux.

Figure 1. Le niveau optimal de protection des données personnelles




#### 1.1.1.5.2 Les conditions d'efficacité des modes de régulation

Tang *et a.l.* montrent que l'efficacité des différents régimes présentés plus haut dépend :

- La sensibilité des consommateurs à la protection de leurs données personnelles ;
- La perte de surplus qu'ils subissent en cas de violation de leur vie privée ;
- Le coût de protection des données personnelles par les vendeurs.

Les normes légales seraient alors préférables lorsque la sensibilité à la vie privée et les pertes subies en cas de violation sont élevées. Le coût social de la règlementation serait plus que compensé par le gain de bien-être ainsi obtenu par les consommateurs. Le régime du *caveat emptor* (« que l'acheteur soit vigilant ») serait plus efficace dès lors que le coût de protection des données personnelles est élevé pour les vendeurs et que la sensibilité et la perte subie par les consommateurs sont faibles. Le bien-être serait d'autant plus élevé sous ce régime que les vendeurs épargnaient le coût de protection de la *privacy*.

Enfin, le régime de la labellisation serait le plus efficace pour des niveaux intermédiaires de sensibilité et de perte de surplus des consommateurs en cas de violation.
Vila *et al.* montrent l'inefficience des solutions de marché, toutes confrontées à un problème de type *lemon market*. Il existe une asymétrie informationnelle entre les vendeurs et les consommateurs pour déterminer si les premiers vont vendre *in fine* les données personnelles collectées. Les engagements de *privacy* des vendeurs peuvent servir de signal, mais risquent d'être insuffisants en raison du différentiel (insuffisant) de coûts entre le respect de la vie privée et la défection des vendeurs.

De même, la prévention ou la technologie seraient insuffisants. Au mieux, elles augmentent le nombre d'internautes sensibles à la *privacy* ou le nombre de firmes la respectant. Par exemple, la mise en place d'infomédiaires privés ne suffit pas : les individus, confiants, cessent de vérifier les engagements et les stratégies des firmes, de même que les intermédiaires privés ont une forte incitation à tricher eux-mêmes (par exemple, revendre les données personnelles dont ils ont la charge).

Par conséquent, la réglementation et les sanctions légales seraient les seuls moyens pour obliger les entreprises à respecter la vie privée : le certificateur public serait le seul à garantir la traçabilité et la certification de l'information.

### 1.1.2 Le cadre législatif national et européen de protection des données personnelles au regard des enjeux contemporains de l'identité numérique

#### *1.1.2.1* ***La protection des données personnelles sur les réseaux sociaux : un cadre juridique propre***

##### 1.1.2.1.1 Au niveau national : l'adaptation des textes à l'évolution des usages d'Internet

Le cadre juridique applicable aux réseaux sociaux n'est pas identique à celle d'un site standard. En fournissant les moyens permettant de traiter les données des membres du réseau et en déterminant la manière dont ces données peuvent être utilisées à de fins publicitaires ou commerciales, y compris la publicité fournie par des tiers, le site en question assume la qualité de responsable du traitement des données, conformément à la loi **Informatique et Libertés du 6 janvier 1978**.

En effet, il appartient à l'administrateur du site de garantir la mise en place de paramètres par défaut respectueux de la vie privée afin de limiter l'accès des données personnelles des membres aux contacts choisis par ceux-ci. Aussi, il est nécessaire dans les conditions générales d'utilisation proposées d'indiquer aux internautes la politique appliquée à cet égard[16].

Il appartient également au réseau social d'assurer un niveau de sécurité approprié des données traitées, tant au moment de la conception du système de traitement, qu'au moment même du traitement.

Par ailleurs, il appartient également au réseau social de mettre en garde les membres contre les risques d'atteinte à leur vie privée et à celle des autres, lorsqu'ils mettent des informations, images ou idées, en ligne sur le réseau social.

[16] Avis n°5/2009 adopté par le groupe de travail « a rticle 29 »

Enfin, il conviendra également de procéder aux formalités préalables déclaratives auprès de la CNIL.

Par ailleurs, sur le fondement de la **directive 95/46 CE** (cf. infra) la **loi n°2004-801 du 6 août 2004** modifie la **loi n° 78-17 du 6 janvier 1978** sur la protection des données au regard du traitement des données personnelles.
Elle prend en compte les risques liés à l'utilisation des nouvelles technologies dans le cadre du traitement, de l'échange et de la circulation des données. Dans ces conditions, la loi s'applique à l'ensemble des traitements de données à caractère personnel, c'est-à-dire à toute opération, quel que soit le procédé utilisé (la collecte, l'enregistrement, l'organisation, la conservation, l'utilisation, etc.) portant sur toute information relative à une personne physique identifiée ou pouvant être identifiée par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Cette loi limite le contrôle a priori des fichiers par la CNIL pour lui substituer le plus souvent un contrôle a posteriori. Les pouvoirs d'investigation ou d'accès aux données de la Commission ainsi que ses possibilités effectives d'intervention seront, en contrepartie, renforcées.

En effet, lors de manquements sérieux au respect de la **loi Informatique, fichiers et libertés**, la CNIL a le pouvoir de prononcer des sanctions administratives, financières ou pénales, la CNIL ayant la possibilité de dénoncer au Procureur de la République les infractions à la loi dont elle a connaissance.

Lorsque des manquements à la loi sont portés à la connaissance de la formation contentieuse de la CNIL, celle-ci peut prononcer un avertissement à l'égard du responsable de traitement fautif, qui peut être rendu public, une mise en demeure à l'organisme contrôlé de faire cesser les manquements constatés dans un délai allant de dix jours à trois mois. Si le responsable de traitement se conforme à la mise en demeure, la procédure s'arrête et le dossier est clôturé.

Si le responsable de traitement ne se conforme pas à la mise en demeure de la CNIL, la formation contentieuse peut prononcer, après une procédure contradictoire, durant laquelle le responsable de traitement incriminé peut présenter des observations orales :

- Une sanction pécuniaire,
- Une injonction de cesser le traitement,
- Un retrait de l'autorisation,
- En cas d'urgence, l'interruption de la mise en œuvre du traitement, et le verrouillage des données pour trois mois,
- En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander, par référé, à la juridiction compétente, d'ordonner toute mesure de sécurité nécessaire.

Par conséquent, le corpus législatif national tente de garantir au mieux la protection des données personnelles des internautes par l'existence de sanctions diverses et dissuasives (pour les sanctions pénales cf.infra)

#### 1.1.2.1.2 Au niveau européen : garantir la protection des données personnelles au-delà des frontières nationales

En 1981, le Conseil de l'Europe élabore la **Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel** qui reste à ce jour, dans ce domaine, le seul instrument juridique contraignant sur le plan international, à vocation universelle, ouverte donc à l'adhésion de tout pays y compris non membre du Conseil de l'Europe.

Cette Convention définit un certain nombre de principes pour que les données soient collectées et utilisées de façon loyale et licite. Ainsi, elles ne peuvent être collectées que dans un but précis et ne peuvent pas être utilisées de manière incompatible avec ce but, elles doivent être exactes, proportionnées à cet objectif et conservées uniquement pendant le délai nécessaire à sa réalisation. Le texte établit, en outre, le droit d'accès et de rectification de la personne concernée et exige une protection

spéciale pour les données sensibles (notamment celles concernant l'appartenance religieuse, les opinions politiques ainsi que les données génétiques ou médicales).

Dans le prolongement de cette Convention du Conseil de l'Europe, l'Union européenne a adopté en octobre 1995 la **directive 95/46/CE**. Cette directive constitue le texte de référence, au niveau européen, en matière de protection des données à caractère personnel.

Elle met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne. Pour ce faire, la directive fixe des limites strictes à la collecte et à l'utilisation des données à caractère personnel, et demande la création, dans chaque État membre, d'un organisme national indépendant chargé de la protection de ces données.

La présente directive s'applique aux données traitées par des moyens automatisés (base de données informatique de clients, par exemple) ainsi qu'aux données contenues ou appelées à figurer dans un fichier non automatisé (fichiers papiers traditionnels).

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 la licéité de ces traitements. Ces principes portent sur: la qualité des données, la légitimation des traitements de données, l'information des personnes concernées par les traitements de données, le droit d'accès et de rectification de ces personnes aux données les concernant

Les principes énumérés peuvent voir leur portée limitée afin de sauvegarder, entre autres, la sûreté de l'État, 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 la protection de la personne concernée.

Ensuite, la directive précise que la personne qui fait l'objet d'une mesure de collecte de ses données personnelles dispose d'un ensemble de droits : le droit d'opposition aux traitements de données, la confidentialité et la sécurité des traitements, et la notification des traitements auprès d'une autorité de contrôle.

Toute personne doit également 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.

#### *1.1.2.2* ***La protection des données personnelles lors de l'utilisation des réseaux sociaux : le cas de la faille de sécurité du site Facebook***

Symantec, l'éditeur de logiciels antivirus à découvert une faille dans le protocole de sécurité sur le site Facebook[17].

Les développeurs d'application sur Facebook utilisent un SSO (« *Single Sign-On* » ou une « *authentification unique* ») qui concrètement permet à un utilisateur de ne se servir que d'un seul protocole d'authentification pour accéder à une pluralité de services. S'agissant de Facebook, l'utilisateur peut accéder aux services fournis par les applications en donnant simplement son autorisation. L'identifiant et le mot de passe ne sont exigés qu'une seule fois ou ne sont pas exigés du tout.

L'avantage pour les entreprises qui utilisent cette procédure réside dans la simplicité et la rapidité de mise en œuvre d'une procédure d'inscription. Par exemple, lorsqu'un utilisateur se connecte à *Deezer, MusicMe, Netvibes* ou tout autre site internet utilisant l'authentification par le biais d'un profil Facebook existant, il permet au programme utilisé par l'un des sites internet précités de créer un «*token* », l'équivalent numérique d'une clef de rechange, qui évite à l'utilisateur d'avoir à s'authentifier en permanence sur ces sites.

La faille de Facebook concernait ce « *token* » qui était visible par les tiers et en particulier par les régies publicitaires. Or, c'est à partir du « *token* » que l'application peut accéder aux informations de l'utilisateur.

[17] www.legavox.fr-faille-de-securite-facebook-recours-contre-la-fuite-des-donnees-personnelles

Juridiquement, le SSO est une relation tripartite entre d'une part, l'utilisateur et le prestataire d'authentification: Il y a acceptation des conditions générales d'utilisation du service, ainsi que tous les documents prévus par le prestataire tels que la politique de confidentialité, etc…..
D'autre part, entre le prestataire d'authentification et l'entreprise qui utilise le SSO : l'intégration du SSO implique une acceptation de conditions générales de la part de l'entreprise qui souhaite utiliser cette méthode d'authentification.
Enfin, entre l'utilisateur et l'entreprise qui utilise le SSO : l'utilisateur accepte le transfert de ses données de connexion vers l'entreprise utilisatrice.

Dans ce contexte, si le site internet Facebook ne respecte pas sa politique de confidentialité (comme c'est peut-être le cas dans cette affaire de fuite de données), il est susceptible de voir sa responsabilité engagée.

Le développeur d'une application se trouve dans une situation de collecte indirecte des données de l'utilisateur. En effet, il s'adresse au prestataire de SSO (Facebook, Google, etc.) pour obtenir les données nécessaires à une authentification. Or la collecte indirecte comporte certaines particularités, explicitées par **l'article 32-III** de la **Loi informatique, fichiers et liberté** modifiée sur ce point en 2004 (cf. supra) : «*Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I*[18] *dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données* ».

Cette contrainte peut être éludée de deux façons : par une acceptation du SSO par l'utilisateur (par un pop up par exemple), c'est cette méthode qu'utilise Facebook, par une information de l'utilisateur (par mail par exemple) de la collecte de ses données de connexion.

[18] « L'identité du responsable du traitement et, le cas échéant, de celle de son représentant; la finalité poursuivie par le traitement auquel les données sont destinées; les destinataires ou catégories de destinataires des données; les droits qu'elle (la personne concernée) tient des dispositions de la section 2 du présent chapitre (c'est-à-dire le droit d'accès et de rectification aux données) ».

Plusieurs recours existent et permettent de réparer les conséquences de la perte ou du vol de données à caractère personnel et confidentiel.

La perte ou le vol de données personnelles peut être sanctionné d'une part, sur le fondement du délit de manquement à la sécurisation des données prévu aux **articles 226-17** du Code pénal qui précise que *« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.* » et **34** de la **loi informatique et libertés** qui précise que : *« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès»*

Le délit de défaut de « *précautions utiles* » précité nécessite de faire la démonstration d'un élément matériel et d'un élément moral du délit. La matérialité de l'infraction apparait lorsque, techniquement, les moyens mis en œuvre pour la protection des données (cryptologie, contrôle, vérification, etc...) étaient insuffisants, par le biais d'une expertise ou éventuellement grâce au travail de la CNIL. Concernant l'aspect moral de l'infraction, la simple imprudence suffit à le caractériser.

D'autre part, sur le fondement du délit de divulgation illicite de certaines données personnelles sanctionné par l'**article 226-22** du Code pénal qui incrimine : *« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ».*

## 1.2 La protection des systèmes de traitement automatisé de données : un enjeux pour la réglementation du cyberespace

### 1.2.1 Un dispositif juridique complet et efficace contre la cybercriminalité en France

La loi du 8 janvier 1988, dite loi Godfrain est considérée comme la loi pionnière en matière de lutte contre la criminalité informatique ses dispositions constituent encore le cœur de la matière. Les dispositions législatives de lutte contre les infractions aux technologies de l'information et de la communication répriment : l'accès ou le maintient frauduleux dans un système de traitement automatisé de données (1), l'entrave au fonctionnement du système (2), l'introduction frauduleuse de données (3), la falsification/suppression frauduleuse de données (3).

#### *1.2.1.1 L'accès et le maintien frauduleux dans un système de traitement automatisé de données*

Le code pénal sanctionne« *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. 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 trois ans d'emprisonnement et de 45000 euros d'amende*. » (**Article 323-1**)
Et« *La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines*. » Cette disposition vise à sanctionner ceux qui cherchent à prendre connaissance d'informations, confidentielles ou non, figurant dans un système de traitement automatisé de données dont l'accès leur est interdit. (**Article 323-7**)

##### *1.2.1.1.1.1 Preuve du caractère frauduleux de l'accès*

Si le caractère protégé ou non du système (**TGI Béthune 10 mars 1992**) n'est pas une condition requise pour la mise en œuvre de l'article 323-1 du code pénal, il facilite la démonstration du caractère frauduleux de l'accès. La preuve peut résulter du contournement ou de la violation d'un dispositif de sécurité, de l'insertion d'un

fichier espion enregistrant les codes d'accès des abonnés (cookies, cheval de troie,.. ;) etc.

La preuve n'est pas rapportée si l'accédant est en situation d'accès normal, par exemple s'il a procédé à une consultation d'informations accessibles au public.
La cour d'appel de Paris a ainsi considérée, dans un arrêt du **30 octobre 2002** qu'il « *ne peut être reproché à un internaute d'accéder aux données ou de s'y maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès* ». Les juges n'ont manifestement pas voulu sanctionner un utilisateur de bonne foi qui, selon eux n'avait pas accédé de manière frauduleuse au système de traitement automatisé de données.

De même, les juridictions considèrent que dans certains cas l'accès est le résultat d'une erreur : dans ce cas, l'accès et le maintient dans un système de traitement automatisé de données n'est pas frauduleux, mais le résultat d'une erreur de manipulation sur les fichiers. Par conséquent, l'action est dépourvue de caractère intentionnel (**CA Paris, 3ème ch., 4 déc. 1992**).

#### *1.2.1.1.1.2Preuve du caractère intentionnel*

Lorsque l'intrusion est effectivement le fait d'une erreur, le simple fait de se maintenir dans le système pourra être constitutif d'une fraude. En effet, une prolongation indue de la présence de l'accédant, au-delà du temps autorisé, et son intervention dans le système pour visualiser ou réaliser une/plusieurs opérations sont autant d'indices qui concourent à prouver le caractère intentionnel de l'intrusion et du maintient anormal dans le système de l'accédant.

En effet, pour la première fois, des « pirates » de services télématiques ont été condamnés par la Cour d'appel de Paris, dans un arrêt du **5 avril 1994**. Leurs agissements répréhensibles consistaient à envoyer grâce à des programmes d'appels automatiques ou semi-automatiques, des messages ayant pour objet

d'inciter les utilisateurs à se connecter sur des services concurrents, et ce, bien que des parades techniques aient été installées par les serveurs victimes de ces pratiques pour les en empêcher. De plus, ces manœuvres aboutissaient parfois à saturer les accès télématiques de services concurrents.

L'arrêt du 5 avril 1994 de la Cour d'appel présente l'intérêt d'avoir appliqué la loi « Godfrain » à un traitement automatisé de données ouvert au public en retenant le délit de maintien frauduleux ainsi que celui d'entrave au fonctionnement du système automatisé de données.

Concernant le délit de maintien frauduleux, la cour reconnaît que l'accès à un système automatisé de données ouvert au public, comme c'est le cas pour beaucoup de services télématiques, n'empêche pas pour autant les dispositions de l'**article 323-1** du nouveau Code pénal de s'appliquer. Elle souligne que, pour être punissable, un accès ou un maintien doit être fait sans droit et en pleine connaissance de cause, sans qu'il soit nécessaire que l'accès soit limité par un dispositif de protection. Elle considère qu'il suffit que le « maître du système[19] » ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées.

Elle précise qu'en outre, même si l'accès à un système automatisé a été au départ régulier, le maintien dans le système peut devenir frauduleux dès lors que l'auteur du maintien perd son habilitation à rester au sein du traitement. En d'autres termes, elle indique que l'accès ou le maintien dans un système suppose le respect des « règles du jeu » de celui-ci, qu'elles soient de nature législative, contractuelle ou relèvent de la volonté du « maître du système », et que dès lors qu'il y a un manquement à ces règles, l'accès ou le maintien devient irrégulier.

Concernant ensuite l'entrave au système automatisé de données, la cour considère que de tels faits sont constitutifs du délit d'entrave au fonctionnement des serveurs télématiques. Elle s'est appuyée, pour fonder sa décision, sur les conclusions du rapport de l'expert dont il ressort que l'envoi automatique de messages, ainsi que l'utilisation de programmes simulant la connexion de multiples Minitels aux centres

[19] « Toute personne physique ou morale, de toute autorité publique, de tout service ou de tout organisme qui est compétent pour disposer du système ou pour décider de sa conception, de son organisation, ou de ses finalités » convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

des serveurs concernés, ont eu des effets perturbateurs sur les performances des serveurs et ont entraîné un ralentissement de leur capacité.

Enfin, lorsque l'accès ou le maintien frauduleux a provoqué « *soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et 45000 euros d'amende* » (**C. pén., Art. 323-1, al. 2**). Dans l'esprit du texte, les dégradations provoquées sont alors involontaires, elles sont la conséquence de l'accès ou du maintien frauduleux dans le système, sans que leur auteur ait voulu délibérément lui porter atteinte. Il conviendra toutefois d'en rapporter la preuve : la suppression, la modification d'une donnée, l'altération du fonctionnement du système sont autant d'indices significatifs.

#### 1.2.1.1.2 Atteinte à l'intégrité du système

Le code pénal précise en son **article 323-2** que le « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende* ». La destruction de fichiers, de programmes, le flaming[20], sont autant d'attaques susceptibles de provoquer des dysfonctionnements du système informatique (ralentissement ou paralysie). L'attaque la plus connue est celle qualifiée d'attaque par « déni de service » ou *denial of service*. Elles se traduisent par une saturation du site, le rendant inaccessible en submergeant de connexions le serveur qui l'héberge.

Par exemple, le tribunal de grand instance de Lyon avait sanctionné l'accès frauduleux et l'altération du système d'information d'une société au moyen d'un logiciel permettant l'envoi de grande quantité de courriers électroniques vides ainsi que l'emploi de gros fichiers au moyen d'un compte anonyme souscrit auprès d'un fournisseur internet avec pour objectif d'encombrer la bande passante de la victime, employeur du prévenu, et de ralentir son système (**TGI Lyon, 20 févr. 2001**)

[20] Le flaming consiste à se livrer à des attaques via l'internet en ayant la volonté de perturber le système d'information de son interlocuteur et en suscitant un encombrement important de la capacité de mémoire.

Ensuite, la cour d'appel de Paris, dans un arrêt du **5 avril 1994** (cf.supra) a jugé que « *l'envoi automatique de messages, ainsi que l'utilisation de programmes simulant la connexion de multiples Minitels aux centres serveurs concernés, ont eu des effets perturbateurs sur les performances des serveurs et ont entraîné un ralentissement de leur capacité. De tels faits sont donc constitutifs du délit d'entrave au fonctionnement des serveurs télématiques* ».

Un virus ou une bombe logique peuvent également constituer un préjudice dans la mesure où il occupe une partie de la mémoire d'un système et ralentit de ce fait le fonctionnement de l'ordinateur.

#### 1.2.1.1.3 Atteinte à l'intégrité des données

L'**article 323-3** du Code pénal rappelle que « *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 cinq ans d'emprisonnement et de 75000 euros d'amende* ».
De plus, l'**art. 323-3-1** Code pénal précise que « *Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des 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* ».

Cette incrimination englobe, notamment, le fait de « déférencer » l'adresse d'un serveur web dans les moteurs de recherche, de s'introduire sur un serveur ou encore de programmer de fausses cartes bancaires.

Ainsi, l'acte délictueux consiste à « fausser » le système, c'est-à-dire à lui faire produire un résultat différent de celui qui était attendu, par exemple, bloquer l'appel d'un programme, d'un fichier, ou encore d'altérer le système d'exploitation d'un réseau de télécommunications. Il faut prouver que l'atteinte à l'intégrité des données

est volontaire. L'élément intentionnel peut se déduire des faits : l'introduction d'un virus dans un système informatique démontre l'intention délibérée du délinquant.
En raison de la rigueur de la loi pénale, certaines entreprises préfèrent se placer sur le terrain de la responsabilité civile en cas de défaillances du détecteur de virus. Mais le plus souvent le fournisseur de détecteur de virus a pris le soin de préciser qu'il n'était tenu que dans la limite de son engagement contractuel, et a pris la précaution d'énumérer les virus susceptibles d'être éradiquer par le détecteur.

La cour d'appel de Paris a considéré que le fait de laisser le personnel d'une entreprise se connecter sans contrôle à des sites considérés comme illicites est une faute. En effet, dans son arrêt du **4 mai 2007**, la cour met en exergue la nécessité pour les entreprises qui permettent à leurs salariés d'accéder à l'Internet et à des réseaux de communications électroniques (exemple : services de messageries et web), d'en encadrer l'usage. Ce dernier peut être plus ou moins strict et contrôlé. Cela dépendra des décisions politiques de l'entreprise, lesquelles se fondent en principe sur une analyse des risques. Ainsi, il sera essentiel de distinguer les communications électroniques professionnelles des personnelles et de préciser les règles applicables à chacune d'elles. En l'espèce, la cour d'appel qualifie de fautive la société incriminée lorsqu'elle a laissé à son personnel l'accès à des sites illégaux et étrangers à l'activité de l'entreprise, donc à une utilisation professionnelle des services web.

Par conséquent, il s'agit de fixer les règles applicables à la gestion des accès aux systèmes d'information, aux contrôles, à la confidentialité et à la conservation des traces informatiques : le laisser-faire en matière d'accès à l'Internet (mais aussi aux ressources informatiques et réseaux) ne peut être admis. Au contraire, les entreprises pour éviter de voir leur responsabilité engagée du fait des agissements de leurs salariés doivent imposer certaines règles de conduite au travers d'un document à usage interne, le plus souvent une charte d'utilisation des moyens informatiques.

Pour illustrer, et selon une jurisprudence constante, le simple fait de consulter les courriers électroniques de tiers en utilisant leurs codes d'accès constitue un accès

frauduleux à un système informatique et une atteinte au secret des correspondances.

C'est le cas d'un ancien consultant informatique de l'entreprise Oddo qui, bien après son départ, avait accédé aux messageries électroniques du directeur général et du directeur des ressources humaines a été condamné par le TGI de Paris à six mois de prison avec sursis. Le frère du consultant, qui avait été salarié de la société avant d'être embauché chez son concurrent, a été condamné pour recel (**TGI Paris, 12ème ch. corr., 1er juin 2007**).

En effet, suite à la plainte déposée par le directeur informatique, une perquisition chez l'ancien consultant a été effectuée et l'analyse de son ordinateur a fait apparaître les traces de connexions aux comptes mails concernés ainsi que les compte-rendus du comité exécutif d'Oddo. Pendant sa garde à vue, il a avoué avoir conservé les codes d'accès aux messageries des deux dirigeants et avoir transmis des messages à son frère pour qu'il surveille le rachat éventuel d'Oddo par son employeur Wargny.
Le TGI considère qu'il y a bien atteinte au secret des correspondances, en vertu de l'**article 226-15** du code pénal qui sanctionne le fait d'ouvrir ou de détourner des correspondances adressées à un tiers. Par ailleurs, il juge que l'accès frauduleux à un système automatisé de données est bien caractérisé. Le tribunal explique que *« l'utilisation d'un code d'accès à une messagerie par un ancien salarié constitue bien une manœuvre, l'intéressé ayant parfaitement conscience qu'il n'a plus le droit d'utiliser ce code et qu'il ne fait plus partie de la liste des personnes autorisées ».*

Pour conclure ce premier point consacré à la présentation du cadre juridique national de lutte contre la criminalité informatique, le corpus législatif permet d'appréhender de manière globale les infractions réalisées contre un système de traitement automatisé de données. Cependant, l'actualité récente des attaques informatiques révèle que la criminalité informatique est, non seulement en expansion, mais prend des formes non prises en compte par la loi Godfrain.

### 1.2.2 L'émergence de nouvelles formes d'attaques informatiques

#### *1.2.2.1 La recrudescence du phishing*

Blue Coat Systems, un fournisseur de solutions de sécurité Web, a, dans son rapport de 2011 sur la sécurité Web, examiné les comportements des internautes et les programmes malveillants auxquels ils sont le plus fréquemment exposés. Au travers de l'analyse des 3 milliards de requêtes Web en temps réel, ce rapport établit un panorama des nouvelles tendances d'utilisation d'Internet et répertorie les nouvelles méthodes d'attaque des cybercriminels[21].

À la lecture de ce rapport il apparaît que les réseaux sociaux sont la nouvelle plate-forme de communication. Les messageries en ligne arrivent en 17ème position des requêtes Web les plus fréquentes en 2010, alors qu'elles étaient en 9ème position en 2009 et en 5ème position en 2008. Leur baisse de popularité se confirme et s'explique par l'adoption croissante des réseaux sociaux comme plate-forme de communication préférée des internautes.

Parmi les attaques les plus répandues, le rapport souligne que les réseaux sociaux sont aujourd'hui les principaux vecteurs d'attaques. En effet, en 2010, les cybercriminels ont usé des relations de confiance entre amis pour infecter autant de nouveaux adeptes des réseaux sociaux que possible. Les deux types d'attaques via les réseaux sociaux les plus employées en 2010 sont le phishing[22] et le clickjacking (détournement de clic). La recrudescence des attaques de phishing par les réseaux sociaux s'explique par la volonté d'obtenir des internautes des identifiants pouvant eux-mêmes permettre d'accéder à d'autres données confidentielles (informations bancaires, financières,…) protégées par les mêmes mots de passe.

[21] http://www.undernews.fr/reseau-securite/rapport-2011-de-blue-coat-sur-la-securite-web-les-nouvelles-tendances-cybercriminalite.
[22] Mode d'usurpation d'identité numérique. Il s'agit d'une technique visant à adresser un mail à un internaute l'invitant à se connecter à un site, copie parfaite d'un site connu de l'internaute et à lui réclamer, sous divers prétextes, des informations confidentielles

En seconde position le détournement de sites légitimes constitue l'une des nouveautés majeures de l'année 2010. Cette technique consiste à faire migrer des infrastructures d'attaques depuis les domaines gratuits vers des sites connus, à la réputation établie et en bonne place dans les classements des catégories acceptables. En piratant ainsi des sites de confiance, les cybercriminels hébergent leurs infrastructures d'attaques derrière des sites apparemment insoupçonnables.

Le terme «*phishing*» est un terme, dérivé de l'anglais «*fishing*» qui signifie pêcher à la ligne et du mot «*phreaking* qui désigne une utilisation frauduleuse des lignes téléphoniques[23]. D'une manière commune, le «*phishing*» désigne l'obtention des identifiants d'une personne, en se faisant passer auprès des victimes pour un individu, une entreprise ou une autorité publique ayant un besoin légitime de solliciter l'information demandée. Cette obtention vise généralement à l'utilisation frauduleuse d'un ou plusieurs comptes bancaires.

Les attaques de «*phishing*» se caractérisent par la combinaison d'un «*social engineering*» (une manipulation sociale), et par un ou plusieurs «*technical subterfuge*» (une manœuvre technologique). Les points communs à tout « phishing » sont l'utilisation :

- d'un support numérique tout au long du parcours infractionnel;
- d'une technique reposant sur la crédulité de la victime ;
- d'une identité réelle et généralement connue à des fins de transmission de coordonnées personnelles que celles-ci soient liées à un organisme bancaire ou financier, un site commercial ou à un service en ligne.

Les moyens qui entourent cette usurpation d'identité sont de nature extrêmement diverse même si le processus consiste généralement en l'envoi massif d'un faux courriel, apparemment authentique, utilisant l'identité d'une institution financière ou d'un site commercial connu, dans lequel on demande aux destinataires, généralement au motif d'un panne informatique, de mettre à jour leurs coordonnées bancaires ou personnelles, en cliquant sur un lien menant vers un faux site web ou l'envoi d'un fax.

[23] F. Duflot, *Phishing, les dessous de la contrefaçon*, RLDI 2006, note 12

#### 1.2.2.1.1 Les moyens de répression du phishing

Le phishing peut être appréhendé pénalement soit *via* sa finalité, soit via les moyens de cette finalité. Dans le premier cas, cette action est susceptible de tomber sous le coup des dispositions de l'article **L. 313-1** du Code pénal sur l'escroquerie qui sanctionne de cinq ans d'emprisonnement et de 375 000 € d'amende l'emploi de manœuvres frauduleuses destinées à tromper une personne, étant avéré que celles-ci s'appliquent aujourd'hui à une chose immatérielle telle qu'une donnée. S'agissant des techniques de «*phishing*», le but étant d'imiter les éléments significatifs d'une institution afin de rendre crédible son attaque, celui-ci sera amené à constituer généralement une contrefaçon de marque et d'œuvre.

Toutefois, le «*phishing*» pourrait également être sanctionné sur le fondement de l'**article 226-18** du Code pénal qui dispose que « *le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* ».

Le « *phishing*» pourra enfin, être appréhendé via le fait que l'utilisation d'un identifiant sans droits afin d'accéder à la partie privée d'un site, ou un intranet, est constitutif de l'élément matériel de l'infraction d'accès frauduleux à un système de traitement automatisé de données prévue par **l'article 323-1** du Code pénal.

### *1.2.2.2 L'usurpation d'identité numérique : une nouvelle incrimination pénale*[24]

Le nouveau délit institué par la **loi d'orientation et de programmation pour la performance de la sécurité intérieure** (LOPPSI 2) adoptée le 8 février 2011 sanctionne l'usurpation d'identité de manière générale, quelle se produise dans le monde physique ou bien sur un réseau de communication au public en ligne. Le législateur a ainsi pris en considération le fait qu'avec le développement d'Internet et

[24] http://www.net-iris.fr/blog-juridique/127-anthony-bem/26884/nouveau-delit-penal-usurpation-identite-sur-internet-et-les-reseaux-sociaux#locate

l'importance des réseaux sociaux, on assiste à une recrudescence du nombre de cas d'usurpation d'identité en ligne.

Concrètement l'usurpation d'identité consiste à utiliser sur internet, sans votre accord, des informations permettant de vous identifier telles que :

- vos nom et prénom,
- votre pseudo,
- votre adresse électronique,…

Cette usurpation peut avoir lieu sur n'importe quel type de site internet : blog, forum de discussion, réseau social, sites de partage, sites institutionnels, chat, etc…

Concrètement, il pourra notamment s'agir de :

- commettre sous votre identité des actes répréhensibles,
- nuire à votre réputation sous votre identité en créant un faux profil, un blog, ou rédigeant des commentaires sous votre identité,
- récupérer à partir d'un faux site des informations personnelles : pirater des boîtes mail ou des comptes Facebook,
- accéder à des comptes sécurisés,
- vous envoyer un message en se faisant passer pour un organisme public ou une entité privée à des fins commerciales, économiques, financières, politiques, etc.

Cette loi a créé un nouvel **article 226-4-1** dans le Code pénal, qui dispose que :

*"Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15.000 EUR d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne."*

Ainsi, ce nouveau délit est susceptible de s'appliquer quand les conditions suivantes sont réunies : d'une part, l'usage d'une ou plusieurs données de toute nature permettant d'identifier une personne, d'autre part, dans le but de troubler sa tranquillité ou de porter atteinte à son honneur ou à sa considération.

Mais l'usurpation d'identité peut également tomber sous le coup des dispositions de la **loi Informatique, fichiers et libertés** puisque cette action donne lieu à un traitement de données à caractère personnel d'un individu sans son accord, délit sanctionné pénalement par 5 ans de prison et 300.000 euros d'amende.

La publication du rapport de Microsoft sur la cybercriminalité et la sécurité des données souligne l'importance de cette nouvelle pratique et la nécessité de faire preuve d'une grande prudence lors de l'utilisation, notamment mais surtout, des réseaux sociaux[25].

Le rapport annonce une hausse de 900% du vol d'identité, passant de 8,3% en janvier dernier à 84,5% en mai 2011, soit huit fois plus que l'usurpation ciblant les sites financiers et 40 fois plus que les sites de jeux en ligne.
Les pirates du net semblent donc délaisser les sites financiers, bien plus exposés aux attaques début 2010 (environ 65%), pour les réseaux sociaux. L'avantage pour les hackers réside en la fréquentation de ces réseaux sociaux, puisqu'une masse considérable d'informations est recueillie sur seulement quelques adresses, contrairement aux sites financiers bien plus nombreux.

En plus de l'usurpation d'informations personnelles, les publicités malveillantes sont aussi en recrudescence. Elles ont augmenté de plus de 70% entre le début et la fin de l'année 2010, principalement via les fenêtres «pop-up» qui s'affichent spontanément.

[25] http://www.zdnet.fr/actualites/microsoft-security-usurpation-d-identite-et-adwares-en-hausse-39760732.htm

## 1.3 La protection des droits d'auteur et des œuvres dans un espace numérique : la difficile conciliation entre un accès libre à la culture et la nécessaire rémunération des auteurs

### 1.3.1 La protection des droits de propriété intellectuelle au regard de la théorie économique : pour un nouveau modèle économique[26]

Internet conduit à une remise en cause des droits d'auteur dans leurs composantes à la fois patrimoniales et morales. Les différents éléments du droit moral ne sont pas tous affectés de la même façon. Par exemple, une œuvre numérisée peut être signée, donc le droit au nom et à la paternité est respecté. En revanche, le droit de repentir est plus difficile à appliquer, ainsi que le droit à l'intégrité : la dématérialisation des supports constitue une forme de désacralisation de son œuvre car tout utilisateur peut la manipuler comme il l'entend. La numérisation ainsi que l'interactivité des réseaux rend toute œuvre aisément transformable. Dans sa composante patrimoniale, la propriété intellectuelle est perçue par des internautes comme une forme d'archaïsme au regard de la diffusion massive d'information permise par l'utilisation d'Internet, alors que la plupart des producteurs et auteurs souhaitent la défendre afin de protéger la création. Un compromis est donc nécessaire entre les partisans d'une information gratuite et accessible au nom d'un droit d'accès à la culture, et les aspirations légitimes des auteurs et de l'ensemble des ayants droits à une « juste » rémunération.

En France, la **loi n° 2004-575 du 21 juin 2004** dite « **Loi pour la confiance dans l'économie numérique** » a instauré, en faveur des fournisseurs d'accès à Internet, un régime dérogatoire au droit commun de la responsabilité civile, excluant toute obligation générale de surveillance de surveiller les informations qu'ils transmettent. Les fournisseurs d'accès à Internet sont cependant tenus de donner suite à des injonctions judiciaires de faire cesser le trouble que constituent les échanges non autorisés de fichiers par l'intermédiaire de logiciels illicites. La loi **n° 2006-961** du **1er août 2006 relative aux droits d'auteur et aux droits voisins dans la société d'information** (DADVSI) leur crée une obligation supplémentaire en

[26] Benhamou F, Farchy J (2007) *Droit d'auteur et copyright*, Paris, La Découverte, coll. Repères

prévoyant qu'ils « adressent à leurs frais, aux utilisateurs de cet accès, des messages des sensibilisation aux dangers du téléchargement et de la mise à disposition illicite pour une création artistique »

#### *1.3.1.1 La remise en cause d'un modèle économique*

##### 1.3.1.1.1 L'incapacité des droits d'auteur à lutter contre la contrefaçon

Le numérique amplifie la caractéristique des industries culturelles qui justifie le recours aux droits d'auteur : une fois le contenu produit, le coût marginal de reproduction et de distribution d'une copie supplémentaire est faible voire nul. Deux conséquences en découlent. D'une part, l'écart entre les coûts de création du prototype et l'ensemble des autres coûts nécessaires à la mise sur le marché d'un contenu culturel se creuse. D'autre part, ce ne sont plus quelques producteurs isolés qui ont l'opportunité d'adopter un comportement de passager clandestin mais l'ensemble des consommateurs. Chaque consommateur peut, en copiant, disposer de sa propre unité de bien à coût nul et quasiment en temps réel.

Alors que les contenus culturels qui circulent sur les réseaux numériques acquièrent de plus en plus la caractéristique économique de non-rivalité des biens collectifs ou informationnels, les droits d'auteurs peinent à exercer leur rôle d'exclusion. Or, l'essence même du droit d'auteur tient en la capacité qu'il confère d'autoriser ou d'interdire à quiconque de reproduire l'œuvre ou la prestation protégée. Le numérique remet en cause le système traditionnel de financement des industries culturelles qui repose sur le paiement direct par l'usager d'œuvres protégées par la propriété intellectuelle et sur les droits exclusifs d'exploitation des œuvres conférés aux titulaires.

##### 1.3.1.1.2 Les effets contrastés du « copiage » sur le bien être social

Face à l'ampleur du nombre de copies circulant sur les réseaux numériques, il est nécessaire de revenir sur la réalité des effets de substitution entre copies et originaux qui jouent un rôle décisif dans les justifications économiques de la propriété

intellectuelle. Dans un objectif de maximisation du bien-être social, l'objectif en matière de propriété intellectuelle est de maximiser la valeur de l'œuvre protégée, non de maximiser le niveau de protection. Le développement des réseaux P2P (peer to peer) a permis le renouvellement de la littérature économique concernant les effets de la copie sur les achats d'originaux et les profits de l'industrie culturelle.

Stanley Liebowitz identifie trois types d'effets positifs potentiels du copiage pour les titulaires de droits : l'appropriabilité indirecte, les externalités de réseau et l'effet d'exposition. Cet auteur développe l'idée que la capacité à copier augmente la valeur que les acheteurs accordent à l'œuvre originale, donc leur consentement à payer, et permet aux offreurs originaux de capturer la valeur des copies. Il distingue deux formes d'exploitation économique des contenus. L'appropriabilité est directe lorsque l'utilisateur est l'acheteur (l'œuvre est protégée par un droit de propriété ou un système technique d'exclusion). Elle est indirecte lorsque l'utilisateur ne contribue pas au financement, mais que l'offreur d'originaux peut bénéficier d'une augmentation de la demande en raison de la valeur produite par les copies non autorisées. Par exemple, la possibilité de copier un CD original pour l'écouter dans sa voiture augmente la demande, car le consommateur valorise cette possibilité. L'appropriabilité indirecte de cette valeur supplémentaire par le producteur d'originaux ne peut avoir lieu qu'à la condition que ce dernier puisse pratiquer une discrimination par les prix entre consommateurs. L'idée d'offrir un même bien à des prix différents aux diverses catégories de consommateurs selon leur disposition à payer afin de capturer l'ensemble du marché potentiel est trouvée par Harold Demsetz qui préconise la discrimination tarifaire afin de faciliter la production privée de biens collectifs.

La stratégie qui consiste pour les entreprises à vendre des biens et services complémentaires afin de réduire les effets négatifs de la copie peut s'interpréter comme une forme particulière d'appropriabilité indirecte. Elle se traduit par des ventes groupées ou par le fait d'associer au bien exposé au copiage un autre bien pouvant plus difficilement être copié. Le bien peut être copié, distribué gratuitement ou à perte, à partir du moment où le consommateur doit forcément l'utiliser en complément d'un matériel dont la production est rentable. L'entreprise inclut le prix du bien copié dans le prix du matériel. C'est le cas de Sony qui s'oppose au piratage

en tant que major du disque, et en parallèle vend des lecteurs MP3 et de Divx (logiciels de compression de musiques et de films) permettant la réalisation de copies.

Les externalités du réseau renvoient au fait que la valeur de certains produits augmente avec le nombre d'utilisateurs. L'utilité d'un ordinateur s'accroit d'autant plus qu'il permet de partager des fichiers avec d'autres utilisateurs. De même, les copies créent des externalités de réseau positives. Parce qu'elle est disponible à moindre coût, une copie pirate augmente le nombre d'individus qui utilisent un bien, et donc sa valeur pour les acheteurs de versions non pirates, qui sont conduits à adopter le produit. Les copies non autorisées peuvent donc bénéficier aux titulaires de droits de propriété intellectuelle c'est-à-dire aux offreurs de copies autorisées, par leurs répercussions en termes de diffusion. Cette thèse s'appuie sur le modèle économique de l'industrie du logiciel dont la stratégie n'est pas de minimiser l'ampleur des copies mais d'étendre la présence de l'entreprise sur le marché.

Troisième effet positif de la copie est l'effet d'exposition ou d'échantillonnage (*exposure* ou *sampling effect*) qui correspond à l'idée que le copie familiarise ses utilisateurs avec des œuvres qui jusqu'alors lui étaient inconnues et peut pousser à l'achat. Les réseaux P2P amélioreraient l'information des consommateurs pour des biens d'expérience (dont la satisfaction ne peut être connue qu'après consommation) et auraient des effets sur la diversité culturelle. Ils permettent la découverte de nouveaux artistes par des majors, ce qui réduit les coûts d'innovation : dans le domaine des jeux sur PC, des éditeurs se servent du P2P pour distribuer des versions d'évaluation de leurs produits et souhaitent susciter l'adhésion grâce au « marketing viral », qui se diffuse massivement via les internautes eux-mêmes.

#### 1.3.1.1.3 Une redéfinition des rapports entre consommateurs et producteurs

La logique gagnants/perdants qui oppose les consommateurs bénéficiant à court terme de la disponibilité de contenus « gratuits », et des titulaires de droits victimes des « effets substitution », est simpliste. La réduction du chiffre d'affaires des producteurs consécutivement au piratage peut conduire à limiter leur incitation à la

création et, à moyen terme, le nombre d'œuvres disponibles pour les consommateurs. Ajoutons que la consommation supposée gratuite est un leurre ; elle suppose un abonnement haut débit et un équipement multimédia du PC au baladeur.

Les plates-formes d'échanges diffusent gratuitement des contenus mais certains ont une vocation commerciale et fonctionnent grâce à un financement publicitaire, à l'exploitation des données personnelles, à la vente de technologies ou de services annexes. Paradoxalement, les réseaux P2P sont victimes de comportements de passager clandestin qu'ils font subir aux industries de contenus. De nombreux utilisateurs téléchargent mais ne mettent rien à disposition, ce qui à terme conduit à la mort du système. Malgré un accès gratuit aux inputs, l'efficacité économique des réseaux P2P nécessite la mise en œuvre de mécanismes d'incitation à contribuer.

Le problème n'est donc pas tant la gratuité que celui du transfert de la rentabilité économique au sein de la chaîne de valeurs entre des industries qui financent les contenus, et des firmes étrangères au monde de la culture, qui profitent de ces contenus pour vendre tout autre chose.

La généralisation de ce modèle pose deux types de problèmes. Le premier a trait à la dévalorisation symbolique de la création lorsque les biens sont conçus pour attirer les faveurs des publicitaires et des sponsors, ou pour vendre les produits dérivés servant à les financer. Cette dévalorisation peut avoir un impact négatif sur l'ensemble de la production artistique. Le second renvoie à la capacité du système de garantir les transferts entre ceux qui financent les contenus et ceux qui en profitent. Parce que cette rentabilité s'accompagne rarement d'un retour vers les industries de contenus et les créateurs, de nouveaux modèles sont en voie d'émergence.

#### *1.3.1.2* ***Répondre au numérique : des modèles alternatifs***

##### *1.3.1.2.1.1 Les solutions publiques*

Pour internaliser l'existence d'externalités positives au profit d'agents économiques dont l'activité bénéficie de la production de contenus culturels, de nombreux économistes préconisent l'instauration de mécanismes de transferts obligatoires.

Neil Netanel propose un système de compensation prélevé sur tous les produits et services en liaison avec le P2P (accès Internet, MP3, graveurs CD/DVD…). Cette compensation forfaitaire donnerait le droit de télécharger gratuitement de façon illimité des contenus dans un but non commercial. Oliver Bomsel envisage de segmenter le marché de l'accès Internet en imposant aux fournisseurs d'accès une tarification asymétrique du haut-débit, dissuasive pour le trafic montant (upload) contenant des fichiers protégés. L'objectif est de favoriser le développement des offres de téléchargement payantes descendantes.

Cependant, l'instauration de nouvelles taxes pose le problème du choix du marché de produits auxiliaires : celui du matériel de reproduction, celui des supports vierges, celui des abonnements Internet, celui des flux upload ? La taxe peut conduire à une baisse de la consommation sur les marchés secondaires taxés : elle pénalise par exemple l'industrie des supports vierges alors que leur utilisation correspond souvent à des usages autres que la reproduction de contenus protégés.

#### *1.3.1.2.1.2 La construction d'une offre marchande autorisée*

##### *1.3.1.2.1.2.1 Les DRM, ou la tentative de restaurer l'exclusion par la technique*

Les Digital Rights Management Systems (DRM) sont des systèmes de gestion des droits pour la distribution sécurisée de contenus numériques, comprenant des mesures techniques de protection de nature matérielle ou logicielle. Ces dispositifs ont été qualifiés de *self-help systems* : à la manière d'un individu défendant lui-même sa nouvelle propriété, le producteur d'une œuvre la protège contre toute tentative d'appropriation non autorisée. Les DRM sont non seulement des mesures techniques de protection qui permettent de contrôler l'accès ou l'utilisation de certains contenus mais également des outils de gestion et d'information des droits. Les DRM s'appuient

sur deux techniques : l'une permet d'encoder le contenu par un système de cryptage. Ainsi, par exemple, une vidéo peut être visionnée depuis un ordinateur mais ne peut pas être enregistrée sur le disque dur, sauf si l'utilisateur dispose d'une clé ou d'une application spécifique. L'autre obéit à une logique de tatouage grâce auquel une information est associée de façon permanente et imperceptible à une œuvre. Il s'agit de marquer une œuvre ou une prestation dans un objectif de protection, d'identification, d'authentification, d'intégrité ou de traçabilité.
Les DRM ouvrent alors la possibilité de préciser une grande quantité d'usages autorisés (reproduction, enregistrement,…) et d'adapter la tarification en fonction des usages.

À la fin des années 90 tout un courant de l'analyse économique a considéré les DRM comme une alternative à la protection légale. La protection des investissements et l'exclusion des consommateurs peuvent être assurées par des dispositifs marchands et des négociations directes entre détenteurs individuels des droits et utilisateurs. Ce modèle contractuel et technologique aurait ainsi l'avantage de mettre en œuvre des systèmes d'exclusion des utilisateurs non payeurs en lieu et place d'une règlementation des droits de propriété ; il éviterait de surcroît les procès en rendant les usages illégaux difficiles, alors que les droits de propriété intellectuelle sont un outil d'exclusion qui n'empêche pas les agents d'utiliser l'œuvre tant qu'une action juridique n'a pas été intentée à leur encontre.

La distribution en ligne grâce aux DRM a cependant suscité un grand nombre d'interrogations d'ordre industriel et technique. Seuls quelques acteurs dominent le marché : Apple, Microsoft, Real Network et Sony. Ces firmes sont en concurrence pour imposer leurs standards. Les DRM, outils de protection des droits de propriété intellectuelle sur les contenus culturels, sont eux-mêmes protégés par des droits de propriété intellectuelle. Certaines entreprises ont fait le choix de restreindre l'accès à leurs DRM et de promouvoir une technologie propriétaire fermée : seuls les iPod peuvent lire les contenus achetés sur le site en ligne de la firme. Inversement, les iPod ne peuvent lire que des contenus protégés par leurs propres DRM et des fichiers MP3 sans DRM associés des réseaux P2P. D'autres entreprises comme Microsoft ont opté pour un système propriétaire « ouvert » : la firme propose ses licences à un prix attractif afin d'éliminer les concurrents, de verrouiller le marché et

de relever les prix à moyen terme. Le point commun entre ces deux stratégies et le contrôle du marché des DRM pour assurer leur position dominante sur le marché des systèmes d'exploitation pour PC. Si la concurrence entre technologie permet une baisse des coûts et une stimulation de l'innovation à court terme, une condition de son efficience à plus long terme suppose de garantir l'interopérabilité, c'est-à-dire de permettre de rendre compatible deux systèmes qui ne le sont pas. Cela permet de bénéficier d'externalités de réseau positives liées à la constitution d'un réseau composé de tous les services et contenus interopérables avec les DRM. En l'absence d'interopérabilité, l'usage de chaque version d'une même œuvre est limité à une plate-forme de distribution ou un terminal. La question de l'interopérabilité concerne essentiellement le marché des baladeurs ce qui pose des problèmes de sécurité et de coûts qui sont répercutés sur les consommateurs alors que la demande d'interopérabilité ne concerne qu'une minorité d'entre eux. De plus, certains DRM collectent des données personnelles qui peuvent être détournées à des fins commerciales. Des technologies de ce genre risquent d'entraîner un comportement de désobéissance plutôt que d'obéissance, d'autant que les protections découragent les utilisateurs néophytes en informatique et laissent une certaine liberté aux internautes capables de les détourner. Alors qu'un livre acheté peut être lu à plusieurs reprises et par différentes personnes, des DRM trop restrictifs sur des œuvres pourtant acquises en toute légalité sont susceptibles d'inciter à la consommation de produits illégaux dont l'usage est plus souple.

D'autres modèles innovants cherchent à exploiter certaines potentialités des réseaux à l'appui du développement d'une nouvelle génération d'offres légales. Le système du « P2P légal » fonctionnant sur la base de la superdistribution[27] ont pour but de réconcilier le respect de la propriété intellectuelle avec les avantages traditionnellement associés au P2P : distribution efficace, capacité de recherche rapide et de partage, effet d'appartenance à une communauté… L'avantage économique est de supprimer la gestion d'un serveur central et de réduire les coûts de la bande passante requise pour répondre aux demandes des internautes, puisque se sont les membres de la communauté qui contribuent à alimenter le réseau, ainsi des prix attractifs peuvent être proposés.

[27] Technologie qui autorise les contenus protégés à être distribués de multiple fois

Toutefois, le P2P légal n'a pas connu les développements attendus, et d'autres modèles économiques plus classiques tentent de se développer. Universal Music et EMI ont ainsi annoncé un projet de téléchargement gratuit de leur catalogue en échange de publicités obligatoires pour l'internaute.

Dans les deux cas, le centre de gravité de la création marchande se déplace au profit des acteurs internationaux qui maîtrisent en aval le marché de la visibilité et de l'accès aux produits, et qui se chargent de négocier le partage des nouvelles sources de valeur avec les producteurs de contenus.

### 1.3.2 La protection des droits d'auteur et des œuvres au regard du cadre normatif national : la difficile conciliation entre les droits des consommateurs et ceux des producteurs

#### *1.3.2.1 La loi relative aux droits d'auteur et droits voisins dans la société de l'information : entre protection des œuvres contre le piratage et principe d'interopérabilité*[28]

La loi **n° 2006-961** du **1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information** a été publiée au Journal Officiel le 3 août 2006. Ce texte est destiné à transposer la **directive n° 2001/29 relative au droit d'auteur et aux droits voisins dans la société de l'information**. Objet de critiques la loi DADVSI a fait l'objet d'une non-conformité partielle de la part du Conseil constitutionnel dans sa décision du 27 juillet 2006[29].

[28] Reynaud P, Verbiest T « Adoption de la loi DADVSI et décision du Conseil constitutionnel : point de répit estival ! » RLDI 2006, n°19

[29] Décision n°2006-540 DC, du 27 juillet 2006, de la loi relative aux droits d'auteur et aux droits voisins dans la société de l'information

#### 1.3.2.1.1 Les exceptions au droit d'auteur et l'introduction du test en trois étapes

##### *1.3.2.1.1.1 Les exceptions au droit d'auteur*

Plusieurs exceptions viennent compléter l'article **L. 122-5 du Code de la propriété intellectuelle**. Pour mémoire, cet article permet au public d'utiliser librement les œuvres protégées par un droit d'auteur sans autorisation des titulaires de droits.
Cinq exceptions sont dorénavant ajoutées à l'article L. 122-5 du Code de la propriété intellectuelle :

- une première exception pédagogique vise l'enseignement et la recherche (C. propr. intell., art. L. 122-5, 3°, e°). Elle est de stinée à couvrir les représentations ou les reproductions d'extraits d'œuvres dans l'enseignement, sous conditions restrictives tout en excluant certains types d'œuvres de son champ d'application. Elle ne sera d'application qu'au 1er janvier 2009 ;
- la seconde exception vise les communications sur les réseaux numériques (C. propr. intell., art. L. 122-5, 6°). Elle permet les reproductions provisoires, accessoires et transitoires sur les réseaux numériques sans accord des ayants droit. C'est la transposition de l'article 5-1 de la directive n° 2001/29 relative au droit d'auteur et droits voisins dans la société de l'information ;
- la troisième exception concerne les exploitations dans les établissements accueillant les personnes qui présentent un handicap (C. propr. intell., art. L. 122-5, 7°) ;
- la quatrième exception couvre les actes de reproduction destinés à l'archivage des œuvres par les musées, les bibliothèques et les services d'archives (C. propr. intell., art. L. 122-5, 8°) ;
- la cinquième exception permet la reproduction ou la représentation d'œuvres graphiques, plastiques ou architecturales dans un but exclusif d'information, sous conditions restrictives. Les photographies de presse sont exclues du champ d'application de l'exception (C. propr. intell., art. L. 122-5, 9°).

##### *1.3.2.1.1.2 Le test en trois étapes*

Le législateur a introduit une importante limite aux exceptions au droit d'auteur (C. propr. intell., art. L. 122-5 *in fine*). Afin de pouvoir profiter des exceptions au droit

d'auteur, chaque utilisation de l'œuvre protégée doit passer l'examen du test « *en trois étapes* ».
Ainsi, seules les utilisations énumérées par l'article L. 122-5 du Code de la propriété intellectuelle (1re étape), qui ne portent pas atteinte à l'exploitation normale de l'œuvre (2e étape), ni ne cause un préjudice injustifié aux intérêts légitimes de l'auteur (3e étape), pourront s'effectuer sans autorisation de l'auteur. C'est la transposition de **l'article 5.5 de la directive n°2001/29 relative a u droit d'auteur et droits voisins dans la société de l'information** qui reprend elle-même **l'article 9-2 de la Convention de Berne du 9 septembre 1886.**

Le Conseil constitutionnel a donné son interprétation de la conciliation entre exceptions au droit d'auteur et mesures techniques de protection des œuvres en ayant recours au test des trois étapes. Ces mesures techniques de protection sont des « *verrous* » sur les œuvres qui peuvent limiter ou interdire la possibilité d'en faire des copies. Elles peuvent aussi véhiculer des informations sur les œuvres et les titulaires de droits. Selon le Conseil Constitutionnel, les titulaires de droits pourront supprimer ou limiter toute possibilité de faire des copies privées, dès lors qu'il apparaît un manquement au test des trois étapes (consid. 37)

#### 1.3.2.1.2 Mesures techniques de protection et exigence d'interopérabilité

Les articles **L. 331-5 et suivants du Code de la propriété intellectuelle** viennent fixer le cadre juridique des mesures techniques de protection. Les mesures techniques de protection doivent être compatibles avec les systèmes de lecture des œuvres. En pratique, une œuvre couverte par un « *verrou* » devra être accessible par les systèmes de lecture qui le souhaitent.

##### *1.3.2.1.2.1 Absence de définition législative de l'interopérabilité*

Les auteurs de la loi DADVSI avaient préféré laisser à la jurisprudence le soin de définir la notion l'interopérabilité. Le Conseil constitutionnel a précisé sur ce point « *Considérant que le législateur a fait de l'interopérabilité un élément qui conditionne le champ d'application de la loi pénale ; qu'il devait en conséquence définir en des*

*termes clairs et précis le sens qu'il attribuait à cette notion dans ce contexte particulier ; qu'en s'abstenant de le faire il a porté atteinte au principe de légalité des délits et des peines* (...) ». La censure du Conseil aboutit à la suppression de l'exception relative à l'interopérabilité. Le champ de l'incrimination s'en trouve mécaniquement élargi. Dès lors, les personnes qui se livreront à des actes de contournement d'une mesure de protection, mais à des fins d'interopérabilité tomberont sous le coup de l'incrimination pénale

##### *1.3.2.1.2.1.1 Mise en œuvre de l'interopérabilité*

La mise en œuvre de l'interopérabilité est assurée par une nouvelle « *autorité de régulation* » dont le statut et la composition sont précisés aux articles **L. 331-7 et suivants.**

Cette autorité peut être saisie uniquement par les professionnels (éditeur de logiciel, fabricant de système, exploitant de services) pour obtenir des « *informations essentielles* » de la part du titulaire des droits sur ses mesures de protection. Ces informations essentielles permettent de mettre en œuvre l'interopérabilité. Le titulaire des droits sur les mesures techniques de protection doit être indemnisé lorsqu'il est contraint de diffuser des informations essentielles sur son système (consid. 41).

Le titulaire des droits sur les mesures techniques peut refuser de communiquer ses informations essentielles s'il apporte la preuve que cette communication porte gravement atteinte à la sécurité et à l'efficacité de la protection technique (C. propr. intell., art. L. 331-7 al. 3).
L'autorité de régulation doit rechercher un accord entre les parties. Celle-ci a deux mois pour rendre sa décision (C. propr. intell., art. L. 331-5-2). À défaut, elle peut ordonner des injonctions sous astreinte et des sanctions pécuniaires. Enfin, le Conseil de la concurrence peut être saisi par le président de l'autorité de régulation en cas d'atteinte au droit de la concurrence.

##### *1.3.2.1.2.1.2 Mesures de protection et exception pour copie privée*

L'autorité de régulation aura pour mission de veiller à ce que le bénéfice de l'exception ne porte ni atteinte à l'exploitation normale de l'œuvre, ni ne cause un

préjudice injustifié aux auteurs. Les articles **L. 331-8 à L. 331-16** viennent fixer les lignes directrices du nouveau régime de la copie privée.
L'autorité fixera le nombre de copies autorisées dans le cadre de l'exception de copie privée (C. propr. intell., art. L. 331-8 *in fine*). Toutefois, selon l'interprétation du Conseil, cette autorité ne fixera le nombre minimal de copies qu'au terme d'un délai raisonnable au cours duquel les titulaires de droits sur ces mesures tenteront de les concilier avec les exceptions au droit d'auteur (consid. 50).
L'autorité aura aussi pour mission de veiller à ce que le bénéfice de l'exception ne porte ni atteinte à l'exploitation normale de l'œuvre, ni ne cause un préjudice injustifié aux auteurs. En cas de non-respect du test des trois étapes, le Conseil constitutionnel a estimé que l'exception de copie privée pouvait entièrement disparaître devant les mesures techniques de protection (consid. 57).
Il est enfin précisé que le bénéfice des exceptions peut être subordonné à la licéité de l'accès à la source de la copie, mais seulement dans la mesure où la technique le permet (C. propr. intell., art. L. 331-9 al. 2).

Par conséquent l'on peut interpréter la règle comme ceci :

- Si la source de la copie est en accès libre, l'exception de copie privée peut jouer pour le strict téléchargement à titre privé, peu importe la licéité de la source ;
- Si la source de la copie est protégée par une mesure de protection technique, le jeu de l'exception est conditionné par la licéité de la source de la copie litigieuse.

Par conséquent, les titulaires de droits sont fortement incités à utiliser des mesures techniques de protection pour pouvoir rejeter toute application de l'exception de copie privée.

#### 1.3.2.1.3 La lutte contre la contrefaçon sur Internet

Le nouvel article **L. 335-2-1 du Code de la propriété intellectuelle** permet d'atteindre les éditeurs et exploitants de logiciels qui mettent à disposition des œuvres protégées sans autorisation des ayants droit. Cet article précise que le fait « *d'éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la*

*mise à disposition du public non autorisée d'œuvres ou d'objets protégés* » (1°) et « *d'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un* (tel) *logiciel* (2°) » est sanctionné d'une peine allant jusqu'à 3 ans de prison et 300 000 € d'amende.

Il s'agit de poursuivre les éditeurs et exploitants qui proposent des logiciels de *PtoP* sans inclure la gestion des mesures de protection technique. Les internautes se voient de nouveau soumis à l'aléa de se voir poursuivre pour délit de contrefaçon pour une simple utilisation des logiciels de *PtoP* .

#### 1.3.2.1.4 La titularité des droits d'auteur des agents publics.

Il s'agit ici d'assurer une certaine cohérence entre d'une part, les principes qui visent à protéger le créateur et les exigences du service public. Il s'agit ici d'assurer une certaine cohérence entre d'une part, les principes qui visent à protéger le créateur et les exigences du service public. ce texte distingue entre une cession obligatoire à l'Administration des droits des fonctionnaires pour l'exploitation non-commerciale de leurs œuvres et un simple droit de préférence de l'Administration en cas d'exploitation commerciale de celle-ci. Par exception, les fonctionnaires qui ne sont pas soumis à un contrôle de leur hiérarchie (par exemple les professeurs d'université) ne sont pas concernés par cette cession automatique. Les modalités pratiques du droit de préférence seront quant à elles déterminées par décret.

### *1.3.2.2 L'adoption des lois « HADOPI » l'arbitrage du Conseil Constitutionnel pour concilier la lutte contre le piratage sur Internet et la liberté d'accès aux réseaux numériques des citoyens*[30]

La loi **n° 2009-669** du **12 juin 2009** « ***favorisant la diffusion et la protection de la création sur internet*** » (dite « *loi HADOPI* » ou « *Création et Internet* ») a été promulguée au *Journal officiel*, le 13 juin 2009.

Le dispositif instauré par la loi repose sur un manquement à une obligation de surveillance de l'accès à internet ayant permis la commission d'un acte de contrefaçon, et non sur l'acte de contrefaçon lui-même. Cette obligation impose à la personne titulaire d'un accès à des services de communication au public en ligne, c'est-à-dire l'abonné à internet, « *de veiller à ce que cet accès ne fasse pas l'objet*

[30] Boubekeur I « De la « loi HADOPI » à la « loi HADOPI 2 », RLDI 2009, n° 59

*d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou un droit voisin sans l'autorisation des titulaires de droits* (...) *lorsqu'elle est requise* ». Cette obligation existait déjà à l'article L. 335-12 du Code de la propriété intellectuelle, issu de la « loi DADVSI » du 1er août 2006, mais n'était jusqu'à présent assortie d'aucune sanction.

Le législateur a entendu s'appuyer sur cette obligation dans le cadre de la lutte contre le téléchargement illicite d'œuvres sur internet en instaurant, en cas de manquement à cette obligation, une procédure d'avertissement suivie, le cas échéant, d'une procédure de sanction. La « petite loi » créait à cet effet, pour la première fois en France, un pouvoir extracontractuel de suspension de l'accès à internet, confié à une autorité administrative indépendante, la HADOPI (Haute Autorité pour la Diffusion des œuvres et la Protection des Droits sur Internet), nouvellement créée en lieu et place de l'ARMT (Autorité de régulation des mesures techniques de protection).

#### 1.3.2.2.1 Présentation de la loi HADOPI 1

L'objectif de la loi « HADOPI 1 » est de responsabiliser les internautes quant à leurs agissements, en sanctionnant le titulaire de l'accès internet à partir duquel l'acte de téléchargement illégal a été réalisé.

Pour cela, une réponse en trois étapes était prévue, correspondant à une « *riposte graduée* ». Cette dernière a été vivement critiquée par le Conseil constitutionnel, le 10 juin 2009, estimant attentatoire aux libertés publiques le fait qu'une autorité administrative indépendante intervienne à défaut d'un juge.

##### *1.3.2.2.1.1 La nouvelle autorité en charge de la protection des droits et des œuvres sur Internet : la HADOPI*

L'article 5 de la loi favorisant la diffusion et la protection de la création sur internet crée une autorité administrative indépendante (HADOPI). Elle veillera à la seule prévention des téléchargements illégaux réalisés sur internet. Cette haute autorité sera composée d'un collège (Conseil d'État, Cour de cassation, Cour des comptes, spécialiste en la matière, un membre du Conseil supérieur de la propriété littéraire et artistique, trois personnes choisies sur proposition conjointe des ministres chargés des Communications électroniques, de la Communication et de la Culture et deux

personnes désignées par les Présidents de l'Assemblée nationale et du Sénat : article **L. 331-16 du Code de la propriété intellectuelle**) et d'une commission, composée de trois personnes, qui aura pour mission d'envoyer les avertissements aux abonnés en cas de manquement à l'obligation de surveillance de leur accès internet consacrée au nouvel article **L. 336-3 du Code de la propriété intellectuelle.**

Au sein de cette HADOPI, les magistrats ou fonctionnaires, qui devaient à l'origine être chargés de missions juridictionnelles, composant la commission de protection des droits, ne prendront finalement que les mesures nécessaires pour prévenir toute atteinte et ne pourront donc, en vertu de la censure du Conseil constitutionnel sur ce point, sanctionner les abonnés qui ne surveilleraient pas correctement leur connexion à internet. En effet, le Conseil ne reconnaît à cette commission qu'un « *rôle préalable à une procédure judiciaire* » (consid. 28).

Le cœur du dispositif est donc remis en cause par cette censure : la HADOPI n'aura pas vocation à sanctionner les internautes, sa commission des droits étant réduite à sa fonction de prévention.

#### *1.3.2.2.1.2 La surveillance par l'abonné de sa connexion*

Le nouvel article **L. 336-3 du Code de la propriété intellectuelle** dispose que « *la personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres I^er^ et II lorsqu'elle est requise. Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé* ».

Ainsi, chaque abonné devra être vigilant quant à l'utilisation de sa connexion internet et devra la protéger comme il se doit (clé WEP[31] ou clé WPA[32]). C'est l'apport essentiel de ce nouveau texte qui crée à la charge de chacun des abonnés une obligation nouvelle de surveillance de son accès à internet.

---

[31] La clé WEP (*Wired Equivalent Privacy*) est un protocole d'échange sécurisé permettant de partager une connexion Wi Fi entre plusieurs ordinateurs

[32] La clé WPA (*Wi Fi Protected Access*) est une norme de sécurité définie par la Wi Fi Alliance.

#### 1.3.2.2.1.3 L'obligation amoindrie des fournisseurs d'accès à internet concernant les outils de sécurité

**L'article L. 331-35 du Code de la propriété intellectuelle** prévoit que : « *Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne font figurer, dans les contrats conclus avec leurs abonnés, la mention claire et lisible des dispositions de l'article L. 336-3 et des mesures qui peuvent être prises par la commission de protection des droits. Elles font également figurer, dans les contrats conclus avec leurs abonnés, les sanctions pénales et civiles encourues en cas de violation des droits d'auteur et des droits voisins* ».

À la lecture de la loi pour la confiance en l'économie numérique du 21 juin 2004 (LCEN), les fournisseurs d'accès à internet (FAI), qui devaient proposer et mettre à disposition un logiciel à leurs utilisateurs au sein de leur offre, ne doivent, désormais, qu'informer leurs abonnés de l'existence des outils de sécurité et de contrôle parental. Le second alinéa de l'article L. 331-35 du Code de la propriété intellectuelle dispose, en effet, que : « *En outre, les personnes visées au premier alinéa du présent article informent leurs nouveaux abonnés et les personnes reconduisant leur contrat d'abonnement sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins* ».

#### 1.3.2.2.1.4 La « réponse graduée »

Il s'agissait de l'un des principaux apports du projet de loi. Déjà censurée en 2006 par le Conseil constitutionnel à l'encontre de la « loi DADVSI » sur d'autres fondements[33], le Gouvernement a tenté de réintroduire ce mécanisme de réponse en trois étapes. Celui-ci consistait, lorsqu'un fait constitutif d'un téléchargement illégal était constaté, à permettre aux ayants droit, qui auront préalablement relevé l'adresse IP du responsable, de saisir la HADOPI pour qu'elle sollicite les FAI afin d'identifier l'abonné. Auparavant, seule l'autorité judiciaire pouvait ordonner la communication de l'identité du titulaire de l'abonnement au regard des données relevées par les agents assermentés. Désormais, la commission des droits est en

[33] Décision n°2006-540 DC du 27 juillet 2006 sur la loi relative aux droits d'auteur et aux droits voisins dans la société de l'information

mesure « *d'obtenir des opérateurs de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à des services de communication au public en ligne a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés sans l'autorisation des titulaires des droits prévus aux livres I*$^{er}$ *et II lorsqu'elle est requise* », selon le nouvel article **L. 331-21 du Code de la propriété intellectuelle**. Une fois l'identification réalisée, la HADOPI pourra mettre en œuvre sa « réponse graduée ». Cependant, et en vertu de la loi «HADOPI 1 », seuls les avertissements, c'est-à-dire, les deux premières étapes à caractère préventif, pourront être mises en œuvre dans le but de dissuader l'internaute dans la poursuite de ses actes. La loi « HADOPI 2 » permettra de mettre en œuvre la suspension de l'accès à internet, c'est-à-dire la dernière étape de la « réponse graduée », mais pas par la Haute autorité pour la protection des œuvres et la protection des droits sur internet elle-même, mais par un juge :

- Un e-mail d'avertissement est envoyé à l'internaute titulaire de la connexion par laquelle un téléchargement illégal a été réalisé,

- Malgré le premier e-mail, si de nouveaux manquements sont observés, la HADOPI procède à l'envoi d'une lettre recommandée avec accusé de réception afin que l'internaute prenne conscience des actes qu'il a commis.

- En cas de manquements répétés, le projet de loi « HADOPI 1 » prévoyait que la Commission de protection des droits de la HADOPI pouvait suspendre l'accès à internet pendant un délai s'étendant de deux mois à un an. L'abonnement devait alors être payé par son titulaire durant la durée de la suspension, à moins que l'abonné décide de résilier son contrat, auquel cas, il devait régler les frais de résiliation en vigueur.

Cette dernière étape a fait l'objet de la censure du Conseil constitutionnel selon lequel le rôle de cette commission et *a fortiori* de la HADOPI n'est pas de prononcer de sanction mais d'agir à titre préventif dans le cadre de sa mission de protection des œuvres et objets auxquels est attaché un droit d'auteur ou un droit voisin, par le biais d'envois de messages d'avertissements.

En effet, le Conseil considère que cette disposition, qui habilitait une autorité administrative indépendante à restreindre ou à empêcher l'accès à internet à des

titulaires d'abonnement, n'est pas conforme à la Constitution, en étant contraire à l'article 11 de la Déclaration des droits de l'Homme et du citoyen de 1789 qui vise la liberté de communication et d'expression car « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services* » (consid. 12). Le Conseil ajoute « *que la liberté d'expression et de communication est d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés* » (consid. 15).

Seul un juge est en mesure de prononcer une telle sanction afin de protéger les ayants droit victimes de téléchargements illégaux de leurs œuvres. De manière générale, il n'est pas exclu, par principe, qu'une autorité administrative puisse prononcer des sanctions « dans la mesure nécessaire à l'accomplissement de sa mission dès lors que l'exercice de ce pouvoir est assorti par la loi de mesures destinées à assurer la protection des droits et libertés constitutionnellement garantis » (consid. 14). En l'espèce, le Conseil en a déduit que la HADOPI ne répondait pas à ces conditions, dès lors que sa compétence « n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ».

#### 1.3.2.2.2 Présentation de la loi HADOPI 2

##### *1.3.2.2.2.1 Le double mécanisme de sanction[34]*

Cette loi, qui complète la loi « HADOPI 1 » dans son volet répressif, prévoit l'intervention d'un juge siégeant dans un tribunal correctionnel afin de procéder, notamment, à la suspension de la connexion internet des internautes ayant illicitement téléchargé une œuvre protégée. Ainsi, la HADOPI ne sanctionnera pas directement l'internaute mais est substituée dans le prononcé de la sanction par un juge unique par le biais d'ordonnances pénales (article 2).

La procédure ainsi choisie, dans le cadre de la loi « HADOPI 2 », réduit l'intervention du juge à un seul rôle « *administratif* ». Son intervention n'est en réalité prévue que

[34] Bitan H. « Réflexions sur la loi « Création et Internet » et sur le projet de loi « HADOPI 2 » RLDI 2009, n°51

pour se conformer à la décision rendue par le Conseil constitutionnel qui, le 10 juin 2009, déclarait inconstitutionnel le fait pour une autorité administrative, comme la HADOPI, de sanctionner un internaute auteur de téléchargement illégal tel que cela était envisagé.

En effet, l'article 1er de cette loi confère aux membres de la commission de protection des droits de la Haute autorité et à certains agents « *des prérogatives de police judiciaire leur permettant de constater les infractions et de recueillir les observations des personnes mises en cause* ».

En somme, la HADOPI instruira chaque dossier et le juge prononcera « *à l'encontre de leurs auteurs une suspension de l'accès au service pour une durée maximale d'un an, assortie de l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur* » (art. 3). Ainsi, s'il estime que les preuves réunies sont suffisantes, le juge rendra une ordonnance pénale qui informera l'internaute de sa culpabilité et de sa peine. Ce dernier disposera d'un délai de quarante-cinq jours pour former opposition à l'ordonnance.

En vertu de la « loi HADOPI 2 », la suspension de l'accès à internet pourra être prononcée à l'encontre de l'auteur de la contrefaçon commise au moyen d'un service de communication au public en ligne ou de communications électroniques. C'est une nouveauté, puisque la première « loi HADOPI » ne prévoyait pas de sanction à l'encontre du contrefacteur mais uniquement à l'encontre de l'abonné n'ayant pas sécurité sa connexion internet.

Désormais, lorsque l'acte de contrefaçon est commis au moyen d'un service de communication au public en ligne ou de communications électroniques, son auteur pourrait en principe se voir condamné, non seulement à la peine d'emprisonnement et à l'amende déjà prévues par les articles **L. 335-2, L. 335-3 et L. 335-4 du Code de la propriété intellectuelle,** soit 3 ans d'emprisonnement et 300 000 € d'amende, mais en outre, « *à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne ou de communications électroniques, pour une durée maximale d'un an* » (**C. propr. intell., art. L. 335-7 nv**).

De surcroît, comme dans la « loi HADOPI » censurée, la suspension sera « *assortie de l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur* » et n'affectera pas « *le versement du prix de l'abonnement au fournisseur de service* », l'article L. 121-84 du Code de la

consommation n'étant pas applicable pendant la période de suspension. En conséquence, en cas de résiliation, l'abonné supportera les frais de cette résiliation. Enfin, avec la disparition du fichier des « suspendus » prévu par la « loi HADOPI » censurée, l'internaute qui se réabonnerait au mépris de l'interdiction imposée par le juge est passible d'une peine de 2 ans de prison et 30 000 € d'amende, sur le fondement de l'article 434-41 du Code pénal sanctionnant l'atteinte à l'autorité de la justice.

Le deuxième mécanisme de sanction concerne le défaut de sécurisation par l'abonné non contrefacteur de sa connexion internet. C'est ce mécanisme qui remplace le dispositif initial.

À la suite des recommandations adressées à l'abonné par la commission de protection des droits le nouvel article **L. 331-37-1 du Code de la propriété intellectuelle** prévoit le principe d'une amende contraventionnelle de cinquième classe (1 500 €) prononcée par le Tribunal de police « *en cas de négligence caractérisée, à l'encontre du titulaire de l'accès à un service de communication au public en ligne ou de communications électroniques préalablement averti par la commission de protection des droits en application de l'article L. 331-26, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date d'envoi de la recommandation* ».

Cette amende pourra être assortie de la suspension de l'accès à internet, peine complémentaire qui « *pourra être prononcée selon les mêmes modalités* », c'est-à-dire avec interdiction de souscrire pendant la même période un autre contrat et obligation de verser le prix de l'abonnement au FAI. La durée maximale de la suspension ne pourra excéder un mois. Un décret devra préciser les éléments caractérisant la contravention. Mais le principe est posé, et la distinction avec l'article L. 335-7 du Code de la propriété intellectuelle clarifiée. En cas de réabonnement de l'internaute, ce dernier serait passible d'une amende de 3 750 €

Par ailleurs, les membres de la commission de protection des droits et les agents assermentés de la HADOPI seront habilités, en vertu du nouvel article **L. 331-21-1 du Code de la propriété intellectuelle** à constater la négligence caractérisée.

Dans tous les cas de suspension, lorsque la décision sera exécutoire, la peine complémentaire devra être notifiée à la HADOPI qui devra à son tour en notifier le fournisseur d'accès à internet. Ce dernier disposera alors d'un délai de 15 jours à

compter de la notification pour couper l'accès à internet de son client et sera passible d'une sanction de 5 000 € en cas de non-respect de cette notification.

#### *1.3.2.2.2.2 La protection des données personnelles*

##### *1.3.2.2.2.2.1 La qualification de l'adresse IP comme une donnée personnelle[35]*

Pour rappel, une adresse IP est « *une succession de chiffres qui permet d'identifier l'accès à partir duquel un ordinateur se connecte à l'internet* »[36.] L'adresse IP est ainsi l'équivalent du numéro de téléphone pour l'internet ; c'est un identifiant unique à un instant « t », permettant de distinguer un terminal connecté au réseau internet d'un autre terminal connecté à ce même réseau. Elle permet donc a priori d'échanger des messages sans erreur de correspondant.

À l'occasion de sa décision sur la loi « Création et Internet », le Conseil constitutionnel semble avoir reconnu la nature de données à caractère personnel des adresses IP. Il mettrait ainsi fin à une récente controverse qui s'est notamment traduite par des décisions contraires des juridictions parisiennes

En effet, défendant son projet de loi, la ministre de la Culture s'était alors prononcée contre la qualification de données personnelles appliquées aux adresses IP[37]. Pour ce faire, elle pouvait s'appuyer sur une position de la Cour d'appel de Paris, apparemment confirmée par la Cour de cassation.

Le **15 mai 2007**, la **Cour d'appel de Paris** avait, en effet, eu à se prononcer dans une espèce où un agent assermenté d'une société de gestion collection avait dressé un constat sur un réseau d'échange de fichiers sur l'internet. C'est précisément le cas de figure visé par la loi « Création et Internet ». La Cour de Paris avait jugé, de façon très nette, que l'adresse IP n'était pas une donnée personnelle[38]. Le **28 mai 2008**, elle confirmait sa position par un deuxième arrêt[39].

---

[35] Simon C. « Les adresses IP sont des données personnelles selon le Conseil constitutionnel », RLDI 2009, n°51

[36] Caron Ch., Qualification de l'adresse « IP » : état des lieux jurisprudentiel, in Comm. com. électr. 2007, n° 12, comm. 144. Repris par X. Buffet Delmas d'Autane et L. Morelli, De quelques évolutions importantes en matière de preuve de la contrefaçon, in Propr. industr. 2008, n° 11, étude 24.

[37] Commission des lois de l'Assemblée nationale, précité.

[38] CA Paris, 13e ch., sect. A, 15 mai 2007, n° 06/01954

[39] CA Paris, 3e ch., n° 07/01064, cité in Flament L., Le numéro d'IP n'est pas une donnée à caractère personnel. La cour d'appel de Paris persiste et signe !, in Dr. pén. 2008, n° 12, étude 27

Le **13 janvier 2009**, la **Cour de cassation** prenait à son tour position[40] et semblait entériner la solution adoptée précédemment par la Cour d'appel de Paris.

Cette position était contestée par la CNIL pour qui « *l'adresse IP présente toutes les caractéristiques d'une donnée à caractère personnel en ce qu'elle constitue un numéro d'identification permettant d'identifier indirectement, via le fournisseur d'accès à internet, une personne physique ayant souscrit un abonnement à internet dans le cadre duquel il utilise un ordinateur auquel ladite adresse IP est rattachée* »[41.] On sait que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés définit à son article 2, alinéa 2, les données à caractère personnel comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». La loi distingue donc deux types de données à caractère personnel : celles directement identifiantes (le nom patronymique par exemple) et celle indirectement identifiantes (un numéro de plaque minéralogique qui permet de remonter d'un véhicule à son propriétaire).

Enfin, un rapport du Sénat appelait à peine deux semaines avant la décision du Conseil constitutionnel à clarifier le statut juridique « flou » des adresses IP en France. Il recommandait que soit « *affirmé sans ambiguïté que l'adresse IP constitue une donnée à caractère personnel*»[42].

C'est finalement à ce courant que le Conseil constitutionnel semble s'être rattaché par sa décision du 10 juin 2009. En effet, c'est au détour du considérant 27 de sa décision que le Conseil constitutionnel prend position : « *Considérant que la lutte contre les pratiques de contrefaçon sur internet répond à l'objectif de sauvegarde de la propriété intellectuelle et de la création culturelle ; que, toutefois, l'autorisation donnée à des personnes privées de collecter les données permettant indirectement d'identifier les titulaires de l'accès à des services de communication au public en ligne conduit à la mise en œuvre, par ces personnes privées, d'un traitement de données à caractère personnel relatives à des infractions* (...) »

---

[40] Cass. crim., 13 janv. 2009, n°08-84.088.

[41] Réponse de la Cnil à un questionnaire adressé par l'Internet Society France sur les adresses IP et les données personnelles : <www.isoc.fr/reponse-de-la-cnil-sur-les-adresses-ip-et-les-donnees-personnelles-article0096.html>.

[42] Détraigne Y. et Escoffier A.-M., La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information, Rapport n°441 (2008-2009), Commission des lois du Sénat, 27 mai 2009

#### *1.3.2.2.2.2.2 La protection des données de connexion par les lois « HADOPI »*

Ce faisant, la loi « HADOPI 1 » précise que dans l'exercice de sa mission, la commission de protection des droits sera amenée à collecter et à traiter des données personnelles. L'article **L. 331-37 du Code de la propriété intellectuelle** autorise ainsi la HADOPI à créer un traitement automatisé de données à caractère personnel portant sur les personnes faisant l'objet d'une procédure d'avertissement, après décret de la Commission nationale de l'informatique et des libertés.

En effet, la commission recueillera, dans un premier temps, les adresses IP transmises par les ayants droit. Dans un second temps, les agents assermentés habilités par la HADOPI pourront, conformément à l'article **L. 331-21 du Code de la propriété intellectuelle**, obtenir, pour les nécessités de la procédure, tous documents, quel qu'en soit le support, y compris les données conservées et traitées par les opérateurs de communications électroniques (en particulier les FAI) et les hébergeurs, notamment l'identité, l'adresse, l'adresse électronique et les coordonnées téléphoniques de l'abonné. Enfin, la commission de protection des droits utilisera les adresses électroniques des abonnés pour leur adresser ses recommandations sous son timbre.

L'article 14 de la loi modifie en conséquence l'article L. 34-1 du Code des postes et communications électroniques, obligeant les opérateurs de communications électroniques à conserver les données pendant un an pour les besoins de la recherche d'un manquement à l'obligation de surveillance et à communiquer ces données à la HADOPI.

Concrètement, la commission de protection des droits pourra donc rendre nominatives les adresses IP.

Le Conseil a toutefois précisé que les données des abonnés « *ne pourront être transmises qu'à la HADOPI et aux autorités judiciaires* » et « *qu'il appartiendra à la Commission nationale de l'informatique et des libertés, saisie pour autoriser ces traitements, de s'assurer que les modalités de leur mise en œuvre, notamment les conditions de conservation des données, seront strictement proportionnées à cette finalité* » (consid. 29). La Cnil devra donc autoriser le traitement, et il lui appartiendra notamment de circonscrire, eu égard à la censure du pouvoir de sanction, le périmètre des données susceptibles d'être collectées et de préciser le délai dans lequel la commission de protection des droits devra effacer les données des

abonnés. A priori, en dehors de tout système de sanction ou de recours au juge, ces données devraient logiquement être effacées dès l'envoi de la deuxième recommandation.

Il est également prévu dans la loi « HADOPI 2 » que la peine de suspension d'abonnement ne sera pas inscrite sur le casier judiciaire, et que la Haute Autorité devra détruire les données personnelles de l'internaute sanctionné une fois son accès à internet rétabli. En effet, la commission devra procéder à « *l'effacement des données à caractère personnel relatives à l'abonné à l'issue de la période de suspension* ». De plus, l'internaute dont la connexion internet est suspendue (pour avoir illégalement téléchargé une œuvre protégée ou pour avoir négligé la protection de son accès internet) doit continuer de verser le prix de l'abonnement au fournisseur du service. S'il décidait de résilier son abonnement, il devra en supporter les frais.

Pour conclure cette partie consacrée au cadre normatif national et européen de lutte contre la cybercriminalité, il apparaît que la législation nationale et européenne permet de sanctionner un large aspect des infractions cybercriminelles. Ce dispositif normatif, pour être complet, suppose d'être couplé à des outils de coopération inter-institutions.

# LA COORDINATION DES ACTEURS ET LA CREATION D'OUTILS DE COOPERATION : LES PREMICES D'UNE REGULATION DES COMPORTEMENTS CYBERCRIMINELS DANS LE CYBERESPACE

## 2 La mise en place d'un cadre international de coopération pour garantir l'efficacité de la répression des actes cybercriminels dans le cyberespace

La cybercriminalité regroupe deux catégories de délits et de crimes : ceux de droits communs commis à l'aide ou exclusivement sur les réseaux numériques ; et les atteintes spécifiques aux données personnelles et aux atteintes spécifiques aux systèmes informatiques.

La répression des infractions de droit commun commises à l'aide ou exclusivement sur les réseaux numériques suppose l'application des règles de droit pénal général. En effet, la répression des infractions spécifiques contre les biens et prévue aux **articles 321-1 à 323-7 du Code pénal** qui répriment les atteintes aux systèmes automatisés de traitement de données (SATD). La répression des infractions contre les personnes est prévue aux **articles 226-16 à 22-24 du Code pénal** qui sanctionnent les atteintes aux données personnelles ayant fait l'objet d'un traitement informatique.

Les victimes d'actes de cybercriminalité portent rarement plainte. Les raisons tiennent à la difficulté d'identifier d'une part, l'auteur de l'infraction sur internet, et d'autre part, de collecter les preuves de l'infraction. En effet, bien que tout mode de preuve soit recevable en matière pénale (**C.pr.pén., art.427**), les preuves peuvent s'avérer difficiles à rapporter dans l'environnement numérique, d'autant que les délinquants peuvent aisément les détruire ou les déplacer. Cette difficulté s'aggrave si les données se trouvent dans un secteur localisé à l'étranger.

## 2.1 Les premières initiatives de coopération internationale : la prise de conscience d'une nécessaire action commune en matière de lutte contre la cybercriminalité

### 2.1.1 La nécessité d'une coopération entre les juridictions : les limites du principe de territorialité

Le principe de territorialité est prévu à **l'article 113-2 du Code de procédure pénal**. Il précise que la possibilité d'un accès en France aux contenus illicites suffit à constituer le délit et à attribuer la compétence aux juridictions nationales, quand bien même les responsables de ces faits se situeraient hors du territoire national. Aussi, le demandeur peut saisir la juridiction du lieu où demeure le défendeur, soit la juridiction du fait dommageable, soit la juridiction dans le ressort de laquelle le dommage a été subi.
La juridiction nationale est compétente pour connaître des faits commis par un étranger hors du territoire national dès lors que ces faits paraissent liés à une infraction imputable à cet étranger et dont elle est également saisit.

Concernant les infractions commises en dehors du territoire, la loi française est applicable à tout crime commis par un français hors du territoire national. En matière délictuelle, la loi pénale française est applicable aux ressortissants de tels agissements si les faits sont punis par la législation du pays où ils ont été commis (**C. pén., art. 113-6**), sauf en matière sexuelle (**C. pén., art. 227-27-1**).
Enfin la loi pénale française s'applique à tout crime ou délit puni d'emprisonnement commis par un français ou un étranger sur une victime de nationalité française (**C. pén., art. 113-7**)

En application du principe de territorialité, le juge pénal est compétent dès lors qu'un message, émanant d'un serveur localisé à l'étranger, peut être perçu par les internautes sur le territoire français.

En effet, la **Cour d'appel de Paris** a considéré dans sa décision du **17 mars 2004** que «*Considérant qu'il est constant que l'Internet connaît une dimension*

*internationale et qu'il n'existe pas, à l'heure actuelle, de règles de droit international élaborées ni même d'harmonisation entre les règles nationales, régissant la compétence du tribunal et la législation applicable aux délits de presse commis à partir ou grâce au réseau Internet ;*

*Qu'en l'état, les règles nationales trouvent donc à s'appliquer, quelles que soient les difficultés qui pourraient être invoquées par les exploitants de sites ou par les fournisseurs de contenus*».

Ensuite, dans sa décision du **9 septembre 2008**, la **chambre criminelle de la Cour de Cassation** a considéré que pour que le juge pénal soit compétent pour statuer sur des actes de contrefaçons réalisés par l'intermédiaire d'un site internet, il faut que le site internet soit actif à l'égard du public français, c'est-à-dire qu'il y ait un lien suffisamment étroit avec la France. Ce faisant, la contrefaçon sera perpétrée sur le territoire français car elle y produira suffisamment ses effets néfastes.

Par un arrêt du **8 décembre 2009**, la **Cour de cassation** est allée plus loin en estimant que, en matière de diffamation, « *le lieu de commission de l'infraction est celui où les menaces ont été proférées et non pas les pays où elles ont été rapportées par la voie télévisée ou de presse écrite ou électronique et par lesquelles l'intéressé a pu en prendre connaissance* ». En l'espèce, des menaces avaient été proférées en Croatie, lors d'une conférence de presse, et avaient été rapportées dans de nombreux pays du monde par les médias, notamment en France. Saisi d'une plainte de la victime, le juge d'instruction français avait rendu une ordonnance de refus d'informer au motif que le délit n'avait pas été commis en France, ce que la Cour de cassation a confirmé.

### 2.1.2 Les mesures politiques prises au niveau européen

La définition d'un cadre de coopération en matière de collecte des preuves dans un environnement numérique, a fait l'objet d'une pluralité d'initiatives politiques dans l'objet de couvrir l'ensemble des domaines concernés par les actes de cybercriminalité. L'objectif de cohérence de l'action européenne et de l'Union européenne ne semble pas avoir été rempli, mais ces mesures ont le mérite

d'instaurer une coopération dans des domaines aussi variés que l'action policière, douanière, le contenu diffusé sur internet…

La **recommandation du Conseil de l'Europe** en date du **11 septembre 1995** a pour objet d'harmoniser les règles de collecte des preuves entre les États. D'une part, il prévoit l'extension à l'environnement informatique de l'obligation traditionnelle qui incombe aux témoins et aux experts d'assister les autorités chargées de l'enquête dans la collecte de la preuve. Cette obligation peut consister à remettre des données, à permettre l'accès à ces données dans les systèmes informatiques ou l'interception d'informations sur un réseau. D'autre part, il garantit au mieux le caractère irréfutable et l'intégrité des preuves électroniques en développant notamment des procédures et méthodes techniques de traitement de ces preuves compatibles entre États et en habilitant les autorités compétentes à ordonner la conservation rapide des données. Les règles de preuve se rapportant aux documents traditionnels devraient s'étendre aux documents électroniques. Enfin, il souligne la nécessité de maîtriser les techniques de décryptage des données.

En parallèle, le Conseil de l'Europe suggérait la constitution d'unités spécialisées pour la répression d'infractions car les technologies de l'information requièrent une expérience spéciale. Cette proposition a été réitérée par Mme Falque-Pierrotin dans son rapport de 1996. La mise en œuvre de ces préconisations c'est faite progressivement et le rapport d'information du Sénat sur « **L'entrée dans la société de l'information** » énumère différents services spécialisés.

| Organisme | Mission |
|---|---|
| **Institut de recherche criminelle de la gendarmerie nationale (IRCGN)** | -Collecter les œuvres numériques afin de les rendre accessibles aux magistrats et aux enquêteurs<br>-missions d'expertise dans le cadre des enquêtes de police judiciaire |
| **Service technique de recherches judiciaires et de documentation (STRJD)** | -traquer les criminels et assister les unités locales de gendarmerie dans leurs investigations contre toutes les infractions |

| | |
|---|---|
| | commises sur internet<br>-analyse du contenu des matériels informatiques saisis lors des perquisitions<br>-surveillance d'internet |
| **Brigades d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)** | -Mission limité à Paris et aux 3 départements constituant la petite couronne : lutter contre les infractions au SATD et à la contrefaçon de logiciels/matériels<br>-lutte contre les infractions à la loi Informatique et libertés…<br>-Assister les autres services de la police judiciaire lorsqu'ils sont confrontés à du matériel informatique<br>-Mission pédagogique auprès des organismes public/privés en matière de fraude informatique<br>-Saisit par le JI et par le parquet |
| **Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)** | -Coordonner au niveau national les forces de police/gendarmerie en matière de lutte contre la cybercriminalité<br>-Formation des investigateurs en cybercriminalité<br>-Point de contact en France pour la coopération policière internationale avec Europol, Interpol et le G8 |
| **Division nationale pour la répression des atteintes aux personnes et aux biens** | Traitement des atteintes aux personnes/biens sur internet |
| **Investigateurs en cybercriminalité** | Recherche d'infractions liées aux nouvelles technologies |
| **DGDDI/DGCCRF** | Lutte contre la fraude dans leur domaine respectif |

Le décret du 1er mars 2011 relatif à l'obligation de communication et de conservation des données par les créateurs de contenus, pris en application de la loi relative à l'économie numérique, a été publié au Journal Officiel.
En vue d'éventuelles réquisitions judiciaires, les hébergeurs devront conserver des informations concernant leurs utilisateurs. Cette obligation concerne aussi les plates-formes de blogs, les sites de partage de vidéos à l'image de Dailymotion, qui vient d'être reconnu comme hébergeur par la Cour de cassation (**Cour Cass., 17 février 2011**).

Aux termes du présent décret, les données qui doivent être stockées sont celles fournies « *lors de la souscription d'un contrat ou la création d'un compte* », comme « *le nom et prénom du contributeur, ses adresses postales, ses pseudonymes, les adresses de courrier électronique ou de compte associées, les numéros de téléphone ou encore le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour* ». Les données devront être conservées pendant un an après la désinscription au service.
Les plates-formes devront également conserver pendant un an suivant la date de publication en ligne de vidéos, textes ou autre création : « *l'identifiant de la connexion, l'identifiant attribué par le système d'information au contenu, les types de protocoles utilisés, la nature ainsi que les date et heure de l'opération* ».

Dans une autre perspective, la **décision du 25 janvier 1999** du Parlement européen et du Conseil institue un programme pluriannuel visant à promouvoir une utilisation plus sûre d'internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux. Le programme c'est échelonné sur les périodes 1999-2002, 2002-2004, 2005-2008. Un nouveau programme pluriannuel est en cours de réalisation.
Ce plan d'action européen est structuré autour de 3 axes : mettre au point des systèmes de filtrage et de classement ; encourager les actions de sensibilisation, de soutient ; évaluation des implications juridiques et coordonner ce plan d'action avec des initiatives internationales similaires et évaluer l'impact des mesures européennes.

### 2.1.3 Le premier outil de coopération et de lutte contre la cybercriminalité

**L'affaire Yahoo !** souligne la nécessaire coopération entre les ordres juridiques nationaux afin d'assurer l'effectivité des décisions de jugement.
Le **22 mai 2000**, le juge des référés du TGI de Paris avait ordonné, sous astreinte, à la société américaine Yahoo de trouver des solutions techniques pour empêcher l'accès des internautes français au site d'enchères sur lequel figuraient des objets nazis dont la simple visualisation constitue une violation des dispositions de **l'article R 645-1 du code pénal**. Confirmée par le TGI de Paris le 20 novembre 2000, l'ordonnance de référé était accompagnée d'un rapport rédigé par un collège d'experts détaillant les mesures susceptibles d'être mises en œuvre, notamment en matière de filtrage des internautes en fonction de leur adresse électronique, afin de faire cesser ce trouble illicite à l'ordre public.

Pour devenir effectives, ces décisions françaises devaient néanmoins être confirmées par un juge américain. Or, avant même que le juge américain saisi au fond ne se soit prononcé, la société américaine s'est adressée à la Cour du 9ème district nord de Californie, selon la procédure dite de « jugement déclaratoire », afin qu'elle examine leur conformité aux dispositions de la constitution américaine protégeant la liberté d'expression. Dans son jugement du 7 novembre 2001, le juge Jeremy Fogel a estimé que les décisions françaises seraient « clairement incompatibles avec le 1er amendement si elles étaient rendues applicables aux Etats-Unis par un tribunal. [...] Bien que la France soit souveraine pour déterminer les limites de la liberté d'expression sur son territoire, cette Cour ne saurait faire exécuter une décision étrangère qui ne respecte pas la Constitution américaine, sauf à annihiler la liberté d'expression protégée à l'intérieur de nos frontières. [...] La Cour adhère nécessairement à certains jugements de valeur qui sont consubstantiels à ces normes, et notamment, à l'idée fondamentale du 1er amendement selon lequel il est préférable d'autoriser l'expression non violente d'avis choquants plutôt que d'imposer des idées issues de règles gouvernementales en matière d'expression ».

Dans cette mosaïque d'instruments juridiques, la Convention sur la cybercriminalité adoptée dans le cadre du Conseil de l'Europe à Budapest le 23 novembre 2001,

constitue le premier traité de coopération dans la collecte des preuves numériques et la lutte contre la cybercriminalité contraignant et complet. En effet, cette convention a pour objectif principal, énoncé dans le préambule, de poursuivre « *une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et l'amélioration de la coopération internationale*».

Pour ce faire, elle prévoit d'une part, la définition des moyens et des axes de la coopération internationale pour lutter efficacement contre les formes que prend la cybercriminalité. D'autre part, la définition des principes de base en matière de procédure afin de trouver et recueillir les preuves électroniques nécessaires à découvrir et poursuivre les auteurs d'infractions perpétrées au moyen des réseaux numérique (conservation des données, perquisition et saisie informatique, collecte de données, interception de communication).

La Convention demande à ce que les États membres adoptent des mesures législatives et autres, nécessaires pour instaurer les pouvoirs et procédures aux fins d'enquêtes ou de procédures pénales spécifiques. Ainsi, les autorités compétentes doivent pouvoir perquisitionner et saisir les informations relatives à l'infraction liée à l'utilisation de l'informatique.

De même, les autorités compétentes pourront collecter les données relatives au trafic et intercepter les données relatives au contenu, soit directement, soit en obligeant le fournisseur de services. Ainsi, chaque pays devra prévoir un système d'interception, ce qui en France existe déjà puisque l'autorité judiciaire peut procéder par voie de réquisition auprès des opérateurs téléphoniques qui doivent alors fournir les données de connexion et s'agissant du contenu des communications, les dispositions sur la législation sur les écoutes téléphoniques à vocation à s'appliquer.

Par ailleurs, les États signataires s'engagent à mener des enquêtes et à mettre en œuvre des moyens coercitifs sur leur territoire, pour le compte d'une partie requérante, du moment que les infractions poursuivies tombent sous le coup de la Convention. En effet, dès le préambule, le projet affirme « *qu'une lutte bien menée*

*contre la cybercriminalité requiert une coopération internationale en matière pénale, rapide et efficace*».

Le chapitre III du projet de Convention, relatif à la coopération internationale, invite les parties à collaborer, «*dans la mesure du possible les unes avec les autres, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électroniques d'une infraction pénale*». Ainsi, il est prévu, l'extradition, pour les infractions pénales, définies dans la convention et punissables, pour les deux États concernés, par une peine privative de liberté, pour une période maximale d'au moins un an ou par une peine plus sévère. Il sera donc désormais possible d'obtenir une extradition auprès d'un pays membre de la Convention si une incrimination est prévue à la Convention et alors même que l'État n'a pas conclu d'accord bilatéral de coopération judiciaire d'extradition.

Selon les termes de la Convention, les services d'enquêtes des États doivent s'unir et s'entendre pour effectuer les actes d'enquête au lieu et place des services demandeurs et leur communiquer les résultats obtenus. Ce qui constitue une nouvelle forme de coopération judiciaire en sus des formes traditionnelles d'entraide et d'extradition. Aussi, et à titre d'illustration, il pourra être procédé à une perquisition et saisie pour le compte d'un autre État et toutes les informations utiles à l'enquête de l'État requérant devront être transmises notamment lorsqu'elles auront transitées par un État intermédiaire.

En matière d'extradition, la Convention dispose que si celle-ci est refusée sur la base de la nationalité de la personne recherchée ou parce que la partie requise s'estime compétente pour cette infraction, à la demande de l'État requérant, l'État requis soumettra l'affaire à ses autorités compétentes aux fins de poursuite à charge de rendre compte, à la partie requérante, de l'issue de l'affaire.

## 2.2 Les mesures efficaces et concrètes adoptées au niveau européen et mondial en matière de collecte des preuves et de coopération

### 2.2.1 Un régime de coopération entre magistrats en matière d'extradition

La loi pénale française est applicable aux infractions commises en France (**C. pén., art. 113-1**). L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ces faits constitutifs a eu lieu sur le territoire (**C. pén., art.113-2**). En outre, la loi pénale française est applicable aux crimes et délits punis d'une peine d'emprisonnement commis hors du territoire national par un français ou par un étranger lorsque la victime est française.

L'extradition est le moyen juridique pour un État de demander à un État requis la mise à disposition d'une personne afin de procéder à sa traduction devant une juridiction de jugement ou à l'exécution de sa peine. La France a ratifié la **Convention européenne d'extradition du 13 décembre 1957**. En-dehors d'un texte international applicable, le droit national applicable est régi par la loi du 10 mars 1927.

Parmi les principes majeurs applicables, pour qu'une extradition obtienne une réponse favorable, il faut que dans les 2 pays l'infraction constatée soit considérée comme un crime, selon le principe de la double incrimination ou réponde à un seuil minimum de gravité. L'extradition pourra ne pas être prononcée par un État à l'égard d'un de ses ressortissants. En outre, conformément aux bonnes pratiques adoptées par les États du G8, un pays refusant l'extradition pour des motifs de nationalité s'engage à soumettre l'affaire à ses autorités judiciaires nationales en vu d'engager des poursuites contre la personne en cause.

Au niveau de l'Union Européenne, divers dispositifs ont été mis en œuvre afin de faciliter les procédures d'extradition entre les États membres. Par un acte du **10 mars 1995**, le Conseil a établi la **Convention relative à la procédure simplifiée**

**d'extradition entre les États membres de l'Union européenne**. La présente convention vise à faciliter l'application entre les États membres de l'application de la Convention européenne d'extradition du 13 décembre 1957, en complétant les dispositions de celle-ci. La Convention européenne d'extradition a été conçue sous l'égide du Conseil de l'Europe.

La convention prévoit l'obligation pour les États membres de remettre les personnes recherchées à des fins d'extradition selon la procédure simplifiée qu'elle détermine, à la double condition que la personne concernée consente à son extradition et que l'État requis donne son accord. En particulier, elle ne subordonne plus la remise de la personne ayant fait l'objet d'une demande d'arrestation à la présentation d'une demande d'extradition et des autres documents requis par l'article 12 de la Convention européenne d'extradition.

Chaque État membre indique dans une déclaration quelles sont les autorités compétentes pour la procédure simplifiée d'extradition.

Pour être exhaustif, il faut rappeler l'existence de la Convention sur l'extradition prévue par un acte du Conseil du 27 septembre 1996. Bien qu'elle ait été remplacée depuis le 1er janvier 2004 par la **décision cadre du Conseil**, du **13 juin 2002**, relative au mandat d'arrêt européen et aux procédures de remise entre États membres, elle s'applique dans les cas non régis par les règles du mandat d'arrêt européen.

La Convention vise à faciliter l'extradition entre les États membres dans les cas qu'elle énonce. Elle prévoit à cette fin une série de principes auxquels les États membres peuvent déroger à certaines conditions. La plupart des États membres ayant à ce jour ratifié la convention ont notifié des réserves en ce sens.

La Convention précise tout d'abord les faits auxquels la procédure d'extradition est applicable. Il s'agit des faits punis par la loi de l'État membre requérant d'une peine privative de liberté ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins douze mois et par la loi de l'État membre requis d'une peine privative de liberté ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins six mois. La convention facilite de manière plus spécifique l'extradition en matière de

conspiration ou d'association de malfaiteurs si ces dernières ont pour but de commettre notamment: une ou plusieurs des infractions visées aux articles 1 et 2 de la Convention européenne pour la répression du terrorisme; toute autre infraction relevant du trafic de stupéfiants ou de certaines formes de criminalité dirigées contre les droits de la personne ou créant un danger collectif.

Sauf réserve exprimée par tout État membre, l'extradition ne peut pas être en principe refusée au motif que la personne qui fait l'objet de la demande d'extradition est un ressortissant de l'État membre requis.

En règle générale, l'extradition ne peut pas non plus être refusée au motif qu'il y a prescription de l'action ou de la peine selon la législation de l'État requis, mais, en revanche, elle doit être refusée pour une infraction couverte par l'amnistie.

### 2.2.2 La création d'organes spécialisés dans la coopération en matière de collecte des preuves et de lutte contre la cybercriminalité

La Convention sur la cybercriminalité complète l'action d'organismes européens chargées de promouvoir la coopération en matière de collecte des preuves numériques et de lutte contre la cybercriminalité. Au niveau mondial, des organismes aux compétences similaires ont été institués, ce qui complète la panoplie des outils de coopération propres à l'Union européenne.

Tout d'abord, **Europol** a été créé lors de la convention signée à Bruxelles le **26 juillet 1995**, devenu **Office européen de police** depuis le **1 janvier 2010.**

La **décision du Conseil du 6 avril 2009** portant création de l'Office européen de police institue l'Office européen de police (Europol) en vue de soutenir et de renforcer la coopération mutuelle entre les États membres dans la prévention et la lutte contre le terrorisme, la criminalité organisée et d'autres formes graves de criminalité. Europol siège à La Haye, aux Pays-Bas, et a la personnalité juridique.

Europol est compétent dans des situations affectant deux États membres ou plus, de sorte qu'une action commune s'impose pour lutter contre la criminalité organisée, le

terrorisme et d'autres formes graves de criminalité. Sa compétence couvre également les infractions connexes.

Europol remplit les fonctions principales suivantes: collecte, stockage, analyse et échange des informations ; assistance aux États membres dans le cadre des enquêtes, demander et coordonner les enquêtes dans des affaires précises…

Chaque État membre désigne une unité nationale qui constitue le seul organe de liaison entre Europol et les autorités compétentes des États membres. Chaque unité nationale détache auprès d'Europol au moins un officier de liaison, qui constituera un bureau national de liaison. Ces officiers représentent les intérêts de leur unité nationale et facilitent l'échange d'informations entre ces unités et Europol.

Europol peut traiter les informations et les renseignements, y compris les données à caractère personnel, aux fins d'exécution de ses fonctions. À cet effet, un système d'information Europol et des fichiers de travail à des fins d'analyse sont créés. Les données saisies dans le système peuvent concerner des personnes qui ont commis ou qui sont suspectées d'organiser une infraction pénale. Il peut s'agir de données directement liées à la personne (nom, nationalité, numéro de sécurité sociale, etc.) et à l'infraction commise. Les unités nationales, les officiers de liaison et le personnel d'Europol peuvent entrer et supprimer des données directement dans le système. Les autorités compétentes désignées des États membres peuvent consulter le système pour vérifier que les données demandées sont disponibles. Les fichiers de travail à des fins d'analyse peuvent être ouverts par Europol pour assembler, traiter ou utiliser des données nécessaires en appui aux enquêtes pénales. Outre les données relatives aux personnes qui ont commis ou qui sont suspectées d'avoir commis une infraction, les fichiers peuvent contenir des données sur les témoignages, les victimes, les contacts et associés de l'auteur de l'infraction.

Toute donnée à caractère personnel extraite des fichiers d'Europol peut être utilisée uniquement par les autorités compétentes des États membres aux fins de prévention et de lutte contre la criminalité. Europol peut utiliser les données à caractère personnel uniquement dans l'exercice de ses fonctions. Un État membre ou un pays tiers ou un organe peut fixer d'autres restrictions à l'utilisation de certaines données communiquées.

Toute personne a le droit de demander une vérification des données à caractère personnel qui la concernent ou d'y accéder. En cas d'erreur, cette personne a le droit de demander la correction ou la suppression des données.

Une autorité de contrôle nationale dans chaque État membre assure que l'entrée, la récupération et la communication des données personnelles par les États membres sont légales. L'autorité de contrôle commune veille à la licéité du stockage, du traitement, de l'utilisation et de la transmission de données à caractère personnel par Europol.

Créée en 2002 (**Décision du Conseil 2002/187/JAI du 28 février 2002**), Eurojust a pour finalité d'instituer une coordination judiciaire entre les États membres. Cette unité est composée de 27 représentants nationaux : procureurs, magistrats et officiers de policiers des États membres de l'UE ayant des compétences équivalentes, détachés par chaque État membre conformément à son système juridique. Chaque EM peut également désigner un ou plusieurs correspondants nationaux qui peuvent aussi constituer un point de contact du réseau judiciaire européen.
Eurojust a pour mission d'intervenir dans les enquêtes et les poursuites contre la criminalité organisée ou transfrontalière pour assurer la coordination entre les autorités des États membres, ainsi que le suivi de l'entraide judiciaire internationale, et les demandes d'exécution d'extradition ou du mandat d'arrêt européen. Il apporte également son concours dans les enquêtes pénales des États membres sur la base des analyses effectuées par Europol.

Un dispositif permanent de coordination (DPC) sera instauré avec un représentant de chaque État membre et avec un correspondant chez Eurojust. Il sera disponible 24 heures/24 et 7 jours/7 de manière à assurer qu'Eurojust puisse agir à tout moment.

Eurojust peut accomplir ses missions tant par l'intermédiaire d'un ou de plusieurs membres nationaux qu'en tant que collège. Eurojust peut demander, entre autres, aux autorités des États membres concernés: d'entreprendre une enquête ou des poursuites ; de mettre en place une équipe commune d'enquête ; de prendre des mesures spéciales ou d'autres mesures d'enquête.

Eurojust peut obtenir et conserver des données de même nature que celles prévues pour Europol.

Au sein d'Eurojust, un membre du personnel est spécialement désigné pour la protection des données. Il assure, entre autres, le traitement licite, la conservation d'une trace écrite de la transmission ainsi que de la réception des données. Les données ne sont conservées que pour la période strictement nécessaire à la conclusion de l'activité d'Eurojust. En tout état de cause, une vérification périodique est prévue tous les trois ans. Eurojust et les États membres protègent les données, en particulier, contre la destruction, la perte, la divulgation, la modification et l'accès illicite.

Un organe ayant caractère indépendant contrôle toutes les activités d'Eurojust afin d'assurer que les données à caractère personnel sont traitées dans le respect de la décision. L'organe de contrôle commun se réunit périodiquement et lorsqu'il est convoqué par son président. Celui-ci est désigné par les membres permanents qui sont dans leur troisième année de mandat.

Afin d'accomplir ses missions, Eurojust entretient des relations privilégiées avec le réseau judiciaire européen, l'Office européen de police, l'Office européen de lutte antifraude, l'Agence européenne aux frontières extérieures, et le Centre de situation conjoint de l'Union européenne. Après approbation par le Conseil, Eurojust pourra conclure des accords de coopération sur l'échange d'informations avec des États tiers, des organisations ou instances internationales et l'Organisation internationale de police criminelle (Interpol). Par ailleurs, Eurojust peut coordonner la coopération judiciaire avec des pays tiers et poster des magistrats de liaison dans ces États pour faciliter cette coopération.

Enfin, en matière de lutte contre la pédopornographie, qui constitue un aspect de la cybercriminalité, différentes mesures permettent à l'Union européenne de lutter contre l'exploitation sexuelle des enfants (action commune de 1997, extension du mandat d'Europol) ou la diffusion de messages à contenu illicite et préjudiciable sur Internet (plan d'action communautaire visant à promouvoir une utilisation plus sûre d'Internet . Toutefois, un acte consacré spécifiquement à la lutte contre la

pédopornographie sur Internet est apparu nécessaire en raison de l'ampleur prise par cette forme de criminalité.

Des mesures seront prises par les États membres afin de:

- encourager les utilisateurs d'Internet à signaler aux autorités répressives les cas de diffusion présumée de matériel pédopornographique sur Internet;
- garantir que les infractions commises fassent l'objet d'enquêtes et soient réprimées, grâce à la création d'unités spécialisées au sein des services répressifs par exemple;
- assurer la réaction rapide des autorités répressives lorsqu'elles reçoivent des informations sur des cas présumés de production, de traitement, de diffusion et de détention de matériel pédopornographique.

De plus, les États membres vérifient régulièrement si l'évolution technologique nécessite une modification de leur procédure pénale dans le domaine de la lutte contre la pédopornographie sur Internet.

Pour faciliter la collaboration entre les États, une liste des points de contacts nationaux disponibles 24 heures sur 24 et des unités spécialisées sera diffusée. Europol devra être informé des cas de présomption de pédopornographie et des réunions entre les services spécialisés nationaux seront organisées.

Les États membres examinent toute mesure qui permettrait d'éliminer la pédopornographie sur Internet et échangent leurs meilleures pratiques. De nouvelles obligations pour les fournisseurs de services Internet seront étudiées: information des autorités compétentes en cas de diffusion de matériel pédopornographique par leur intermédiaire, retrait de tel matériel, conservation de ce matériel pour le mettre à la disposition des autorités, voire création de leurs propres systèmes de contrôle. En partenariat avec le secteur industriel, la création de filtres ou d'autres dispositifs techniques empêchant et détectant ce type de matériel sera encouragée.

Le Conseil organisera des visites sur place afin d'évaluer dans quelle mesure les États membres respectent les obligations découlant de la décision du Conseil. En fonction des résultats de ces évaluations, il examinera la nécessité d'adopter des mesures supplémentaires.

À ces organes propres à l'Union européenne, s'ajoutent des acteurs qui ont une vocation mondiale, qui complètent ainsi leur action. Il est d'ailleurs prévu l'adhésion des États membres de l'Union européenne à ces organismes voire leur coopération à travers leurs institutions judiciaires.

En effet, le **G8 High-Tech Crime Subgroup** (HTCSG), composé des fonctionnaires des ministères de l'Intérieur et de la Justice de chacun des pays du G8 et de la Commission, s'est réuni régulièrement depuis 1997 et s'est imposé comme leader face aux problèmes croissants induits par le cybercrime. Le High-Tech Crime Subgroup a crée un réseau disponible 24 heures/24 et 7jours/7 (24/7 contact) : le High-Tech Crime Point of Contact Network conçu pour faciliter une coopération internationale rapide, en particulier dans la sauvegarde et la sécurisation des preuves électroniques dans des affaires de cybercrime de haute importance.
L'objectif de cet organe est d'encourager une coopération opérationnelle dans les affaires en cours, et d'éviter la perte des traces électroniques.

Par une **recommandation du 25 juin 2001,** concernant les points de contact assurant un service vingt-quatre heures sur vingt-quatre pour lutter contre la criminalité liée à la haute technologie, le Conseil invite les États membres à adhérer au réseau d'information du G8 (accessible vingt-quatre heures sur vingt-quatre) afin de traiter le plus rapidement possible et de manière qualifiée les différents types de criminalité liés à la haute technologie et de mieux préserver les preuves. Ce réseau permettra aux pays adhérents d'avoir une vue d'ensemble de la criminalité liée aux systèmes informatiques vu qu'elle s'exerce souvent dans plusieurs pays en même temps.

À l'occasion d'une réunion qui s'est tenue à **Washington les 9 et 10 décembre 1997**, les ministres de la justice et des affaires intérieures du G8 avaient adopté les principes fondateurs du réseau. Ensuite, un plan d'action avait été adopté, prévoyant d'accueillir aussi les pays qui ne font pas partie du G8. Le réseau a été mis en place dans la période allant de 1998 à 2000.

Les États membres de l'Union européenne ne faisant pas partie du réseau susmentionné ont adhéré au "National Central Reference Point System" (NCRP) d'Interpol. Toutefois, il faut souligner que les points de référence centraux nationaux

d'Interpol ne sont pas toujours ouverts vingt-quatre heures sur vingt-quatre. Les deux réseaux travailleront dans un esprit de collaboration. En outre, les États membres de l'Union européenne qui ne font pas partie du G8 devraient pouvoir rendre opérationnelles vingt-quatre heures sur vingt-quatre leurs unités spécialisées qui font partie du réseau d'Interpol.

Ensuite, **Interpol**, créé en 1923 compte 183 pays membres. Son rôle consiste à coordonner l'action des polices des États membres et les échanges d'informations afin de leur faciliter la lutte contre le trafic de stupéfiants, le terrorisme, la criminalité informatique ou économique. À cet effet, il collecte, recoupe et regroupe les informations collectées par ses Bureaux centraux nationaux (BCN), constituant ainsi un puissant dispositif de stockage et d'échanges d'informations entre policiers des pays membres. Interpol dispose de points de contacts fonctionnant 24h/24 et 7 jours/7 dans les services de police des États associés.

En France c'est l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication qui remplit ce rôle.

Interpol dispose également d'une base de données centrale, notamment sur les empreintes digitales, alimentée par plusieurs États. Il prévoit également la création d'une base de données internationale sur l'exploitation sexuelle des enfants. Enfin, Interpol a créé une cellule spéciale dénommée « projet Guardian » pour lutter contre l'exploitation des enfants sur Internet, notamment l'utilisation des photographies de mineurs destinés à encourager leur exploitation sexuelle.

### 2.2.3 L'institutionnalisation d'un espace juridique européen

L'Union européenne a créé un espace institutionnalisé de coopération en matière de captation et d'échange des données numériques. Cet espace a permis de développer des outils propres à favoriser la coopération en matière pénale entre les magistrats de l'Union européenne.

Le **14 juin 1985** a été conclu à Schengen, un accord visant dans le cadre défini par l'acte unique européen, la création d'un espace communautaire sans frontières intérieures. Une convention signée en 1990 complète cet accord et en

précise les modalités d'application. La création de l'espace Schengen suppose la suppression des frontières intérieures, le renforcement des contrôles aux frontières extérieures, une coopération policière et judiciaire renforcée, et la mise en place d'une politique commune des visas.

Le système d'information Schengen (SIS) permet la collecte automatisée de données sur les personnes et l'échange d'informations entre les États signataires. Ces outils sont susceptibles d'être utilisés aux fins de la répression de la diffusion et du recel d'images pédopornographiques entre États frontaliers signataires.

Des dérogations ont été accordées à certains états pour qu'ils puissent participer à la construction de l'espace Schengen : le Danemark peut choisir d'appliquer ou non toute nouvelle mesure fondée sur l'ex titre IV du traité CE, aujourd'hui titre VII du traité sur le fonctionnement de l'Union européenne, dans le cadre de l'Union européenne. Le Danemark est toutefois lié par certaines mesures en matière de politique commune des visas ; l'Irlande et le Royaume-Uni peuvent participer à tout ou partie des dispositions de l'acquis de Schengen après un vote du Conseil à l'unanimité des États parties aux accords et du représentant du gouvernement de l'État concerné ; enfin, l'Islande, la Norvège, la Suisse et le Liechtenstein ont le statut de pays associés.

Actuellement, le système d'information Schengen permet aux autorités compétentes des États membres de disposer d'informations relatives à certaines catégories de personnes et d'objets. Il constitue donc un élément essentiel au bon fonctionnement de l'espace de sécurité, de liberté et de justice. À ce propos, il contribue à la mise en œuvre des dispositions prévues tant en matière de circulation des personnes qu'en ce qui concerne la coopération judiciaire en matière pénale et la coopération policière.

Diverses règlementations européennes se sont succédées afin de renforcer l'efficacité de la capture, du traitement, de l'accès et de l'échange des données enregistrées au sein du système d'information Schengen. Aussi, Europol et Eurojust ont accès aux données introduites dans le Système d'information Schengen, ainsi que les autorités judiciaires nationales responsables en matière de poursuite dans le cadre des procédures pénales et des enquêtes judiciaires…

Une **décision du Conseil 2007/533/JAI** du **12 mai 2007** prévoit la mise en place d'un système d'information Schengen de deuxième génération (SIS II)

Cette décision ajoute des données qui pourront être enregistrées afin de soutenir la coopération opérationnelle entre la police et les autorités judiciaires en matière pénale : données sur les personnes disparues, les personnes recherchées en vue d'une arrestation ou d'une extradition, les objets en vue de leur saisie dans le cadre d'une procédure pénale…

Un État membre signalant est responsable de l'exactitude, de l'actualité et de la licéité de l'introduction de données dans le système information Schengen II. Seul l'État membre signalant est autorisé à modifier, compléter, rectifier, mettre à jour ou effacer les données qu'il a introduites.

La décision définit le régime de conservation des données en fonction de leur nature et de leur finalité.

L'Union européenne a ensuite créé des procédures de coopérations entre magistrats européens dans le cadre de la poursuite en matière pénale.

Par une **décision cadre n°2002/584/JAI du 13 juin 2002** , le Conseil institut le mandat d'arrêt européen.

Le Conseil européen de Tampere des 15 et 16 octobre 1999 invitait les États membres à faire du principe de la reconnaissance mutuelle la «pierre angulaire» d'un véritable espace judiciaire européen.

Toutefois, les États membres restent libres d'appliquer et de conclure des accords bilatéraux ou multilatéraux dans la mesure ou ceux-ci facilitent ou simplifient davantage les procédures de remise.

La présente décision-cadre définit le mandat d'arrêt européen comme toute décision judiciaire adoptée par un État membre en vue de l'arrestation ou de la remise par un autre État membre d'une personne aux fins de : l'exercice de poursuites pénales, l'exécution d'une peine, et l'exécution d'une mesure de sûreté privative de liberté.

Le mandat est applicable en présence d'une condamnation définitive à une peine d'emprisonnement ou une mesure de sûreté ayant, au moins, une durée de 4 mois; ou d'une infraction pour laquelle une peine d'emprisonnement ou une mesure de sûreté d'un maximum supérieure à un an est prévue. À condition qu'elles soient punies dans l'État membre d'émission par une peine d'au moins trois ans, les infractions pouvant donner lieu à la remise sans contrôle de la double incrimination du fait sont, entre autres: le terrorisme, la traite des êtres humains, la corruption, la participation à une organisation criminelle, le faux monnayage, l'homicide, le racisme et la xénophobie, le viol, le trafic de véhicules volés, la fraude, y compris la fraude aux intérêts financiers de l'Union.

Pour les actes criminels autres que ceux susmentionnés, la remise peut être subordonnée à la condition que le fait pour lequel est demandée la remise constitue une infraction en application du droit de l'État membre d'exécution (règle de la double incrimination), sauf lorsque l'incrimination est punie de 3 ans d'emprisonnement.

Chaque État membre ne donne pas exécution au mandat d'arrêt européen si: un jugement définitif a déjà été rendu par un État membre pour la même infraction contre la même personne (principe de *"ne bis in idem"*), l'infraction est couverte par une amnistie dans l'État membre d'exécution, la personne concernée ne peut pas être considérée responsable par l'État membre d'exécution en raison de son âge.

En présence d'autres conditions (prescription de l'action pénale ou de la peine en application des dispositions de l'État membre d'exécution, jugement définitif pour le même fait émis par un pays tiers, etc.), l'État membre d'exécution peut refuser de donner exécution au mandat. Il peut également refuser d'exécuter un mandat si la personne concernée ne s'est pas présentée en personne au procès où la décision a été rendue, sauf si des garanties appropriées sont prévues. En tout état de cause, le refus doit être motivé.

Les mesures relatives au mandat d'arrêt européen sont codifiées à l'**article 695-23 du Code pénal** par la **loi n° 2004-204 du 9 mars 2004** portant adaptation de la justice aux évolutions de la criminalité

De plus, par une **décision-cadre 2008/978/JAI du Conseil du 18 décembre 2008** est institué un mandat européen d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédures pénales.

Le mandat européen d'obtention de preuves est une décision judiciaire qui permet d'obtenir des objets, des documents et des données de la part d'un autre État membre. Le mandat européen d'obtention de preuves est émis par les autorités compétentes désignées par les États membres. Une autorité d'émission peut être un juge, une juridiction, un magistrat instructeur, un procureur ou une autre autorité judiciaire. Les États membres doivent également désigner les autorités compétentes pour reconnaître et exécuter le mandat européen d'obtention de preuves.

L'État d'émission doit s'assurer que les preuves demandées sont nécessaires et proportionnées aux fins de ces procédures. En outre, l'obtention de telles preuves dans des circonstances similaires au sein de l'État d'émission doit être prévue dans son droit national. Le mandat européen d'obtention de preuves ne peut être émis que lorsque ces conditions sont réunies.

Lorsque l'autorité compétente d'un État d'émission est fondée à croire que des preuves pertinentes se trouvent sur le territoire d'un autre État membre, elle peut transmettre le mandat européen d'obtention de preuves à l'autorité compétente de cet État membre. Le mandat européen d'obtention de preuves doit être transmis sans attendre par l'autorité d'émission à l'autorité d'exécution par un moyen permettant de laisser une trace écrite. À cette fin, les États membres peuvent désigner une ou plusieurs autorités centrales qui assisteront les autorités compétentes. Les États membres peuvent également utiliser le système de télécommunication sécurisé du Réseau judiciaire européen pour la transmission de mandats européens d'obtention de preuves.

L'autorité d'exécution reconnaît le mandat européen d'obtention de preuves sans aucune autre formalité. L'autorité d'exécution prend les mesures nécessaires pour exécuter le mandat européen d'obtention de preuves, à moins qu'elle ne décide de se prévaloir d'un motif de non-reconnaissance, de non-exécution ou de report. Si le mandat européen d'obtention de preuves n'a pas été émis ou validé par un juge, une

juridiction, un magistrat instructeur ou un procureur, l'autorité d'exécution peut décider que l'exécution du mandat ne donne pas lieu à une perquisition ou à une saisie. Toutefois, l'autorité d'exécution doit consulter l'autorité compétente de l'État d'émission avant de statuer. Les États membres peuvent déclarer qu'ils demandent une telle validation si, dans une procédure nationale similaire, leur loi exige que les mesures d'exécution soient ordonnées ou dirigées par un juge, une juridiction, un magistrat instructeur ou un procureur.

Sauf stipulation contraire dans la décision-cadre, l'autorité d'exécution respecte les formalités prévues par l'autorité d'émission. Toutefois, ces formalités ne doivent pas être contraires aux principes fondamentaux du droit de l'État d'exécution.

L'État d'exécution peut refuser de reconnaître ou d'exécuter le mandat européen d'obtention de preuves dans un délai de trente jours après sa réception dans certaines conditions définies par la décision.

La reconnaissance ou l'exécution d'un mandat européen d'obtention de preuves ne peut être subordonnée au contrôle de la double incrimination que si une perquisition ou une saisie est nécessaire pour son exécution et s'il n'est pas lié aux infractions énumérées dans la décision-cadre.

Les États membres doivent s'assurer que la reconnaissance et l'exécution d'un mandat européen d'obtention de preuves puissent faire l'objet d'un recours juridique de la part de toute personne concernée. Ces recours peuvent être limités aux cas où des mesures coercitives sont employées. Les actions sont engagées devant une juridiction de l'État d'exécution; toutefois, les motifs de fond à l'origine de l'émission du mandat européen d'obtention de preuves ne peuvent être contestés que devant une juridiction de l'État d'émission.

Enfin, la **décision du Conseil 2008/976/JAI du 16 décembre 2008** institue le réseau judiciaire européen.

Le réseau est composé des autorités centrales des États membres et d'autres autorités compétentes à des fins de coopération judiciaire internationale. Chaque État membre établit un ou plusieurs points de contact judiciaires parmi lesquels un

correspondant national est désigné pour le réseau. Les États membres désignent aussi un correspondant chargé des aspects techniques. Les magistrats de liaison nationaux, qui remplissent des fonctions analogues à celles des points de contact, sont également associés au réseau. La Commission nomme un point de contact pour les questions qui lui incombent.

La principale tâche du réseau est de faciliter la coopération judiciaire entre les États membres en matière pénale en améliorant la communication entre les points de contact, en organisant des réunions périodiques des représentants des États membres et en fournissant les informations de base nécessaires.

Les points de contact sont des intermédiaires chargés de faciliter la coopération judiciaire entre les États membres en matière de lutte contre toutes les formes graves de criminalité. Leur rôle est d'établir des contacts directs avec les autorités judiciaires locales et les autres autorités compétentes, ainsi qu'avec les autres points de contact au sein de l'Union européenne. À cette fin, les points de contact doivent échanger et fournir aux autorités compétentes les informations juridiques et pratiques nécessaires.

Pour conclure cette partie, l'on peut constater que les outils de coopération tant normatifs qu'institutionnel permettent d'appréhender le développement de la cybercriminalité. Cependant, l'efficacité de tels dispositifs supposent en amont une formation adéquate des personnels concernés aux méthodes de travail dispensées hors du territoire national, ainsi qu'une sensibilisation aux enjeux de la coopération institutionnelle entre les différentes administrations nationales, vouées à travailler de concert si les États membres souhaitent sanctionner efficacement les cybercriminels.

Ceci d'autant que les infractions cybercriminelles sont commises au sein d'un environnement dématérialisé : le cyberespace.

# 3 La régulation du cyberespace : un enjeux juridique et géopolitique contemporain

## 3.1 Quelques considérations sur le droit du cyberespace

### 3.1.1 Les diverses techniques de réglementation de l'Internet et le rôle du droit étatique

### 3.1.2 De la diversité des modes de réglementation

Une réglementation a pour but de prescrire des normes de comportement. Il existe cependant une diversité des modes de production et d'application des normes selon quatre normes : l'objet, l'auteur, le sujet et la sanction de la norme.

On notera également que la dimension internationale de l'Internet conduit à une certaine concurrence entre divers ordres réglementaires nationaux. Lorsqu'un État veut réglementer, il est aisé pour les acteurs de déplacer leurs activités vers un autre État et de préférer trouver un cadre juridique moins contraignant. Cette forme de dumping réglementaire est une réalité[43].

#### *3.1.2.1 Les normes étatiques*

Les modes d'élaboration de la norme sont décrits dans des textes et des procédures qui entourent cette élaboration. L'application de la norme est confiée à des juridictions entourées de garanties d'indépendance et de fonctionnement contradictoire.

[43] Poullet Y (2000) Quelques considérations sur le droit du cyberespace *in* Les dimensions internationales du droit du cyberespace (2000), Economica, coll. Droit du cyberespace pp 185-235

Concernant les environnements électroniques on peut noter deux tendances du droit étatique. L'une qui consiste à préférer le recours à des notions à contenu vague, évolutif et susceptible de diverses interprétations. L'autre, qui est de confier l'interprétation des standards à des organes-relais appelés également autorités administratives indépendantes.

La dimension internationale des autoroutes de l'information conduit les États à rechercher, *via* des instances internationales des modes d'élaboration du droit ou de coopération d'autorités chargées de l'application des droits nationaux. Diverses initiatives sont prises pour maintenir le rôle de l'État dans la protection et la sauvegarde des droits des individus et des intérêts supérieurs de la société.

#### *3.1.2.2* ***Les normes privées***

##### 3.1.2.2.1 L'autoréglementation

L'interactivité des réseaux donne au consentement de l'internaute des potentialités d'application importantes. Qu'il s'agisse de révéler ou non son identité, d'accepter ou non des cookies…la technique offre à l'internaute la possibilité de prendre ses propres responsabilités. De ce fait, l'on peut admettre qu'à la responsabilité de l'État de réglementer les comportements, il est possible de substituer celle du citoyen qui, par son consentement ou ses consentements successifs, autorisera ou non telle ou telle opération.

L'autoréglementation, définit par Pierre Trudel comme « les normes volontairement développées et acceptées par ceux qui prennent part à une activité », peut se justifier au regard de trois éléments. D'une part, à l'argument du caractère technique et évolutif de l'objet, s'ajoute celui de la qualité des auteurs, seuls capables de percevoir les enjeux des solutions et d'autant plus enclins à respecter la règle qu'ils l'auront eux-mêmes formulée. D'autre part, l'autoréglementation garanti l'effectivité et l'adéquation des sanctions : par exemple le blocage immédiat d'un site pédopornographique après avoir été dénoncé. Enfin, la possibilité d'une élaboration

à l'échelon mondial apparaît un argument supplémentaire au moment où la dimension globale des questions posées par l'essor d'Internet est incontestée.

Au-delà de l'élaboration des normes, l'autoréglementation prétend aujourd'hui offrir des modes d'application de la norme dans des communautés virtuelles distinctes des communautés spatiales localisées dans des territoires donnés et soumis aux juridictions étatiques. Les premières expériences de « cyber magistrates », tribunaux virtuels chargés de régler les litiges apparus dans le monde virtuel et la création de conseils chargés d'appliquer les chartes de l'Internet constituent la démonstration de l'aptitude de l'autoréglementation non seulement à élaborer avec souplesse le droit de l'espace Internet mais également à le sanctionner.

#### 3.1.2.2.2 La certification

Dans un monde global où le réseau constitue la seule manière d'entrer en communication, la certification qui se définit comme une procédure par laquelle un tiers garanti la qualité spécifique d'une personne ou d'un produit, constitue une solution souhaitable.

La certification a pour finalité de garantir l'internaute non seulement sur l'existence, l'identité et l'adresse de l'interlocuteur voire sa qualité, mais au-delà assure la conformité des produits ou des services à des normes en termes de qualité et de sécurité.

La certification présente une solution qui peut être complémentaire soit à une source normative étatique, soit à l'autorégulation, dans la mesure où elle se référera à une loi ou un code de bonne conduite. Elle repose à la fois sur l'indépendance et l'expertise des autorités de certifications et des procédures de vérification, ainsi que sur la responsabilité effective de ces autorités en cas de délivrance indue d'un certificat.

#### 3.1.2.3 *La promotion de l'ordre juridique privé au regard de la directive 95/46 sur la protection des données personnelles*[44]

Le principe de la directive est simple : l'autorégulation comme la certification constituent en aval des principes de la directive des outils efficaces pour la mise en œuvre de tels principes. Ils contribuent à améliorer l'image de celui qui s'y soumet et accroissent la confiance de l'internaute. Leur souplesse et leur spécificité les rendent aptes à offrir des solutions évolutives adaptées aux particularités de chaque secteur. Enfin, leur caractère européen permet de garantir une équivalence de protection à propos des traitements opérés au sein de l'Union Européenne.

La reconnaissance par l'ordre étatique de ces codes de conduite s'opère de deux manières. D'une part, la procédure formelle d'homologation s'opère au regard de critères de fonds que constitue le respect des dispositions de la directive et de critères procéduraux. D'autre part, les codes de bonne conduite n'exemptent pas les secteurs concernés l'application des législations nationales qui garantissent l'effectivité des droits et devoirs reconnus aux personnes concernées.

À la lecture de l'article 25 de ladite directive il est précisé qu'une protection adéquate des données personnelles doit être garantie dans chaque État membre. Cette notion ne signifie pas une seule transposition des principes énoncés dans la directive mais la recherche d'une confrontation entre lesdits principes et les moyens existant dans l'État concerné. Ce faisant, une telle lecture permet un meilleur respect des structures et des caractéristiques juridiques nationales.

En particulier, à propos des instruments de protection mis en place dans le pays tiers, l'article 25 se réfère non seulement aux normes issues de l'autorité publique, mais également à la *soft law* constituée des codes de bonne conduite, voire des mesures techniques.

---

[44] Directive 95/46/CE du Parlement Européen et du Conseil du 24/10/1995 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

Pour conclure, la norme privée est d'autant mieux acceptée qu'elle est définie dans le cadre de principes ou de standards fixés par la norme étatique. De tels standards permettent en effet d'évaluer la conformité du contenu de la norme privée aux attentes sociétaires mais garantissent en retour à la norme privée une effectivité plus grande. Ensuite, la norme privée est perçue comme adéquate à une norme étatique dès lors que, la procédure de création garanti sa légitimité ; et si l'effectivité de la norme est réelle, c'est-à-dire si des sanctions efficaces et proportionnées sont énoncées par une autorité dotée de pouvoirs d'investigation, indépendante, et dont les règles de fonctionnement la rende transparente.

### 3.2 La cybercriminalité dans le cyberespace : la criminalité numérique comme nouvel outil des relations diplomatiques

Dans son rapport « **Dans la ligne de mire : les infrastructures sensibles à l'âge de la guerre numérique** » le Center for strategic and international studies révèle que :

- 54% des cadres interrogés déclarent avoir été confrontés à des attaques ou des infiltrations furtives par un adversaire de haut niveau (crime organisé, terroriste ou État) ;
- 59% est convaincue de l'implication de certains États étrangers dans ces infiltrations et attaques lancées contre les infrastructures critiques de leurs pays ;
- La Chine enregistre le plus fort taux d'adoption de mesures de sécurité (+62%) suivie par les USA, la Grande-Bretagne et l'Australie, dont les taux varient entre 50 et 53%, l'Italie, l'Espagne, et l'Inde présentent des taux d'adoption faibles avec des valeurs toutes inférieures à 40%.

Les USA sont considérés comme un modèle en matière de lutte contre les cyberattaques pour 44% des sondés, mais ils sont aussi considérés comme l'un des 3 pays les plus vulnérables aux cyber-attaques sur les infrastructures critiques dans leur secteur, suivis par la Chine et la Russie.

Les pays considérés comme des agresseurs potentiels varient en fonction des secteurs d'activité : dans le secteur de l'énergie le premier pays cité est la Russie, les

USA et la Chine sont au coude à coude dans les télécommunications, le secteur minier considère la Chine comme une plus grande menace, et le domaine de la Défense craint l'Europe et les États-Unis.

Quotidiennement, des milliers d'attaques de différents types ont lieu sur Internet. Ainsi, en moyenne, les ordinateurs des départements gouvernementaux britanniques reçoivent plus de 20 000 courriels malveillants et font l'objet de 10 000 cyber-attaques chaque mois. Parallèlement, des pays souvent cités comme sources d'attaques sont également parmi les plus touchés : c'est le cas notamment, de la Chine qui a relevé en 2010 une augmentation de 68% des attaques contre ces sites gouvernementaux, avec 4 600 sites gouvernementaux infiltrés par les hackers. C'est également le cas de la Russie, considérée comme l'une des patries du cybercrime, qui enregistrait plus de 15 000 cyber-crimes en 2009 contre 3000 en 2001[45].

**Attaques de type DOS (attaque par déni de service)**

| Rang | Pays | Nombre d'attaques | Part du total (en %) |
|---|---|---|---|
| **1** | Chine | 138 | 15,9 |
| **2** | Royaume-Uni | 33 | 3,8 |
| **3** | Espagne | 21 | 2,4 |
| **4** | Allemagne | 20 | 2,4 |
| **5** | Australie | 12 | 1,4 |
| | Autres | 642 | 74,1 |

Source : ATLAS, le 14/03/2011

**Cibles des attaques**

| Rang | Pays | Nombre d'attaques | Part du total (en %) |
|---|---|---|---|
| **1** | États-Unis | 143 | 20,5 |

[45] Bautzmann, A « Géopolitique de la cybercriminalité » Géopolitique de l'information, Les grands dossiers n°2, Diplomatie Avril-Mai 2011

| | | | |
|---|---|---|---|
| **2** | Brésil | 87 | 12,4 |
| **3** | Philippines | 64 | 9,2 |
| **4** | Chine (+ Hong Kong) | 52 | 7,4 |
| **5** | Malaisie | 37 | 6,3 |
| | Autres | 309 | 44,2 |

Source : ATLAS, le **14/03/2011**

### 3.3 La régulation d'Internet : un enjeu de domination dans les relations internationales

En France, le Livre blanc sur la défense et la sécurité nationale de 2008 a défini l'Internet comme une infrastructure vitale[46]. Un secteur d'activité d'importance vitale est défini comme composé d'installations ou d'ouvrages dont « le dommage ou l'indisponibilité ou la destruction à la suite d'un acte de malveillance, de sabotage, ou de terrorisme risquerait, directement ou indirectement : d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation »[47]. Ce faisant, la protection des systèmes de traitement automatisé de données (STAD) constitue l'axe de réflexion de l'élaboration d'une stratégie de défense numérique. Les cyber attaques ont été reconnues comme une des plus importantes menaces pesant sur le pays avec une probabilité d'occurrence et un impact potentiellement forts. Afin de faire face à ces nouveaux enjeux, la France devra se doter d'une nouvelle capacité défensive et offensive dans le cyberespace : l'informatique de combat sera un facteur de puissance et contribuera à la résolution du conflit, à ce sujet une réforme de l'Agence Nationale de Sécurité des Systèmes Informatiques est envisagée[48]. Ce projet s'articule autour de plusieurs axes complémentaires :

[46] Livre blanc sur la défense et la sécurité nationale, chapitre 11, « Protéger les systèmes d'information »
[47] Décret n°2006-212 du 23 février 2006
[48] http://www.zdnet.fr/actualites/france-une-brigade-speciale-et-un-intranet-ministeriel-pour-resister-aux-cyber-attaques-39761211.htm

D'une part, la création d'un « groupe d'intervention rapide intégré à l'ANSSI, formé d'experts capables d'intervenir sur les systèmes d'information de l'État et des opérateurs qui en feraient la demande, qui permettra de traiter dans les meilleurs délais les attaques les plus graves. L'ANSSI préconise également d'augmenter le nombre d'agents affectés à la protection du réseau informatique ministériel.

D'autre part, constatant l'indépendance des réseaux de chacun des ministères français et pour éviter toute coupure Internet, la deuxième solution, d'après l'ANSSI, serait de construire un intranet sécurisé et « homogène » afin d'accroître la sécurité du réseau informatique ministériel.

Enfin, le Premier ministre souhaite sensibiliser aux enjeux de la cybercriminalité par, dans un premier temps, la création d'une fondation. Cette entité prendre la forme d'un partenariat public-privé, et aura pour but de soutenir les capacités de recherche nationales et de développer un centre spécifiquement dédié à la recherche en sécurité des systèmes d'information, dans les domaines techniques et non techniques (politique, géostratégique, économique, etc.).

Puis dans un second temps, en renforçant la formation en matière de lutte contre la criminalité informatique au sein des spécialités informatiques et des écoles d'ingénieurs. Le Premier ministre souhaite également sensibiliser aux enjeux de la cybersécurité par l'introduction de formations spécifiques dans l'enseignement supérieur.

Début mai les États-Unis ont clairement affirmé leur intention de se positionner comme leader dans la mise en place d'une stratégie de coopération internationale renforcée dans le domaine de la lutte contre la cybercriminalité. En effet, Hillary Clinton, Éric Holder, 82ème procureur général des États-Unis et Howard Smichdt, Coordinateur Cyber-Sécurité de l'administration Obama, ont tout trois présenté un document intitulé « **International strategy of cyber-espace: Prosperty, Security and Opennes, in a Networked World**» qui présente les priorités en matière de sécurisation d'Internet et de lutte contre la cybercriminalité[49].

[49]http://www.leveilleur.fr/?p=423

En substance, le rapport précise que, les États-Unis souhaitent construire un environnement international qui assure que les réseaux soient ouverts à de nouvelles innovations, interopérables dans le monde entier, garantissent la sécurité des supports de travail, et suffisamment fiables pour gagner la confiance des internautes. Pour y parvenir, le président Obama souhaite bâtir et maintenir un environnement dans lequel des normes de comportement guideront les actions des États, permettront d'entretenir des partenariats, et de garantir la primauté du droit.
Le rapport conclue qu'avec nos « *partenaires du monde entier, nous allons travailler pour créer un avenir pour le cyberespace qui assure la prospérité, améliore la sécurité, et garantit l'ouverture dans notre monde en réseau. C'est l'avenir que nous recherchons, et nous invitons toutes les nations et les peuples, à nous rejoindre dans cet effort*».
Ce projet est d'autant plus pertinent que de nombreuses cyber-attaques ciblées, souvent fondées sur des procédés de *social engineering*, ont été recensées ces derniers temps et notamment à l'encontre des intérêts américains. Pour les contrer, les États-Unis s'efforcent depuis quelques mois de construire une coopération internationale entre acteurs publics et privés.

En effet, le bureau des services secret américain a ouvert un bureau de lutte contre la cybercriminalité en Estonie, un pays qui a été victime de nombreuses attaques informatiques au cours des dernières années. Les quatre employés qui travailleront au bureau estonien n'auront aucun pouvoir judiciaire. Ils offriront des séances de formation afin d'aider les forces de l'ordre de l'Estonie, de la Lettonie et de la Lituanie à combattre non seulement les crimes informatiques, mais également d'autres infractions comme le blanchiment d'argent ou l'usurpation d'identité.

Dans un contexte, où de nombreux acteurs testent leurs cyber-capacités d'influence notamment, Israël et la Corée du Nord les États-Unis semblent vouloir s'imposer comme défenseur et leader d'un Internet libre, ouvert et sécurisé quitte à employer la force armée. En effet, dans le rapport susmentionné Le président des États-Unis prévoient le recours à la légitime défense en cas d'attaques informatiques sur des infrastructures vitales pour l'économie[50] : « *Lorsque c'est justifié, les États-Unis*

[50] http://pro.01net.com/editorial/533805/les-experts-critiquent-le-projet-de-cyber-riposte-du-pentagone/

*répondront aux actes hostiles dans le cyberespace comme nous le ferions pour n'importe quelle autre menace sur notre pays. Tous les États possèdent un droit inhérent à la légitime défense, et nous reconnaissons que certains actes hostiles menés via le cyberespace pourraient contraindre à des actions au titre des engagements que nous avons avec nos partenaires des traités militaires. Nous nous réservons le droit d'utiliser tous les moyens nécessaires, diplomatiques, informationnels, militaires et économiques, le cas échéant et conformément au droit international applicable, afin de défendre notre nation, nos alliés, nos partenaires et nos intérêts* »

La position américaine qui consiste à assimiler les attaques informatiques comme des actes de guerre est critiquée car de telles attaques soulignent deux sortes de difficultés. D'une part, celle de la preuve de l'attaque, l'attaque par le virus Stuxnet est imputée à de nombreux États dont Israël et les États-Unis sans preuves.

Pour sa part, la Corée du nord crée actuellement des équipes de hackers formés par l'Université de Mirim dans lequel le Collège Amrokgang du génie militaire, l'Université de la Défense Nationale, l'Académie de la Force aérienne et l'Académie de Marine formeraient leurs spécialistes en guerre électronique[51]. Aujourd'hui la Corée du Nord dispose de 30 000 spécialistes de guerre électronique et de 1 200 personnes répartis dans deux brigades de guerre électronique. L'efficacité d'une telle organisation militaire est réelle : dans un rapport de 2006, l'armée sud-coréenne s'est alarmée du fait que les pirates nord coréens pourraient paralyser le poste de commandement des États-Unis du Pacifique. Les experts américains estiment que les pirates Nord coréens sont aussi bons que leurs homologues de la CIA.

Israël a créé une unité spécialisée dans la cryptographie (Unité 8200) chargée de déchiffrer les messages secrets iraniens concernant leur programme nucléaire[52].

Enfin, la Chine serait passée devant les États-Unis dans la course à l'espionnage informatique. Dernièrement des données sur les systèmes d'armements américains auraient été piratées : Pékin aurait dernièrement dérobé plusieurs téraoctets de

[51] http://english.chosun.com/site/data/html_dir/2011/03/08/2011030800611.html
[52] http://www.strategypage.com/htmw/htiw/articles/20110518.aspx

données sensibles. Les informations contiendraient les noms d'utilisateurs et les mots de passe donnant accès à des schémas de systèmes d'armements américains. Les pirates chinois auraient donc entre les mains des brevets estimés à plusieurs milliards de dollars. En avril 2009, Wikileaks avait d'ailleurs mis en évidence l'existence d'une « cyber armée populaire de libération » composée de pirates à la solde du régime chinois. Pour autant, le lien entre le gouvernement de Pékin et ces attaques reste à déterminer.

Par voie de conséquence, le cyberespace constituera à terme le nouveau champ de bataille sur lequel s'affronteront non plus des soldats mais des ordinateurs et dont l'objectif n'est pas de détruire militairement l'adversaire mais de le déstabiliser en fragilisant son économie, l'accès à ses ressources

### 3.4 Le cyberespace : un nouvel espace d'affrontement des puissances

Le cyberespace a été intégré par certaines puissances dans le champ des affrontements globaux. La cyber-guerre risque de déborder de son champ purement informatique et immatériel pour rejoindre celui de l'affrontement armé[53].

La guerre informationnelle est donc un nouveau domaine de la guerre classique, opérant dans un milieu spécifique (le cyberespace) et poursuivant des buts qui lui sont propres, immatériels pour la plupart mais dont les effets sont mesurables (vol de données, blocage de systèmes électroniques,…). L'accumulation de ces effets, couplée à la capacité de déterminer avec certitude l'auteur de l'attaque, pourrait alors servir de déclencheur à des opérations armées.

Les grandes puissances, conscientes de leurs vulnérabilités, ont progressivement organisé leur système de défense afin de protéger les réseaux et infrastructures jugés vitaux. La création du Cyber command aux USA puis sa certification opérationnelle à la fin du mois de novembre 2010, illustre ce mouvement. Les récents développements dans le domaine de la guerre informationelle viennent confronter la thèse des colonels chinois Qiao Liang et Wang Xiang dans La guerre hors limites qui prophétisaient l'avènement d'une révolution dans les affaires

[53] Boyer, B «La cyberguerre ou le mythe du blitzkrieg numérique », Géopolitique de l'information, Les grands dossiers n°2, Diplomatie Avril-Mai 2011

militaires, conséquence de l'apparition d'une arme révolutionnaire. Le principe étant qu'un « clic de souris » peut suffire à paralyser les systèmes de commandement adverses. Cette guerre éclair mettrait l'adversaire dans l'impossibilité de réagir de façon cohérente.

Cependant, ce concept semble peu réaliste car il ne prend pas en compte la globalité de l'affrontement. En effet, en l'état, la forme classique d'attaque demeure le virus, or certains analystes considèrent que son emploi à grande échelle est peu probable par crainte d'un « effet boomerang » sur nos propres systèmes de sécurité ou ceux de nos alliés. En effet, une fois diffusé, un virus peut muter, se répandre et engendrer des réponses non prévisibles sur des systèmes qui n'étaient pas initialement visés.
Pour l'heure, la majorité des attaques se borne à des dénis de service (distributed denial of service attack, ou DDoS attack) orchestrées depuis des machines zombies en réseau (botnet[54]).

Pour conclure cette étude dédiée à la présentation et l'analyse du cadre institutionnel et de normatif de lutte contre la cybercriminalité dans le cyberespace, il faut souligner qu'Internet est aujourd'hui le vecteur de diffusion d'une nouvelle forme de criminalité et un outil de définition des relations internationales. L'objectif poursuivi par les grandes puissances est de maîtriser les flux d'informations qui transitent à travers les réseaux pour déstabiliser l'adversaire en attaquant ses infrastructures vitales. La lutte pour le contrôle du cyberespace s'accroît en même temps que notre dépendance à l'information et aux réseaux qui la véhiculent. L'arme virale, sans devenir « l'ultima ratio », trouverait donc sa place au sein d'opérations militaires du futur. De fait, sans être une nouvelle forme de guerre, elle est un domaine nouveau.

Par conséquent, les cyber capacités militaires doivent se comprendre dans un environnement beaucoup plus large que le seul cyberespace en apportant de nouvelles perspectives aux capacités traditionnelles des armées. Les capacités informatiques ne sont pas une simple extension de capacités existantes pour les

[54] Une attaque par déni de service a pour but de rendre indisponible un service ou empêcher son utilisation par l'inondation d'un réseau, la perturbation des connexions entre machines ou l'obstruction d'accès ciblée. Une machine zombie est un ordinateur contrôlé à distance par un pirate à l'insu de son propriétaire afin d'attaquer d'autres machines en dissimulant son identité.

communications et l'aide à la décision, il s'agit de nouvelles capacités défensives/offensives évoluant dans un nouvel espace d'affrontement profondément imbriqué dans la population mondiale, les économies et le fonctionnement des organisations étatiques ou privées. L'informatique peut modifier ou influer sensiblement l'action sur le terrain par des effets de surprise stratégique ou tactique, la désinformation et la déstabilisation des populations comme des forces déployées.

**Bibliographie**


Arpagian N (2010) *La cybersécurité*, Paris, PUF, coll. Que sais-je ?, 126 p.

Benhamou F, Farchy J (2007) *Droit d'auteur et copyright*, Paris, La Découverte, coll. Repères, 123 p.

Balsano A. (2000) *Un instrument juridique international pour le cyberespace ? Une analyse comparative avec le droit de l'espace in Les dimensions internationales du droit du cyberespace* (2000), Economica, coll. Droit du cyberespace pp. 159-185

Bautzmann, A « *Géopolitique de la cybercriminalité* » Géopolitique de l'information, Les grands dossiers n°2, Diplomatie Avril-Mai 2011

Belloir, P., *LOPPSI : un projet de captation des données informatiques*, RLDI, 2009 n°50

Belloir, P., *Perquisition et saisie en matière de lutte contre la cybercriminalité*, RLDI, 2010 n°60

Bitan H. « *Réflexions sur la loi « Création et Internet » et sur le projet de loi « HADOPI 2* » RLDI 2009, n°51

Bologna G.-J *An Organizationnal Perspective on Enhancing Computer Security*, *in* Martin D (1997). *La criminalité informatique*, Paris, PUF, p. 68

Boubekeur I « *De la « loi HADOPI » à la « loi HADOPI 2* », RLDI 2009, n°59

Boyer, B « *La cyberguerre ou le mythe du blitzkrieg numérique* », Géopolitique de l'information, Les grands dossiers n°2, Diplomatie Avril-Mai 2011

Breton D. (2004) *L'interactionnisme symbolique*, Paris, PUF, coll. Manuel, 241 p.

Chawki M., *Essai sur la notion de cybercriminalité*, IEHEI, juillet 2006

Chopin, F., *Les politiques publiques de lutte contre la cybercriminalité*, AJ Pénal, 2009

Deffains B, Langlais E (2009) *Analyse économique du droit*. *Principes, méthodes, résultats*, Paris, De Boeck, 407 p.

Desgens-Pasanau G., *Protection des mineurs sur Internet*, LPA 1er août 2001 p. 10

Finet N., « *Dernières évolutions de la responsabilité des acteurs des services de communications électroniques en matière pénale* », RLDI 2005 n°130

Lepage, Agathe, *LCEN. Cybercriminalité. Libertés sur internet*, CCE, Septembre 2004, Études 24

Mattelard, A. (2009) *Histoire de la société de l'information*, La Découverte, coll. Repères, 127 p.

Mannoni P (2010) *Les représentations sociales*, PUF Que sais-je ?, 126 p.

Maupeou S*., Cybercriminalité, cyberconflits*, Revue Défense nationale et sécurité collective, Mars 2009

De Maupeou S., *World War Web 3.0 : l'informatique dans les conflits*, Revue Défense Nationale, Mars 2010

Moscovici (1961) *La psychanalyse, son image et son public*, Paris, PUF, coll. Bibliothèque de psychanalyse, 501 p.

Poullet Y (2000*) Quelques considérations sur le droit du cyberespace in Les dimensions internationales du droit du cyberespace* (2000), Economica, coll. Droit du cyberespace pp 185-235

Quéméner, M , Ferry, J., *La guerre du cyberespace aura bien lieu*, Revue Défense nationale et sécurité collective, Mars 2009

Reynaud P, Verbiest T « *Adoption de la loi DADVSI et décision du Conseil constitutionnel : point de répit estival !* » RLDI 2006, n°19

Rochelandet F. (2010) *Économie des données personnelles et de la vie privée*, Paris, La découverte, coll. Repères, 125 p.
Rosé P *La criminalité informatique*, Paris, PUF, coll. QSJ ?, 125 p.
Roussel P., *L'influence de l'informatique sur l'administration de la preuve pénale*, CCE 2005, Études 43
Schuhl C., *La collecte des preuves numériques en matière pénal*, AJ Pénal, 2009
Schull C. (2011) *Cyberdroit. Le droit à l'épreuve de l'internet*, 6ème édition, Paris, Dalloz
Simon C. « *Les adresses IP sont des données personnelles selon le Conseil constitutionnel* », RLDI 2009, n°51
Tissier, G., *Lutte informatique et droit international*, Défense nationale et sécurité collective, Mars 2009
Tribe L (1991) *The Constitution in Cyberspace : Law and Liberty beyond the Electronic Frontier*, Harvard University Press, Cambridge
Vincent S. *Cyberespace : pour une stratégie globale*, Revue Défense nationale, juin 2011

**SITOGRAPHIE**

www.legalis.net

www.01net.com

www.spyworld-actu.com

www.zdnet.fr

www.undernews.fr

www.net-iris.com

www.securite-informatique.gouv.fr