Association Internationale de Droit Pénal
Colloque préparatoire au XIX Congrès de Rio de Janeiro (Société de l'information et droit pénal,2014)
Section 1 « concept de cybercriminalité », Vérone (Italie), novembre 2012 *

Rapport pour la France par Frédérique CHOPIN, Maître de Conférences habilitée à diriger les recherches, Secrétaire générale de l'Association Française de Droit Pénal
Aix-Marseille Université, CDS EA 901, 13100, Aix-en-Provence, France

A. champ d'application du concept de « cybercriminalité » en France

Le terme « cybercriminalité » n'est pas utilisée dans les codes français, il est fait référence à l'utilisation d'un « réseau de communications électroniques » ou d'un « réseau de communication au public en ligne ».
Les infractions servant de base à la réression de la cybercriminalité en France ont toutes pour point commun l'utilisation des systèmes et réseaux informatiques tantôt en tant qu'objets de l'infraction (ex atteintes aux systèmes de traitement des données, infractions en matière de fichiers ou de traitement informatique), tantôt encore, en tant que supports de l'infraction (ex pédopornographie, infractions de presse, atteintes aux personnes et à la personnalité) , tantôt enfin, en tant que moyens de l'infraction (ex fraudes et autres infractions contre les biens commises par internet, contrefaçon, téléchargement illégal, paris et jeux en ligne).
Ces infractions de cybercriminalité relèvent pour certaines du droit pénal de droit commun (ex vol, escroquerie) alors que d'autres ont fait l'objet de dispositions spécifiques (ex téléchargement illégal, usurpation d'identité). La plupart de ces infractions sont incriminées dans le code pénal, mais certaines sont prévues intégralement ou pour partie par d'autres codes tels que le code de la propriété intellectuelle (ex contrefaçon), le code des postes et des communications électroniques (ex : conservation des données à caractère personnel), la loi du 29 juillet 1881sur la liberté de la presse (ex diffamation) ou encore le code monétaire et financier (ex paris et jeux en ligne).

B.Criminalisation

1. Quels sont les intérêts juridiques spécifiques nécessitant une protection offerte par le droit pénal (ex l'intégrité des systèmes de traitement des données, la confidentialité des données stockées) ?

Il s'agit d'abord, d'assurer la protection des systèmes de traitement des données notamment « la confidentialité (…), l'intégrité [et] la disponibilité des données »[1] (cf lois relatives à une violation des systèmes d'information personnels). C'est donc un moyen de protéger la liberté d'expression et de communication .
Il s'agit ensuite, de sécuriser les échanges qui se développent sur le réseau internet, notamment en matière de fraude aux moyens de paiement (fraude à la carte bancaire, phishing).
Les infractions liées aux identités virtuelles ou numériques ont elles pour objet de protéger la personne contre les troubles à sa tranquillité ou à celle d'autrui et contre les atteintes à son honneur ou à sa considération.

2. Exemples typiques de lois pénales

[1] M.Chawki, *Combattre la cybercriminalité*, Ed.de Saint Amans, 2008, p.40.

* Attention: Le texte publié constitue la dernière version originale du rapport national envoyé par l'auteur, sans révision éditoriale de la part de la Revue.

**Lois pénales relatives aux attaques contre les systèmes d'information*

La loi Godfrain du 5 janvier 1988[2] est venue réprimer dans les articles 323-1 à 323-7cp les atteintes à un système de traitement automatisé de données (ex ordinateur, smartphone, disque dur, système de carte bleue).
Ainsi, le code pénal vise les diverses attaques qui peuvent être menées contre les systèmes de traitement automatisé de données.
L'article 323-1 du code pénal vise l'intrusion ou le maintien dans un système de traitement automatisé de données. Il le rend passible de 2 ans d'emprisonnement et de 30.000 euros d'amende. Lorsque ces infractions « ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende » en application de la loi du 27 mars 2012 relative à la protection de l'identité[3].
L'article 323-2 cp quant à lui vise le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données qui est passible de cinq ans d'emprisonnement et de 75000 euros d'amende.
L'article 323-3 cp vise l'introduction frauduleuse de données ou leur suppression ou modification, dans un système de traitement automatisé de données. Elle est passible de 5 ans d'emprisonnement et de 75 000 euros d'amende.
Lorsque ces infractions (art 323-2 et 323-3cp) ont été commises « à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende », en application de la loi du 27 mars 2012.
L'article 323-3-1 cp vise quant à lui les moyens qui permettent ces attaques et punit des mêmes peines l'importation, la détention, l'offre, la cession et la mise à disposition de ces moyens techniques, matériels ou logiciels.
Enfin, la tentative de commission de tous ce délits est punie des mêmes peines (article 323-7 du code pénal).

**Lois pénales relative à une violation des systèmes d'information personnels :*

Le droit pénal français a, depuis 1978[4], mis en place un dispositif de contrôle d'une part, sur le contenu des données traitées (ex : interdiction de collecter des données personnelles pouvant servir de base à une discrimination et sans lien avec l'objet du fichier) et d'autre part, sur le mode de traitement de ces informations, notamment en limitant les interconnexions entre fichiers. La loi « informatique et libertés » de 1978 a conduit à la mise en place de la Commission Nationale Informatique et Libertés (CNIL), autorité administrative indépendante, « chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Dans le cadre de cette loi, les dispositions pénales (art 226-16 à 226-24cp) sont destinées à sanctionner le non respect -y compris par négligence - des formalités exigées pour la collecte et le traitement de données personnelles.
Mais, la loi de 1978 n'envisageait pas les atteintes susceptibles d'être portées à l'outil informatique[5]. C'est la raison pour laquelle, en 1988, a été adoptée une loi nouvelle destinée à lutter contre les atteintes aux systèmes informatiques (art 323-1 à 323-7cp) complétée par la loi du 21 juin 2004 pour la confiance dans l'économie numérique[6]. Ces dispositions pénales

[2] Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique, J.O 6/1/1988, p.231.
[3] Loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité, JO 28/3/2012, p.5604.
[4] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO 7/1/1978, p.227.
[5] V.en ce sens, M.Quémener et J.Ferry, *Cybercriminalité, Défi mondial et réponses*, Economica, 2007, p.65.
[6] Loi n°2004-575 pour la confiance dans l'économie numérique, JO 22/6/2004, p.11168.

ont pour objectif de protéger « la confidentialité (…), l'intégrité [et] la disponibilité des données »[7].
Dans le même temps, afin de tenir compte de l'apparition du réseau internet en tant que nouveau moyen pouvant porter atteinte aux personnes, la loi du 21 juin 2004 met en place un cadre juridique adapté au réseau internet, afin de lutter plus efficacement contre la cybercriminalité en sécurisant les échanges. Ces dispositions ont fait l'objet de modifications ultérieures par la loi du 6 août 2004[8] qui a notamment introduit le terme de « traitement de données à caractère personnel », contrairement à la loi de 1978, qui d'une part, faisait référence à un traitement « automatisé » et d'autre part, visait « des informations nominatives ».
L'ordonnance n° 2011-1012 du 24 août 2011[9] vient transposer en droit français les dispositions issues des directives européennes du Paquet Télécom à savoir la directive 2009/136/CE (PE et Cons. UE, dir. 2009/136/CE, 25 nov. 2009, modifiant la directive « vie privée et communications électroniques » 2002/58/CE, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur de communications électroniques : JOUE n° L 337, 18 déc. 2009, p. 11) et la directive 2009/140/CE (PE et Cons. UE, dir. 2009/140/CE, 25 nov. 2009, modifiant la directive « cadre » 2002/21/CE, relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques : JOUE n° L 337, 18 déc. 2009, p. 37). Il s'agit de renforcer les obligations à la charge des fournisseurs de services de communications électroniques afin de pouvoir répondre plus efficacement aux atteintes graves à la sécurité des systèmes d'information. En l'occurrence, l'ordonnance vient rendre obligatoire la notification des violations de données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public.

**Loi relative à la falsification et à la manipulation des données stockées numériquement*

La loi du 16 novembre 2001 sur la sécurité intérieure insère les articles L.163-4-1 et L.163-4-2 (modifiés par l'ordonnance n°2009-866 du 15 juillet 2009) au Code monétaire et financier, afin de réprimer pénalement désormais dans l'article L.163-4 « le fait de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour contrefaire des cartes ». Ces dispositions permettent d'incriminer de façon spécifique la contrefaçon et la falsification de cartes de paiement.

De même, l'article 323-3 du code pénal vise l'introduction frauduleuse de données ou leur suppression ou modification, dans un système de traitement automatisé de données. Elle est passible de 5 ans d'emprisonnement et de 75 000 euros d'amende. Quant à l'article 323-3-1 cp il vise quant à lui les moyens qui permettent ces attaques et punit des mêmes peines l'importation, la détention, l'offre, la cession et la mise à disposition de ces moyens techniques, matériels ou logiciels.

**Loi relative à la diffusion de virus informatiques*

Ce sont les dispositions de l'article 323-3-1du code pénal qui répriment « le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement,

[7] M.Chawki, préc.
[8] Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, JO du 7/8/2004, p.014063.
[9] Ordonnance prise sur le fondement de l'article 17 de la loi du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques. Ce texte autorise le Gouvernement à prendre par voie d'ordonnance les dispositions de nature législative nécessaires à la transposition des directives visées par la loi.

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 323-3cp ». ainsi, est sanctionné non seulement le fait de faire entrer le virus dans le système d'information mais aussi le fait de détenir un virus. Cette infraction permet de sanctionner l'offre, la cession, la détention ou la mise à disposition de virus informatiques, sans qu'il soit besoin que le virus ait été introduit frauduleusement dans un système de traitement automatisé de données.

**Loi relative aux infractions liées aux identités virtuelles des utilisateurs (usurpation d'identité, vol de personnalités virtuelles, dommages aux identités virtuelles des utilisateurs*) :

La loi du 14 mars 2011[10] crée notamment un nouvel article 226-4-1cp sanctionnant d'un an d'emprisonnement et de 15.000€ d'amende « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou de 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 ». Cette disposition qui renvoie à « une ou plusieurs données de toute nature permettant de l'identifier » plus large que celle de « données personnelles » devrait permettre d'inclure l'adresse IP, une adresse courriel, un pseudonyme, une image, un numéro de téléphone….
Le second alinéa étend le champ d'application de l'infraction au cas où « elle est commise sur un réseau de communication au public en ligne », ce qui renvoie non seulement à la téléphonie mais surtout à internet. Sont ainsi visés l'usurpation d'adresse IP, d'identité sur un réseau social ou encore d'une adresse. Ce texte peut donc s'appliquer aux utilisations frauduleuses telles que le phishing, téléchargement illégal en utilisant l'adresse de connexion d'un tiers, etc..

**Loi relative à d'autres interdictions pénales dans le domaine des TIC et d'internet (ex criminalisation de la création et de la possession de certaines images virtuelles, violation du droit d'auteur dans la sphère virtuelle)*

L'article 227-23 du code pénal punit de cinq ans d'emprisonnement et 75.000€ d'amende deux comportements distincts : d'une part, le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique. Le code pénal distingue image et représentation du mineur sachant que la représentation vise les images et films de synthèse ou virtuelles telles que les bandes dessinées, les mangas et autres, lorsque ces représentations sont pornographiques[11]. D'autre part, est incriminé le fait d'offrir, de rendre disponible ou de diffuser une telle image, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter. Sont ici visés par exemple, les systèmes d'échange de fichiers sur des sites pédophiles.

La loi du 14 mars 2011 a ajouté à certaines infractions du code de la propriété intellectuelle une circonstance aggravante tenant à sa commission sur un réseau de communication au public en ligne. Ce sont les atteintes aux droits et modèles (art L.521-10), aux droits du titulaire d'un brevet (L.615-14), détention et commerce de marchandises contrefaites, contrefaçon de marques (L.716-9 et 716-10).

[10] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JO 15 mars 2011.
[11] V.F.Chopin, Rep.pénal Dalloz, « Cybercriminalité », n°93.

3. comment l'élément matériel est généralement défini dans ces crimes (par la description de l'acte, de ses conséquences etc ?) Comment est défini l'objet (données, écrits, contenu) ?

L'élément matériel des délits concernés est généralement défini par la description de l'acte. Ainsi, par exemple, l'accès ou le maintien frauduleux dans un système de traitement automatisé de données (art 323-1cp) est défini par les actes « accéder ou se maintenir, dans tout ou partie d'un système de traitement automatisé de données ». De même, en matière de pédopornographie (art 227-23cp), le code pénal punit « le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation » à caractère pornographique d'un mineur.
En matière de fraude à la carte bancaire, est puni « le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre les infractions prévues au 1° de l'article L. 163-3 ».

Quant à l'objet, lorsqu'il s'agit de données, il est fait référence aux données à caractère personnel, c'est à dire « 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne »[12]. De même, en matière d'usurpation d'identité, l'objet de l'infraction , ce sont les données de toute nature permettant d'identifier la personne.

4. Existe t-il une responsabilité pénale à l'égard de certaines cyber-infractions ne visant que certains groupes particuliers d'auteurs et/ou de victimes ?

Il n'existe pas de responsabilité pénale visant certains groupes particuliers d'auteurs ou de victimes mais plutôt une responsabilité pénale à l'égard de certaines cyber-infractions liées à la participation à un groupe ou à une entente formée en vue de commettre des fraudes informatiques. Tel est le cas par exemple, de l'article 323-4cp qui réprime la commission en bande organisée d'atteintes au système de traitement automatisé de données. Cette circonstance aggravante qu'est la bande organisée se retrouve également en matière d'infractions aux cartes (art L.163-4-2 code monétaire et financier) ou dans le cadre du code de la propriété intellectuelle (par exemple, art L.521-10).

5. La responsabilité pénale dans le domaine des TIC et internet s'étend elle aux actes commis par négligence ou imprudence ?

En principe, la responsabilité pénale dans le domaine des TIC et d'internet ne concerne que des infractions intentionnelles. Cependant, plusieurs infractions visent les comportement non intentionnels dans le domaine des Tic et internet.

-«Article 226-16 « *Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.*

[12] Loi n°2004-801, préc. article 2.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

-Article 226-16-1-A « *Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende*. »
Ces deux textes qui prévoient des peines très élevées, sont très peu appliqués.

-Article 226-3 cp incrimine dans son premier alinéa divers actes comme la fabrication, la détention, la location, la vente – et ce, en l'absence d'autorisation ministérielle (conditions d'octroi fixées par un décret en Conseil d'État) – d'appareils ou de dispositifs techniques conçus pour réaliser des opérations pouvant constituer des atteintes à la personnalité telles que l'atteinte au secret des correspondances électroniques (art. 226-15, al. 2cp) l'atteinte à l'intimité de la vie privée par enregistrement des conversations (art 226-1cp) ou de ceux qui ont « pour objet la captation de données informatiques prévue par l'article 706-102-1 du code de procédure pénale ». L'ordonnance du 24 août 2011 a pris comme modèle les articles 226-16 et 226-16-A cp et a ajouté à l'article 226-3 « lorsque ces faits sont commis, y compris par négligence »[13].

- Art R.335-5 du code de la propriété intellectuelle prévoit la contravention de négligence caractérisée qui sanctionne le défaut de sécurisation de l'accès à internet[14].

6. Y a t il des différences spécifiques entre la définition de la cyber-infraction et celle des infractions « traditionnelles » ?

La définition de la cyber-infraction comme celle des infractions traditionnelles repose toujours sur les trois éléments constitutifs de l'infraction que sont les éléments légaux, matériels et moraux.
Certaines infractions traditionnelles voient leur champ d'application étendu aux cas où la commission de l'infraction s'est réalisée « par l'utilisation d'un réseau de communications électroniques ». Tel est le cas par exemple, de la corruption de mineur (art 227-22cp), du délit de proposition sexuelle à un mineur (art 227-22-1cp).
Parfois, l'utilisation d'un réseau de communications électroniques est érigée en circonstance aggravante de l'infraction (ex pédopornographie art 227-23cp ; atteintes sexuelles sur mineurs art 227-26cp ; proxénétisme art 225-7,10°cp ; agressions sexuelles art 222-28,6°cp ; viol art 222-24, 8°cp). Tel est le cas également en matière d'atteintes à la propriété intellectuelle par l'usage d'internet (art L.521-10, L.615-14, L.623-32, L.716-9, L.716-10 code de la propriété intellectuelle).

Enfin, la cryptologie constitue une circonstance aggravante générale (art 132-79cp) dès lors qu'elle a été utilisée pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission.

La loi du 29 juillet 1881 sur la liberté de la presse s'applique aux infractions commises par la voie de la presse ou par tout autre mode de publication –internet- et sanctionne des infractions

[13] Article 226-3cp modifié par la loi du 14 mars 2011 puis par l'ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques.
[14] V.F.Chopin, « Téléchargement illégal et Hadopi »,AJ Pénal Mai 2012, p.258.

telles que les diffamations et injures publiques, les provocations ou encore les délits de contestation de crime contre l'humanité. Là encore, aucune différence n'est faite selon le support de l'infraction.

C. Technique législative

1.Y a t-il des problèmes spécifiques en ce qui concerne le principe de la légalité (flou, référence ouverte à la définition des crimes dans d'autres textes)

non

2.Comment la législation évite-t-elle des effets de craintes excessives par rapport à l'utilisation légitime des TIC ou d'internet ?

C'est essentiellement en matière bancaire qu'il existe des craintes importantes quant au risque de piratage (notamment phishing) des données bancaires. Les difficultés ont trait au paiement à distance par internet face aux attaques de serveurs commerçants, au piratage des données bancaires, à la défiguration de site, etc…Se sont multipliés les dispositifs d'authentification non rejouable auprès des porteurs de cartes de paiement. Dans le même temps, le régime de responsabilité financière de la fraude a été considérablement amélioré en faveur du consommateur. Ainsi, il résulte des articles L,133-18 et suivants du code monétaire et financier que la banque émettrice de la carte, doit rembourser immédiatement, sans aucune franchise, à son titulaire, tout paiement non autorisé, effectué grâce à une contrefaçon de la carte ou à une utilisation frauduleuse de ses données d'utilisation alors que la carte est restée en sa possession. De même, la banque doit rembourser à celui-ci la totalité des frais bancaires qu'il a supportés. Ces remboursements sont totalement indépendants du dépôt d'une plainte.

Quant aux données personnelles, la France a transposé les directives européennes dites « Paquet Télécom » par la publication de l'ordonnance du 24 août 2011. Cette ordonnance vient confier à la Commission Nationale Informatique et Libertés (CNIL) une nouvelle mission qui consiste à examiner les notifications des failles de sécurité des opérateurs de communications électroniques. Plus précisément, les fournisseurs de services de communications électroniques ont l'obligation de communiquer à la CNIL les failles de sécurité qui ont entrainé, de manière accidentelle ou illicite, une perte, une altération ou un accès non autorisé à des données à caractère personnel. De même, cette ordonnance consacre le principe européen de l'accord préalable de l'internaute à l'utilisation des cookies.

3. Comment la législation pénale évite t elle de devenir obsolète du fait de la rapidité des innovations technologique ?

Ex la façon dont les changements dans l'utilisation des réseaux internet et des réseaux sociaux sont pris en compte

Ex la façon dont la loi est adaptée au progrès technologique (ex par référence aux réglementations administratives).

La législation pénale a évolué à plusieurs reprises ces dernières années afin d'inclure la répression d'un certain nombre de comportements susceptibles d'être commis par l'utilisation d'internet. Elle a donc ajouté pour bon nombre d'infractions, la possibilité de les commettre « par l'utilisation d 'un réseau de communication au public » ou des formules similaires. De même, en matière d'infractions de presse, le support est indifférent (audio, papier, vidéo, internet).

En vue de s'adapter au progrès technologique, le 25 juin 2012 la CNIL a proposé sa définition du "Cloud Computing" : « le déport vers « le nuage Internet » de données et d'applications qui auparavant étaient situées sur les serveurs et ordinateurs des sociétés, des organisations ou des particuliers. Le modèle économique associé s'apparente à la location de ressources informatiques avec une facturation en fonction de la consommation »[15]. La loi française a du mal à s'appliquer ici en raison de la difficulté à déterminer les pays dans lesquels les données sont transférées par cloud computing. Pour l'instant, la CNIL fait des recommandations aux entreprises utilisatrices. Ce système rend plus difficile la localisation de l'infraction ou d'un élément constitutif de l'infraction et la mise en œuvre de la responsabilité pénale.

D. Mesures de la criminalisation

1. **Dans quelle mesure les lois pénales couvrent-elles de simples actes préparatoires qui comportent un risque de favoriser les abus tels que l'acquisition ou la possession d'un logiciel qui peut être utilisé pour le «piratage», le «phishing», la fraude informatique, ou pour contourner les protections contre le téléchargement illégal? Si oui, y a-t-il eu controverse au sujet de ces lois? Le législateur fait-il des efforts particuliers pour éviter la sur-criminalisation?**

Afin de lutter contre la copie numérique illicite, des dispositions du code de la propriété intellectuelle érigent en infractions par exemple, toute importation, fabrication ou activité de diffusion ou promotion en faveur de procédés technologiques conçus ou spécialement adaptés pour porter atteinte à une mesure technique de protection ou à un dispositif d'information sur le régime des droits d'auteur (art L.335-3-1 et L.335-3-2cPI).
De même, en matière de lutte contre le téléchargement illégal, l'article L.335-2-1cpi punit de trois ans d'emprisonnement et de 300.000 euros d'amende le fait « d'éditer, de mettre à 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'oeuvres ou d'objets protégés et d'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un tel logiciel ». Cependant, lorsqu'un logiciel est « principalement utilisé pour la mise à disposition illicite d'oeuvres ou d'objets protégés par un droit de propriété littéraire et artistique », le président du tribunal, statuant en référé, peut ordonner toute mesure nécessaire à la protection du droit menacé (art L.336-1cpi).
Les personnes coupables de ces infractions peuvent également être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne 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 L.335-7cpi).
En matière d'atteintes au système de traitement automatisé de données, l'article 323-3-1cp punit le fait « 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 les faits prévus par les articles 323-1 à 323-3cp ». Ce texte s'inspire dans ses éléments constitutifs de l'article L.163-4-1 du code monétaire et financier qui réprime la tentative de contrefaçon ou de falsification des moyens de paiement.

2. Dans quelle mesure la simple possession de certaines données a-t-elle été criminalisée? Dans quels domaines, et pour quels motifs? Comment est définie la «possession» de ces données? La définition inclut-elle la possession temporaire ou la simple visualisation?

[15] Y.Cohen-Hadria, Cloud computing et protection des données à caractère personnel, http://www.village-justice.com/articles/Cloud-Comuting-protection-donnees,12532.html

La simple possession de données n'est pas visée par le code pénal qui incrimine la détention de données. La possession se démarque de la "détention"qui est la situation dans laquelle se trouve une personne qui, en vertu d'un contrat, dispose d'un bien dont elle a seulement l'usage ou la garde pendant la seule durée du contrat (ex : le dépositaire, le mandataire ou le locataire). En droit pénal, la détention de données est incriminée notamment lorsque ces données sont des images à caractère pédopornographique (art 227-23al1cp). De même, l'article 226-19cp interdit de mettre ou de conserver en mémoire informatisée, sans l'accord de l'intéressé, des données nominatives.

3. Dans la mesure où la possession ou l'octroi de l'accès à certaines données ont été définis comme des infractions, la responsabilité pénale s'étend-elle aux prestataires de services ayant permis l'accès à ces données (par exemple, l'hébergement ou les fournisseurs d'accès)? Quelles sont les exigences pour engager leur responsabilité, en particulier, concernant l'intention? Les fournisseurs sont-ils tenus de surveiller et de contrôler les informations qu'ils fournissent ou auxquelles ils offrent accès? Les fournisseurs sont-ils tenus d'empêcher l'accès à certaines informations? Si oui, sous quelles conditions et doivent-ils en supporter le coût? Sont-ils responsables pénalement en cas de violation de ces obligations?

En droit français, les fournisseurs d'accès désignent ceux « dont l'activité est d'offrir un accès à des services de communication au public » (L.21 juin 2004, art 6.I.1). Ils se distinguent des hébergeurs qui sont « les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public, par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services » (L.21/6/2004, art 6.I.2).
La loi pour la confiance dans l'économie numérique a mis à la charge des fournisseurs d'accès et d'hébergement trois types d'obligations qui ont avant tout pour objectif de lutter contre certaines infractions commises sur l'internet. Ces trois obligations sont : une obligation de surveillance, la mise en place d'un dispositif de signalement et la mise en place d'un dispositif de filtrage.

-Une <u>obligation de surveillance</u> : la directive du 8 juin 2000 (art 15,1) et la loi du 21 juin 2004 (art 6.I.7) précisent tout de même qu'il n'existe pas, pour les fournisseurs d'accès et d'hébergement, d'obligation générale de surveillance « des informations qu'ils transmettent ou stockent », ni « d'obligation générale de rechercher des faits ou des circonstances révélant des activités illicites ». Cependant, cette absence d'obligation générale de surveillance ne fait pas obstacle à une activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire (art 6.I.7, §2, LCEN). De même, les fournisseurs d'accès et d'hébergement ont obligation de déférer aux décisions de justice destinées à faire cesser ou à prévenir un dommage. Ainsi, l'article 6.I.8 de la loi de 2004 énonce que *« l'autorité judiciaire peut prescrire en référé ou sur requête, aux fournisseurs d'hébergement ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir un dommage occasionné ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ». Enfin, la loi instaure également une obligation de surveillance limitée à la charge des fournisseurs d'accès et d'hébergement afin de les impliquer dans la lutte contre les infractions les plus graves pouvant être commises sur l'internet, à savoir l'apologie des crimes contre l'humanité, l'incitation à la haine raciale , la pornographie enfantine, l'incitation à la violence, les atteintes à la dignité humaine, les infractions de l'article 24 al5 et 8 (L.1881) et les infractions prévues aux articles 227-23 et 227-24 cp. Afin de permettre la mise en œuvre de cette surveillance limitée, la loi impose aux fournisseurs d'accès et d'hébergement de mettre en place un dispositif de signalement.

- Un dispositif de signalement : la loi impose aux fournisseurs d'accès et d'hébergement de *« mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données* ». Une charte des prestataires de services d'hébergement en ligne et d'accès à internet en matière de lutte contre certains contenus spécifiques dite « charte contre les contenus odieux » a été élaborée à l'initiative de l'association des fournisseurs d'accès (AFA) afin de mettre en œuvre les obligations posées par la loi. Il en découle que depuis 1997, l'AFA a créé un point de contact permettant à toute personne de signaler des contenus et activités illicites sur l'internet et expliquant toutes les procédures à suivre afin de signaler ces contenus aux autorités publiques compétentes (www.pointdecontact.net). Ils doivent également informer les autorités publiques (police, parquet) de l'existence de ces sites et rendre public les moyens qu'ils consacrent à la lutte contre ces activités illicites (art 6.I.7§4, LCEN). La loi exige donc des fournisseurs d'accès et d'hébergement qu'ils consacrent des moyens à la lutte contre ces sites, sachant que ces moyens ne peuvent consister en une obligation générale de surveillance du réseau ou en la recherche d'activités illicites, puisque ces dernières sont expressément exclues par l'article 6.I.7§1 de la loi de 2004. Les fournisseurs d'accès et d'hébergement doivent, lorsque le contenu est manifestement illicite au sens de l'article 6.I.7 (LCEN), procéder au retrait immédiat du contenu, sans attendre une décision de justice. Dans les autres cas, ils doivent simplement apprécier le caractère manifestement illicite des contenus (ex en matière de contrefaçon[16]), en se fondant sur les éléments avancés par les personnes qui se prétendent victimes.

- Un dispositif de filtrage : la loi pour la confiance dans l'économie numérique met à la charge des fournisseurs d'accès l'obligation d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et l'obligation de leur proposer au moins l'un de ces moyens. Cette obligation n'est pas assortie de sanctions pénales ou civiles et est aujourd'hui complétée par l'obligation des fournisseurs d'accès de mettre en place des dispositifs de contrôle parental.

La loi du 14 mars 2011 a complété ces obligation dans l'article 6.I-7 de la loi du 21/6/2004 en précisant « *lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du Code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai* ». La loi institue ici le blocage administratif des sites contenant des images de mineurs à caractère pornographique. Ce dispositif permet à l'autorité administrative, indépendamment de l'autorité judiciaire, de demander aux fournisseurs d'accès de bloquer l'accès des internautes aux sites notifiés par l'administration.

Quant aux sanctions, « *Est puni d'un an d'emprisonnement et de 75.000€ d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'activité de fournisseur d'hébergement ou d'accès, de ne pas satisfaire aux obligation définies à l'article 6.I.7, §4 et 5 de la LCEN* ». Les personnes morales peuvent être déclarées pénalement responsables de ces infractions et encourent une peine d'amende au quintuple de celle encourue par les personnes physiques éventuellement assorties des peines complémentaires de l'article 131-39, 2° et9°cp .

Outre ces trois obligations, les fournisseurs d'accès et de contenu sont tenus de conserver certaines données définies par la loi, qui peuvent leur être demandées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

[16] TGI Paris, 3ème ch., 15 avril 2008, affaire Dailymotion, D.2008.Act.p.1341

Les fournisseurs d'accès à internet bénéficient depuis la loi du 21 juin 2004 d'une irresponsabilité pénale de principe alors que les fournisseurs d'hébergement obéissent à un régime autonome de responsabilité.

Une irresponsabilité de principe des fournisseurs d'accès

En vertu de l'article L.32-3-3 du code des postes et communications électroniques « *Toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission* ». Ainsi, le fournisseur d'accès comme l'opérateur sont, en principe, exonérés de toute responsabilité civile et pénale.

Toutefois, la responsabilité du fournisseur d'accès est engagée d'abord, lorsqu'il ne respecte pas les obligations prévues par la loi (v.supra) telles que l'obligation de mettre à disposition un dispositif de filtrage. Ensuite, lorsque le fournisseur d'accès n'a pas « accompli les diligences normales » pour faire cesser un contenu illicite il peut être déclaré pénalement responsable. Il en est ainsi par exemple, lorsque l'autorité judiciaire prescrit en référé ou sur requête, au fournisseur d'hébergement, ou, à défaut, au fournisseur d'accès , « des mesures propres à interrompre l'accès, à partir du territoire français », au contenu d'un site illicite[17].». Se pose alors la question de la conciliation des dispositions relatives à la responsabilité des intermédiaires techniques et de celles relatives à la protection de la liberté d'expression au sens de l'article 10 Conv.EDH : peut on par exemple, au nom de la lutte contre le racisme et la xénophobie imposer au fournisseur d'accès ou d'hébergement d'empêcher l'accès à un contenu illicite ? Dans son arrêt rendu le 19 juin 2008[18], la cour de cassation confirme qu'en application de l'article 6.I.8 de la loi pour la confiance en l'économie numérique du 21 juin 2004 (LCEN), les fournisseurs d'accès à internet doivent être prêts à mettre en place des mesures de filtrage constitutives d'une obligation de moyen.
Enfin, le fournisseur d'accès est pénalement responsable lorsqu'il « *est à l'origine de la transmission litigieuse* », qu'il « *sélectionne le destinataire de la transmission* » ou qu'il « *sélectionne ou modifie les contenus faisant l'objet de la transmission* ».

Un régime autonome de responsabilité des fournisseurs d'hébergement

Depuis la loi du 21 juin 2004, l'article 6.I.3 précise que *« les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, de stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, ne peuvent pas voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient effectivement pas connaissance de l'activité ou de l'information illicite ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible* ». Ainsi, la loi de 2004 pose un principe d'irresponsabilité pénale de l'hébergeur quant au contenu. Toutefois, cette irresponsabilité s'efface lorsqu'il a connaissance de l'activité ou de l'information illicite et qu'il n'agit pas pour retirer ces informations ou en rendre l'accès impossible .

[17] Ca Paris, 24 novembre 2006, Légipresse, mars 2007, n°239, I, 29
[18] Cass.Civ 1, 19 juin 2008, pourvoi n°2007-70719.

Tout d'abord, la loi pose une présomption de connaissance des faits litigieux par l'hébergeur lorsqu'il reçoit notification de différents éléments énumérés par la loi (art 6.I.5, LCEN) à savoir, la date de la notification, l'identité du notifiant (personne physique ou morale), les noms (ou dénomination) et domicile (ou siège social) du destinataire, la description des faits litigieux et leur localisation précise, les motifs pour lesquels le contenu doit être retiré comprenant la mention des dispositions légales et des justifications de faits, la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté. Cette notification a un caractère facultatif et elle est en plus soumise à des appréciations variables par les juges du fond. Ainsi, le tribunal de grande instance de Paris [19]a écarté la responsabilité de l'hébergeur en relevant que la notification ne faisait « *nulle mention des dispositions légales essentielles pour la vérification par le destinataire du caractère manifestement illicite que doit revêtir le contenu en question* ». De même, dans une affaire mettant en cause Dailymotion[20] à propos de la diffusion d'œuvres arguées de contrefaçon, le juge rappelle *« qu'il ne suffit pas prétendre subir une contrefaçon d'œuvres dont on prétend détenir les droits, encore faut il préciser, en les nommant, les dénombrant et les identifiant, les œuvres dont on revendique la paternité pour justifier de sa qualité à agir et de son intérêt à agir* » . On constate toutefois une tendance à la déresponsabilisation des plateformes d'échanges vidéo, tendance qui avait déjà été annoncée par plusieurs décisions qui ont systématiquement écarté la qualité d'éditeur au profit de celle d'hébergeur . Au fil du temps, la définition de l'hébergeur donnée par la jurisprudence ne correspond pas à celle donnée dans la loi puisqu'est précisé que sont hébergeurs les personnes qui « *mettent à la disposition du public (...) » et non celles qui « pour mise à disposition du public (...)* ». La définition donnée par la jurisprudence conduit à faire des hébergeurs des personnes qui mettent à disposition du public (…) le stockage de données de toute nature, ce qui ne correspond plus du tout à la définition de la loi de 2004…

Ensuite, lorsque le fournisseur d'hébergement a eu connaissance de l'activité ou de l'information illicites, il commet une faute si d'une part, il persiste à la diffuser, et d'autre part, s'il n'agit pas promptement.

Quant à la faute en raison de la diffusion du contenu notifié comme illicite, le Conseil constitutionnel a précisé que les dispositions de l'article 6.I, 2 et 3 (LCEN) « ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge » (Conseil Constitutionnel, décision n°2004-496, DC 10 juin 2004, JO du 22 juin 2004, p.11182). Reste alors à déterminer les cas dans lesquels les contenus sont « manifestement illicites » des cas dans lesquels une notification doit être envoyée à l'hébergeur. En effet, le conseil constitutionnel n'a pas précisé ce qu'il entendait par « manifestement illicite ». Dans l'application faite de ces dispositions, les juridictions ont eu tendance à retenir comme manifestement illicites les contenus dits odieux visés à l'article 6.I,7 (LCEN) à savoir l'apologie des crimes contre l'humanité, l'incitation à la haine raciale, la pornographie enfantine, l'incitation à la violence, les infractions prévues à l'article24 al5 et 8 de la loi sur la presse et les infractions prévues par les articles 227-23 et 227-24cp mais, rien n'oblige le juge à se cantonner à ces contenus odieux. L'hébergeur n'est tenu responsable que pour autant qu'il a eu une connaissance effective du caractère manifestement illicite des contenus stockés. Cette connaissance effective découle de la notification qui lui est faite par un tiers. Ainsi, le juge est amené à apprécier au cas par cas le caractère manifestement illicite d'une activité ou d'un contenu et le comportement de l'hébergeur à son égard, afin de se prononcer sur l'éventuelle responsabilité de ce dernier. La notification n'est qu'un moyen pour dénoncer le caractère illicite d'un contenu et donc la connaissance de l'hébergeur, autrement dit, l'hébergeur se doit d'agir dès lors qu'il en a

[19] TGI Paris, réf.29 octobre 2007, Wikimédia Foundation, JurisData n°2007-344652
[20] TGI Paris, 18 décembre 2007, J.Y Lafesse et autres c/Dailymotion, www.legalis.net

connaissance, même en l'absence d'une quelconque notification. La cour de cassation[21] précise que sur internet,le prestataire technique n'a pas forcément la capacité d'agir sur les contenus mis en ligne et n'engage pas responsabilité à ce titre. En outre, toute notification de contenus illicites doit être précise afin de permettre à l'hébergeur d'identifier ce contenu en vue de le supprimer.

L'hébergeur engage ensuite sa responsabilité quand il n'agit pas « promptement ». Là encore, le législateur n'a pas défini ce terme « promptement », il fait donc l'objet d'interprétations variables. Il s'agit à chaque fois d'une appréciation in concreto du caractère prompt de l'intervention de l'hébergeur. Mais, un jugement du Tribunal de grande instance de Toulouse[22] a précisé que le terme « promptement » devait être entendu comme signifiant « immédiatement » , ce qui signifie que dès la notification, le fournisseur d'hébergement doit procéder au retrait sans attendre une décision de justice.

Finalement, même si l'hébergeur n'a pas d'obligation de surveillance générale, il est tenu à une obligation de surveillance, en quelque sorte particulière, à partir du moment où il a eu connaissance du caractère illicite du contenu .

Les fournisseurs sont-ils obligés de fournir des informations sur l'identité des utilisateurs?

La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a introduit dans les articles L.34-1-1 du code des postes et des communications électroniques et dans l'article 6 II de la loi du 21 juin 2004, une obligation de conservation et de communication des données de connexion. Cette obligation de conservation des données de connexion est dérogatoire au droit commun qui pose un principe d'effacement des données de communication dès la fin de la communication. Elle est revanche conforme à la directive 2006/24/CE du 15 mars 2006 relative à la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication qui impose aux Etats membres de prévoir une obligation de conservation des données comprise entre six et vingt quatre mois à compter de la communication.
La loi du 23 janvier 2006 a également précisé quelles sont les données concernées par cette obligation. Ainsi, l'article L.34-1, V nouveau du code des postes et des communications électroniques précise que *« les données conservées et traitées dans les conditions définies aux II, III et IV portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.*
Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ».
La durée de conservation des données techniques est d'un an à compter du jour de l'enregistrement (art R.10-13cpce). Si le fournisseur refuse de mettre à disposition ces informations, il encourt une peine d'un an d'emprisonnement et de 75000€ d'amende (art 60-2al3cpp).

En vertu de l'article 6.II de la loi du 21 juin 2004, les fournisseurs d'accès et d'hébergement « *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires. Les fournisseurs d'accès et d'hébergement donnent également aux personnes qui éditent un service de communication au public en ligne « des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III (l.21-6/2004,*

[21]Cass.civ1ère, 17 février 2011, 3 arrêts, n°09-13,202, 09-67,986, 09-15.857)
[22] Ordonnance de référé 13 mars 2008, Krim K. / Pierre G., Amen, www.legalis.net

*art 6).*L'autorité judiciaire peut requérir ces personnes dans le cadre de l'article 60-2cpp. Autrement dit, l'hébergeur est tenu de communiquer les éléments d'identification qu'il est dans l'obligation de posséder, à savoir l'adresse IP et l'adresse de courrier électronique. Cependant, l'article 6-II, dernier alinéa avait prévu qu' *« un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation* ». Ce décret en date du 25 juillet 2011 précise d'une part, quelles sont les données que les fournisseurs d'accès et les hébergeurs doivent conserver et d'autre part, leur durée de conservation.
Quant aux données, tout d'abord, le fournisseur d'accès doit conserver pour chaque connexion de ses abonnés : l'identifiant de la connexion, l'identifiant attribué par le fournisseur d'accès à l'abonné, l'identifiant du terminal utilisé pour la connexion quand il y a accès, les dates et heures de début et de fin de la connexion, les caractéristiques de la ligne de l'abonné. L'hébergeur quant à lui doit conserver, pour chaque opération de création : l'identifiant de la connexion à l'origine de la communication, l'identifiant attribué par le système d'information au contenu, objet de l'opération, les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus, la nature, les dates et heures de l'opération, l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni.
En outre, fournisseurs d'accès et d'hébergement doivent conserver les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte : au moment de la création du compte, l'identifiant de cette connexion ; les nom et prénom ou la raison sociale ; les adresses postales associées ; les pseudonymes utilisés ; les adresses de courrier électronique ou de compte associées ; les numéros de téléphone ; les données permettant de vérifier le mot de passe ou de le modifier, dans leur dernière version mise à jour (D. n° 2012-436, 30 mars 2012, art. 28) . Dans l'hypothèse où la souscription du contrat ou du compte est payant, les informations relatives au paiement (type de paiement, référence du paiement, montant, date et heure de la transaction) doivent être conservées pour chaque opération de paiement.

Quant à la durée de conservation de ces données ensuite, cette durée est d'un an , à compter soit du jour de la création de contenu, soit du jour de la résiliation du contrat ou de la fermeture du compte, soit de la date d'émission de la facture ou de l'opération de paiement.

L'article R.92,23°du code de procédure pénale inclut dans les frais de justice « *Les frais correspondant à la fourniture des données conservées en application du II de l'article L. 34-1 du code des postes et des communications électroniques »*.Quant à l'article R.213-1cpp, il précise *: « Les tarifs relatifs aux frais mentionnés au 23° de l'article R. 92 correspondant à la fourniture des données conservées en application du II de l'article L. 34-1 du code des postes et des communications électroniques sont fixés par un arrêté du ministre de l'économie, des finances et de l'industrie et du garde des sceaux. Cet arrêté distingue les tarifs applicables selon les catégories de données et les prestations requises, en tenant compte, le cas échéant, des surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture de ces données »*.

En revanche, le surcoût lié à la conservation des données n'est pas pris en compte, ce qui risque d'entraîner une augmentation du prix des abonnements des prestataires techniques ou un changement dans leur mode de fonctionnement (ex en recourant davantage à la publicité, ou en proposant de plus en plus de services payants.).

Les fournisseurs d'accès et d'hébergement qui répondent à une demande administrative au titre des missions de prévention des actes de terrorisme (art 6.II bis, LCEN) peuvent voir les surcoûts identifiables et spécifiques des demandes administratives (fourniture des données de connexion sur demande) faire l'objet d'une compensation (art. L. 34-1-1, al. 3 Cpce). L'article 10 du décret du 25 février 2011 renvoie à un remboursement par l'État « par référence aux tarifs et selon des modalités fixés par un arrêté conjoint du ministre de l'intérieur et du ministre chargé du budget ».

4. **Quels éléments généraux, notamment quelles limites constitutionnelles à la criminalisation d'un comportement, ont été discutées en matière d'infractions commises dans le cadre des TIC et d'internet (par exemple, la liberté d'expression, la liberté de la presse, la liberté d'association, le respect de la vie privée, «principe du préjudice», l'exigence de l'élément matériel, l'exigence de l'élément moral)?**

Le conseil constitutionnel a été saisi à l'occasion de l'adoption de la plupart des lois relatives à la cbercriminalité. Ainsi, d'abord, par une décision du 28 décembre 2000[23], il est venu préciser qu « s'il est loisible au législateur, dans le respect des libertés constitutionnellement garanties, d'imposer aux opérateurs de réseaux de télécommunications de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population, est étranger à l'exploitation des réseaux de télécommunications ; que les dépenses en résultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs ».
Ensuite, concernant la répression des manquements à l'obligation de surveillance[24], le Conseil constitutionnel sur le fondement de l'article 11 »[25] de la Déclaration des droits de l'homme et du citoyen de 1789, affirme que la liberté de communication implique la liberté d'accéder aux services de communication au public en ligne mais que le droit de propriété lui même consacré par la Déclaration de 1789 justifie la lutte contre les pratiques de contrefaçon qui se développent sur internet et répond à l'objectif de sauvegarde de la propriété intellectuelle. Dès lors, « il est loisible au législateur d'édicter des règles de nature à concilier la poursuite de l'objectif de lutte contre les pratiques de contrefaçon sur internet avec l'exercice du droit de libre communication et de la liberté de parler, écrire et imprimer ; toutefois, 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 et les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi ».
Enfin, l'institution par la loi du 14 mars 2011 dans son article 4 (non entré en vigueur) d'un dispositif de blocage des adresses électroniques donnant accès à certains sites internet en vue de la lutte contre la diffusion d'images pédopornographiques a été contestée en raison de l'atteinte portée à la liberté de communication par l'impossibilité d'accéder à ces sites. Le conseil constitutionnel[26] a souligné « qu'en instituant un dispositif permettant d'empêcher l'accès aux services de communication au public en ligne diffusant des images pornographiques représentant des mineurs, le législateur n'a commis aucune erreur manifeste d'appréciation ; qu'en prévoyant que les surcoûts résultant des obligations mises à la charge des opérateurs seraient, s'il y a lieu, compensés, il n'a pas méconnu l'exigence constitutionnelle du bon usage des deniers publics », En outre, il ne s'agit que de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile. La décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé. « Dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la

[23]Décision n° 2000-441 DC du 28 décembre 2000 - Loi de finances rectificative pour 2000
[24]Décision n° 2009-580 DC du 10 juin 2009 - Loi favorisant la diffusion et la protection de la création sur internet
[25]« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi »
[26]Décision n°2011-625 DC du 10 mars 2011- Loi d'orientation et de programmation pour la performance de la sécurité intérieure

liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ».

5. La loi prévoit-elle des sanctions pénales visant spécifiquement les cyber-criminels, (par exemple, une interdiction temporaire d'utiliser l'Internet)?

Lorsqu'une infraction de contrefaçon est commise au moyen d'un service de comunication au public en ligne, le prévenu encourt les peines prévues par la loi pour le délit de contrefaçon, soit trois ans d'emprisonnement et 300.000€ d'amende (une amende d'1,5 millions d'euros pour la personne morale assortie éventuellement de peines complémentaires) et, éventuellement, en application de l'article L.335-7 du code de la propriété intellectuelle, la peine complémentaire de suspension de l'accès à internet pour une durée maximale d'un an. Cette suspension ne dispense pas l'auteur de l'infraction du versement du prix de l'abonnement en raison de l'inexécution fautive du contrat par l'abonné. Si la personne qui télécharge n'est pas le titulaire de l'abonnement à internet, ce dernier peut être sanctionné pour non-surveillance et négligence caractérisée. En cas de contravention de négligence caractérisée, la peine complémentaire de suspension de l'accès à internet est d'une durée maximale d'un mois (art L.335-7-1CPI). Dans les deux cas, cette suspension d'accès ne concerne pas les autres services éventuellement inclus dans l'abonnement (ex téléphonie, télévision), elle se révèle donc, en pratique, impossible à réaliser. En outre, la suspension de l'accès à internet empêche aussi l'accès à l'offre légale , ce qui constitue une atteinte car la liberté d'accéder à internet se rattache à la liberté d'expression.

E. Alternatives à la criminalisation

1. **Quel est le rôle du droit pénal par rapport à d'autres moyens de lutte contre l'abus des TIC et d'internet?**

Quelles sont les relations qui existent entre les sanctions civiles ou les sanctions administratives (paiement de dommages et intérêts, la fermeture de l'entreprise, etc) et les sanctions pénales dans le domaine des TIC?

Le droit pénal, par rapport à d'autres moyens de lutte contre l'abus des TIC et d'internet, joue un rôle dissuasif à l'égard du passage à l'acte, en raison du pouvoir de contrainte attaché à la règle pénale. Cet arsenal répressif est utilement complété par des dispositions civiles qui sont orientées vers la réparation des préjudices éventuellement causés par l'abus des TIC ou d'internet et vers la remise en cause du lien contractuel unissant les parties. Quant aux sanctions administratives, elles émanent pour l'essentiel d'autorités administratives indépendantes qui usent de leur pouvoir d'une part, de prévention, par des mises en demeure, et d'autre part, de sanctions, par le prononcé de sanctions à caractère pécuniaire pour l'essentiel.

Pour de nombreuses infractions commises par internet, des sanctions civiles peuvent être prononcées. Tel est le cas par exemple, en cas de violation de la vie privée, d'atteintes au droit à l'image. Dans le cadre de la lutte contre le téléchargement illégal, des mesures de blocage de l'accès à internet pourraient être prises (art 4, Loi du 14 mars 2011) outre, les poursuites pour contrefaçon exposant à des sanctions pénales (amende, emprisonnement, confiscation du matériel informatique) et le risque de sanctions civiles telles que la résiliation de l'accès à internet, la condamnation à des dommages et intérêts au profit de plaignants.

Dans le cadre de la mise en œuvre des traitements de données personnelles, la CNIL peut infliger des sanctions administratives (art 44 à 49, L,6/1/1978), essentiellement à caractère pécuniaire, dès lors que les dispositions de la loi du 6 janvier 1978 relative au traitement de

données personnelles ne sont pas respectées. Ces dispositions sont complétées par des sanctions pénales prévues aux articles 226-16 à 226-24cp.

(2) Quels moyens d'attaques non criminelles sont utilisés/propagés à l'encontre de sites Web (par exemple, fermeture des sites Web, blocage de l'accès aux sites Web) ?

La loi du 14 mars 2011 (LOPPSI 2) a introduit la possibilité pour l'autorité administrative « lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23cp le justifient » de notifier aux fournisseurs d'accès à internet les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ceux-ci doivent empêcher l'accès sans délai. Il s'agit ici d'un moyen pour priver d'accès à internet à propos duquel certains, lors des débats autour de la loi, ont émis des craintes quant au risque d'abus dans le filtrage.Le Conseil constitutionnel a été saisi de cette question et a considéré que ce dispositif tend à la protection des internautes.Il vise principalement à lutter contre les sites hébergés à l'étranger. Les décisions de filtrage sont adressées aux fournisseurs d'accès à internet par l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.
Les personnes coupables d'infractions de contrefaçon, notamment en cas de téléchargement illégal, peuvent également être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne 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 L.335-7cpi).

(3) Par quels moyens les utilisateurs des TIC devraient-ils se protéger (par exemple, par le cryptage des messages, en utilisant des mots de passe, en utilisant la protection du logiciel)?

La loi du 21 juin 2004 pour la confiance dans l'économie numérique est venue libéraliser la cryptologie en posant le principe de la liberté d'utilisation des moyens de cryptologie càd « tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète ».
La loi rappelle que la communication au public par voie électronique est libre et que « l'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.
Outre la cryptologie, les utilisateurs de TIC sont invités à protéger leurs données par l'installation de programmes antivirus, d'anti spyware etc..Mais, il n'y a aucune obligation légale ou réglementaire en la matière.

Y a-t-il des sanctions pour ne pas avoir protégé son ordinateur, dans la mesure du raisonnable (par exemple, en utilisant un logiciel antivirus ou en protégeant l'accès à des réseaux privés par mot de passe)? Le manque d'auto-protection raisonnable fournit-il un moyen de défense pour les mis en cause accusés d'avoir pénétré illégalement dans le réseau ou d'avoir abusé du réseau informatique d'autres personnes ou d'avoir abusé de leurs données?

En matière de téléchargement illégal, la contravention de négligence caractérisée sanctionne non pas la contrefaçon constatée par l'Hadopi au sens des articles L.335-2 et s. CPI mais le défaut de sécurisation de l'accès à internet. Selon l'article R.335-5 du code de la propriété littéraire et artistique, toute personne titulaire d'un service de communication au public en ligne qui, sans motif légitime, n'a pas mis en place un moyen de sécurisation de cet accès ou a manqué de diligence dans la mise en œuvre de ce moyen est passible d'une contravention de cinquième classe. Au préalable, la personne devra avoir reçu une recommandation de la commission de protection des droits et avoir, malgré celle-ci, à nouveau utilisé son accès à internet en violation des droits d'auteur dans l'année qui suit. Les personnes jugées coupables pourront également être condamnées à la peine complémentaire de suspension de l'accès à internet.

Or, des difficultés probatoires se posent car il peut y avoir eu échange de fichiers illégaux même si un dispositif de sécurisation a été mis en place, auquel cas, la négligence caractérisée de l'utilisateur est présumée dans le procès verbal dressé par l'Hadopi. Ce procès-verbal fait foi jusqu'à preuve contraire.

F. Limiter l'anonymat

1. Y a-t-il des lois ou des règlements obligeant les fournisseurs de services internet à stocker des données personnelles des utilisateurs, y compris l'historique de l'utilisation d'Internet?

Cf point D.3
La conservation des données de connexion est une obligation prévue par la loi. En cas de manquement à cette obligation des peines sont prévues par les articles 6-VI de la loi du 21 juin 2004 (dite LCEN) et L. 39-3 du Code des postes et communications électroniques : un an d´emprisonnement et 75.000 euros d´amende, le quintuple pour les personnes morales.
Sont concernés par cette obligation de conservation des données personnelles des utilisateurs, y compris les données de connexion :

- les opérateurs de communications électroniques
- les fournisseurs d'accès (art 6.II de la loi du 21 juin 2004, les fournisseurs d'accès et d'hébergement « *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires. Les fournisseurs d'accès et d'hébergement donnent également aux personnes qui éditent un service de communication au public en ligne « des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III »)*
- les personnes privées qui offrent au public une connexion internet telles que les cybercafés, les hôtels, les compagnies aériennes etc.. (art. L34-1 du CPCE),
- certains organismes publics et privés (ex établissements financiers, organismes sociaux) ;
- les entreprises qui offrent un accès internet à leurs salariés ;

Les fournisseurs peuvent-ils être contraints de fournir ces données aux autorités judiciaires?

L'autorité judiciaire peut requérir ces personnes dans le cadre de l'article 60-2cpp. Ces données doivent pouvoir être mises à la disposition des autorités des services chargés de la lutte contre sous peine de sanctions civiles ou pénals. C´est en effet la loi n°2006-64 du 23

janvier 2006 (contre le terrorisme qui a introduit, aux articles L.34-11 du Code des postes et communications et 6 II bis de la loi du 21 juin 2004, dite LCEN, cette obligation. En vertu de ces textes, les « agents individuellement désignés et dûment habilité des services de police et de gendarmerie» en charge de la lutte anti-terrorisme peuvent obtenir des opérateurs la communication de certaines des données conservées et traitées en application de l´article L.34-1 du Code des postes et communications électroniques, sans autorisation judiciaire préalable. En effet, la décision revient à une personnalité qualifiée qui apprécie les demandes motivées de communications adressées par les services de lutte contre le terrorisme. Cette personnalité est désignée par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l´Intérieur, auprès de qui elle est placée. La Commission dispose d´un pouvoir de contrôle restreint : si elle peut contrôler les opérations de communication des données, elle ne peut, en cas de constat de manquement aux règles de communication des données ou d´atteintes aux droits et libertés, qu´adresser des recommandations au ministre de l´Intérieur.

2. Y a-t-il des lois ou des règlements obligeant un fournisseur de services Internet à enregistrer les utilisateurs avant de leur fournir des services?

La loi oblige tout fournisseur d'accès à internet (y compris par wifi) à conserver toutes les données de connexion des utilisateurs pendant un an et à les tenir à la disposition des autorités judiciaires. Le décret du 25 février 2011 (n° 2011-219), relatif à la conservation et à la communication des données précise cela en énonçant que les FAI et les cybercafés doivent obligatoirement conserver certains contenus et certaines données pendant un an :
• Identifiants de connexion ;
• Identifiants attribués aux abonnés ;
• Identifiants du terminal utilisé pour la connexion lors d'un accès ;
• Dates et heures de début et de fin de connexion ;
• Caractéristiques de ligne de l'abonné.

Les « fournisseurs de Wi-Fi » peuvent choisir d'offrir la connexion à internet sans procéder à l'identification des personnes. Ils ne sont alors tenus de détenir que les données techniques créées par l'utilisation de leurs services. Dans ces conditions, il n'existe aucune obligation de constitution de fichiers nominatifs des utilisateurs pour les services de communication électroniques offerts au public. Ces données de trafic pourront alors être consultés par la police et la gendarmerie dans un cadre judiciaire ou par la voie d'une réquisition administrative pour prévenir le terrorisme. es opérateurs wifi ne sont pas obligés de relever et de conserver l'identité des utilisateurs désireux de se connecter. Il ne son donc pas obligés de créer un fichier nominatif. Ainsi, si l'opérateur décide de ne conserver que les seules données techniques de connexion, il n'a aucune obligation de déclaration de son fichier auprès de la CNIL (ou de contrôle par son CIL). En revanche, s'il fait le choix de procéder à l'identification préalable des utilisateurs, en leur faisant remplir une fiche d'inscription par exemple, il est soumis à une obligation de déclaration auprès de la CNIL (ou à un contrôle par un CIL). En effet, toute connexion par identifiant implique la collecte de données personnelles et donc un traitement particulier. Seules les autorités judiciaires disposent de possibilités d'accès à de telles données (à l'aide d'une commission rogatoire). Toute autre personne ne peut accéder qu'à des données anonymisées.
La loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet a modifié l'article L. 34-1 du CPCE de façon à permettre aux opérateurs de communications électroniques de communiquer à l'HADOPI les données à caractère personnel et informations relatives à leurs abonnés recueillies en application de l'article L. 34-1 du CPCE. Le décret du 5 mars 2010 a mis en place le « Système de gestion des mesures pour la protection des œuvres sur internet » sur lequel sont enregistrées les données à caractère personnel et

informations relatives aux abonnés recueillies auprès des opérateurs de communications électroniques par l'HADOPI. Selon le décret du 5 mars 2010, ces données sont les suivantes : Nom de famille, prénoms ; adresse postale et adresses électroniques ; crdonnées téléphoniques ; adresse de l'installation téléphonique de l'abonné. Or, depuis la loi du 23 janvier 2006, les « fournisseurs de Wi-Fi » sont soumis aux mêmes obligations que les opérateurs de communications électroniques classiques.Ils peuvent donc être amenés à répondre à une réquisition adressée par l'HADOPI. Pour autant, et comme précédemment indiqué, il ne résulte ni de l'article L. 34-1, ni de l'article R.10-13 du CPCE une obligation pour celui-ci d'identifier les utilisateurs, ni de se faire communiquer préalablement à la connexion leurs noms, prénoms, adresses et coordonnées téléphoniques. Ils doivent simplement disposer d'éléments permettant cette identification.

3. Y a-t-il des lois ou des règlements limitant le cryptage des fichiers et des messages sur internet? Les suspects peuvent-ils être contraints de divulguer les mots de passe qu'ils utilisent?

L'article 434-15-2cp punit de trois ans d'emprisonnement et de 45.000 euros d'amende, le fait, pour quiconque ayant connaissance de la convention secrèteee de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités. Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75000 € d'amende. Ce délit est intentionnel puisqu'ici, on incrimine le comportement d'une personne qui a connaissance de la convention secrète de déchiffrement et qui « refuse » de remettre celle ci.

G. Internationalisation

1. Le droit interne s'applique-t-il aux données introduites sur internet depuis l'étranger? Y a-t-il une exigence de «double incrimination» à l'égard de la saisie des données provenant de l'étranger?

2. Dans quelle mesure le droit pénal de votre pays dans le domaine des TIC et d'internet est-il influencé par les instruments juridiques internationaux?

3. Votre pays participe-t-il à des discussions sur l'harmonisation des législations dans le domaine de la cybercriminalité (comme le groupe intergouvernemental d'experts sur la cybercriminalité de l'ONU)?

H. Les développements futurs

Veuillez indiquer les tendances actuelles de la législation et les débats juridiques dans votre pays dans le domaine les TIC et de la criminalité sur internet ?

En matière de téléchargement illégal sur internet, l'Union européenne a signé en janvier 2012, le traité ACTA (Anti-Counterfeiting Trade Agreement) qui vise essentiellement à une coopération entre les ayants droits et les opérateurs privés sur internet, en permettant aux ayants droit, dans le cadre d'une procédure judiciaire, de demander, sans l'autorisation ou le contrôle du juge, aux fournisseurs d'accès à internet des informations à caractère privé, sur un

site. Ce traité a pour objectif d'harmoniser au niveau international la lutte contre le téléchargement illégal et impose aux entreprises une forme d'obligation de surveillance. Or, la CJUE s'est déjà prononcée , en se fondant sur les directives européennes en la matière, contre le filtrage par les fournisseurs d'accès de toutes les communications électroniques de leurs clients afin de bloquer le transfert de fichiers provenant d'un logiciel de pair à pair qui porte atteinte au droit d'auteur. La CJUE considère que le droit de protection de la propriété intellectuelle ne peut pas être assuré de façon absolue. C'est sans doute la raison pour laquelle elle a renforcé, récemment encore, cette position en considérant que « l 'exploitant d'un réseau social en ligne ne peut être contraint de mettre en place un système de filtrage général visant tous ses utilisateurs, pour prévenir le chargement illicite d'œuvres musicales et audiovisuelles ». Elle justifie l'interdiction du filtrage par l'atteinte portée aux droits fondamentaux des citoyens européens ;en effet, le filtrage imposerait « une surveillance générale des informations stockées, ce qui est interdit par la directive sur le commerce électronique ». Dans un tel contexte, peut-on envisager, comme certains le préconisent, de demander aux fournisseurs d'accès et aux moteurs de recherche d'empêcher l'accès aux sites de streaming ou de téléchargement illégal ? L'Hadopi, sur la base des évaluations qu'elle est en train de réaliser, songe à faire évoluer ses techniques de lutte (notamment le rôle des Labs) et les outils juridiques mis à sa disposition. Il est, notamment, prévu d'engager le dialogue avec les sites, les plateformes concernées ainsi que les intermédiaires (Etablissements bancaires, intermédiaires de paiement) afin de voir comment il serait possible de les impliquer dans la lutte contre le téléchargement illégal. Cette perspective découle de deux projets américains similaires - PIPA et SOPA -, qui veulent autoriser le filtrage de tous les sites qui proposent du téléchargement illégal, et proposaient même, dans leur version initiale, le blocage de ces sites par nom de domaine (DNS) . Quant aux sites de téléchargement direct ou de streaming, ces projets envisagent leur déréférencement sur les moteurs de recherche et l'interdiction faite aux opérateurs de paiement en ligne (ex : paypal) de travailler avec les sites en cause.

Ensuite, loin de ces objectifs à tendance fortement répressive, il apparaît alors opportun d'appréhender le phénomène du téléchargement illégal dans une perspective de conciliation des intérêts en présence plutôt que d'opposition vaine. En effet, la démarche de labellisation entreprise par l'Hadopi permet, d'une part, à l'internaute de s'assurer du caractère légal des offres en ligne auxquelles il accède et d'autre part, aux auteurs d'être rémunérés pour leurs œuvres. Elle est encouragée par le constat, suite à la fermeture de MegaUpload, « d' un déplacement des utilisateurs vers les offres légales directement substituables, accessibles sur le Web depuis un ordinateur personnel » . A plus long terme, l'existence d'une offre légale diversifiée et labellisée s'oppose à la reconnaissance de la bonne foi de l'utilisateur d'un site illicite.

Enfin, certains membres de la Commission Olivennes ont en leur temps suggérer de « favoriser l'émergence de nouveaux modèles économiques diversifiant les modes d'accès à la culture pour éviter encore la rigidité d'un choix entre le tout payant et le tout gratuit » . C'est alors la licence globale qui est soutenue par certains, en tant que « dispositif visant à financer une partie de la production de contenus audiovisuels en rémunérant les artistes, auteurs-compositeurs et producteurs, sur la base d'une rétribution forfaitaire payée par les internautes en supplément de leur abonnement à Internet. En contrepartie de cette rétribution, les internautes ont l'autorisation d'accéder à des contenus audiovisuels en ligne, de les télécharger et de les échanger entre eux à des fins non commerciales » . La licence globale a été rejetée, notamment lors des débats sur Hadopi, car elle constitue, à certains égards, une atteinte au droit d'auteur « à la française » mais aussi, une solution économique permettant d'assurer une rémunération à la création. Il convient de prendre en compte les exigences des conventions internationales, notamment la directive sur l'harmonisation de certains aspects du droit d'auteur et les traités de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) , qui reconnaissent à l'auteur un droit exclusif quant à la mise à disposition de ses œuvres, quel que soit le support. Dès lors, la licence globale qui vise à transformer ce droit exclusif en droit

à rémunération violerait en l'état, les dispositions de l'article 55 de la Constitution. Dans une perspective d'harmonisation au niveau de l'union européenne, une étude réalisée par la Direction générale des politiques internes de l'Union Européenne à la demande du Parlement européen et publiée fin 2011 préconise la mise en place d'un « forfait sur le contenu » pour les œuvres audiovisuelles, acquises légalement. Il s'agit d'une licence globale mensuelle qui s'ajouterait, facultativement, au montant du forfait internet et qui permettrait aux internautes de télécharger des films et oeuvres audiovisuelles en toute légalité en partage de fichiers (P2P). Cette licence globale mensuelle pourrait être proposée à un tarif d'environ 5€ par mois, ce qui la rendrait compatible avec les offres premium en matière de VOD et d'abonnement DVD. Cette proposition d'harmonisation au niveau de l'Union européenne s'avère nécessaire pour protéger les droits des auteurs et des artistes-interprètes et elle constituerait une solution intermédiaire de licence globale de l'offre légale . Mais elle confirme surtout qu'il est illusoire de croire que l'on peut revenir au système de protection antérieur à la naissance d'internet. L'Hadopi a, sans doute, dans ce contexte, une nouvelle place à prendre dans le contrôle et la régulation des pratiques.