# LA CYBERCRIMINALITÉ, CRIMINALITÉ DU XXI^E SIÈCLE

Marc WATIN-AUGOUARD

*Directeur du Centre de recherche de l'EOGN*
*Président du Centre expert de lutte contre la cybercriminalité français (CECyF)*
*Fondateur du Forum international de la cybersécurité (FIC)*

En 1969, alors que Léonard Kleinrock vient d'opérer la première connexion du réseau ARPANET entre quatre universités américaines[1], l'informatique suscite peu d'inquiétudes. L'accès aux bibliothèques, l'échange de documents entre scientifiques ne semblent pas encore de nature à générer une forme nouvelle de criminalité. Mais, quelques années plus tard, la cybercriminalité est en plein essor. Le cyberespace est le nouvel Eldorado des criminels et des délinquants. La transformation numérique de la société leur offre une extraordinaire opportunité, grâce à un transfert du champ du « réel » vers celui de « l'immatériel » qui optimise les gains escomptés avec un risque pénal très faible. Le « chiffre noir » de la cybercriminalité est l'un des plus élevés, notamment parce que les personnes physiques ou morales visées ignorent souvent les faits[2]. Jamais, sans doute, le prédateur n'a été aussi près de sa victime puisqu'il est avec elle[3], devant elle et, demain, en elle[4]. Jamais aussi il n'a été aussi loin de son juge, ne serait-ce qu'en raison des frontières juridiques et de la lenteur de la coopération judiciaire comparée à la vitesse des transactions sur la Toile. C'est pour ces raisons que l'on peut parler de « criminalité du XXI^e siècle[5] ».

Il n'y a pas de définition universelle de la cybercriminalité. La Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, principal instrument normatif international, ne donne pas de définition mais dresse une liste d'infractions qui en relèvent :

- Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, domaine de la sécurité des systèmes d'information (SSI) : accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs ;

---

[1] Le 5 déc. 1969, un premier lien unit l'université de Californie à Los Angeles, le Stanford Research Institute, l'université d'Utah et l'université de Californie de Santa Barbara.
[2] Selon le rapport 214-M-Trend de Mandiant, une entreprise découvre une « menace persistante avancée » (APT) au bout de 229 jours, en moyenne. Sébastien Héon (Airbus Défense Sécurité) avance une durée de 416 jours.
[3] Tous les objets connectés (smartphones, bracelets, lunettes à réalité augmentée, etc.) sont des portes d'entrée pour la cybercriminalité.
[4] Par exemple, au travers d'organes, de prothèses, etc. On sait intervenir à distance sur un pacemaker, ce qui permet d'exercer un chantage.
[5] Watin-Augouard M., éditorial FIC 2007.

- Les infractions informatiques : falsification informatique, fraude informatique ;
- Les infractions se rapportant au contenu et portant sur la pornographie enfantine ;
- Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

Plus simple et sans doute plus opérante est la définition retenue par le rapport du procureur général Marc Robert[6] : « la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement internet ». Elle est très voisine de celle de l'Union Européenne, pour qui « la cybercriminalité devrait s'entendre comme des infractions pénales commises à l'aide de réseaux de communications électroniques et de systèmes d'informations ou contre ces réseaux ou systèmes [7]». Elle retient la cible et l'outil sans risquer de se perdre dans une classification selon les auteurs, les mobiles ou les modes d'action.

Initialement, la première prise de conscience du risque « cyber » concerne le rapport entre l'État et le citoyen, au moment où les fichiers automatisés se développent. Après 1978 et la loi relative à l'informatique, aux fichiers et aux libertés, le législateur porte son attention sur les attaques visant les systèmes de traitement automatisés de données qui font l'objet de la loi Godfrain (1988). Puis la cybercriminalité élargit son périmètre aux « contenus ». Il ne s'agit pas, dans ce cas, d'infractions dont le cyberespace est la cible mais le vecteur. Les contenus, hébergés, échangés ou diffusés, sont susceptibles de constituer des infractions qui existent déjà dans le monde réel mais prennent une autre dimension en raison de la diffusion planétaire des messages, de leur accessibilité et de l'application encore incertaine d'un « droit à l'oubli ».

Outre les infractions de contenu, des infractions, identifiées de longue date dans le monde réel, ont des conséquences d'une toute autre ampleur en raison du nombre potentiel de victimes et de la capacité de dissimulation des auteurs. Ces infractions « facilitées » par les technologies numériques concernent le plus souvent la délinquance économique et financière. Il s'agit notamment du blanchiment, de l'escroquerie, des fraudes de toute nature. Elles font souvent appel à l'ingénierie sociale, forme déloyale d'acquisition d'informations exploitant les failles humaines et sociales de la victime. Ces infractions sont parfois associées à une usurpation d'identité en ligne[8] et à des techniques de hameçonnage[9], de piratage de nom de

[6] Robert M., *Protéger les internautes*, rapport sur la cybercriminalité, février 2014, p. 12.

[7] « Vers une politique générale en matière de lutte contre la cybercriminalité », communication COM(2007) de la Commission au Parlement européen, au Conseil et au Comté des régions, du 22 mai 2007.

[8] L'usurpation d'identité en ligne (art. 226-4-1 du code pénal) est une infraction créée par la loi n° 201-267 d'orientation et de programmation pour la performance de la sécurité intérieure. Il est courant de recevoir un mail d'un proche appelant au secours depuis l'étranger ; son identité a été usurpée, son carnet d'adresse exploité.

[9] Le hameçonnage ou filoutage (*phishing*) permet une récupération de données personnelles par usurpation d'identité de personnes morales publiques ou privées de grandes sociétés ou d'organismes financiers. Un lien hypertexte renvoie vers une page qui est une copie conforme d'une page officielle. Cette méthode permet un collecte frauduleuse de données à caractère personnel, notamment bancaires.

domaine[10] ou de carte bancaire[11]. L'escroquerie « à la nigériane », l'escroquerie « au faux président » ou les rançongiciels[12] constituent des cyber-infractions désormais classiques. Le cyberespace est un refuge pour les trafiquants, grâce aux marchés noirs qui s'y développent[13]. Il est un vecteur idéal pour la traite des êtres humains, les trafics de stupéfiants, de médicaments contrefaits, de produits dopants. Si toutes les monnaies virtuelles ne relèvent pas de la cybercriminalité financière, beaucoup y contribuent[14].

Le corpus juridique relatif à la cybercriminalité se développe de manière pragmatique, au fur et à mesure que les usages des technologies numériques révèlent des comportements illicites. Depuis la loi relative à la sécurité quotidienne du 15 novembre 2001, chaque loi concernant la sécurité comprend des dispositions nouvelles qui modifient le droit ou la procédure pénale. On peut citer la LOPSI (2002), la loi pour la sécurité intérieure (2003), la loi dite Perben II (2004), la loi relative à la prévention de la délinquance (2007) et la LOPPSI (2011). Mais des lois poursuivant un autre objet peuvent aussi créer de nouvelles incriminations ou de nouvelles procédures, telles la loi pour la confiance dans l'identité numérique (2004), la loi relative à la protection de l'identité (2012), la loi sur l'égalité réelle entre la femme et l'homme (2014), bonnes illustrations d'un développement quasi-simultané de nouveaux usages et d'infractions spécifiques.

D'une manière générale, les conséquences humaines ou matérielles de la cybercriminalité poussent le législateur à durcir, par des circonstances aggravantes, la répression d'infractions commises dans le monde réel, en considérant que l'usage, par leur auteur, d'un réseau de communication électronique augmente leur dangerosité.

L'écosystème législatif relatif à la cybercriminalité ressemble à un « mille-feuille ». Il se forme par sédimentation. La logique de codification ne favorise pas une vision globale d'une législation aujourd'hui éclatée entre plusieurs codes (code pénal, code des postes et télécommunications électroniques, code du commerce, code de la consommation, code des postes et des communications électroniques, code de la propriété intellectuelle, code monétaire et financier, code de la défense, code de la sécurité intérieure, etc.).

La loi du 13 novembre 2014[15] renforçant les dispositions relatives à la lutte contre le terrorisme s'inscrit dans cette construction législative en modifiant le droit et la procédure pénale et en renforçant les pouvoirs de police administrative

[10] Le *pharming*, piratage d'un nom de domaine (le plus souvent d'une banque). Un cheval de Troie redirige l'internaute vers un faux site web qui reçoit ses données personnelles, notamment bancaires.
[11] *Skimming* (piratage et clonage de cartes bancaires à partir des distributeurs automatiques de billets), *carding* (création de cartes virtuelles à partir d'éléments acquis frauduleusement sur internet).
[12] Logiciels malveillants qui bloquent l'ordinateur d'une victime et réclament le paiement d'une rançon. Par exemple, faux mail de la gendarmerie imposant le paiement d'une amende pour exploration de sites illégaux (pédopornographiques, en particulier).
[13] CEIS, *Les marchés noirs de la cybercriminalité*, Paris, juin 2011. www.ceis.eu
[14] Liberty Reserve, en particulier. Ses membres fondateurs et administrateurs ont été mis en accusation par le procureur de New York, le 28 mai 2013.
[15] Loi n° 2014-1353 du 13 nov. 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

spéciale. En particulier, elle enrichit la loi Godfrain et renforce le contrôle sur les contenus.

## I. Les atteintes aux systèmes de traitement automatisé de données (STAD)

Le législateur est avant-gardiste lorsqu'en 1988 il adopte la proposition de loi du député Jacques Godfrain[16] qui incrimine les atteintes aux systèmes de traitement automatisé de données. Environ 5000 machines sont alors reliées à Internet[17]. Ce texte n'a pas pris de rides, car il n'a pas été associé à des technologies particulières qui auraient pu le rendre obsolète dès leur première évolution. Il est hélas plus que jamais d'actualité, tant les systèmes de traitement automatisés de données apparaissent aujourd'hui vulnérables aux attaques, qu'il s'agisse de l'informatique de gestion, des serveurs web, des systèmes numériques de contrôle-commande (SNCC), des systèmes de supervision et de contrôle (SCADA[18]) ou des automates programmables industriels (API). La loi Godfrain[19] est régulièrement abondée par des apports comme ceux de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, de la loi du 27 mars 2012 relative à la protection de l'identité, de la loi de programmation militaire du 18 décembre 2013, ou de la récente loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. La loi Godfrain est donc vivante, évolutive.

### *A. L'accès ou le maintien frauduleux dans un STAD*

L'article 323-1 du code pénal sanctionne le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données. Le terme « frauduleux » souligne bien la conscience chez le délinquant que l'accès ou le maintien lui est interdit. La cour d'appel de Paris a considéré que « l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais entre dans un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication ». L'entrée frauduleuse oblige souvent à « casser » un mot de passe, mais elle peut être constituée par l'utilisation d'un système auquel un individu n'a pas de droit d'accès. Elle peut aussi être facilitée par un logiciel espion ou un « cheval de Troie » qui permet de prendre le contrôle d'un ordinateur à distance.

Mais le délit n'est pas constitué si le système n'est pas protégé contre les intrusions[20]. Ainsi, l'accès par erreur à un site non sécurisé ne peut être incriminé[21]. Si la cour d'appel de Paris du 5 février 2014 sanctionne un internaute entré par erreur sur l'extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES), c'est parce qu'il avait « conscience de son

[16] Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique.
[17] C'est en 1989 qu'Internet s'ouvre au grand public et à l'exploitation commerciale.
[18] *Supervisory Control And Data Acquisition.*
[19] Ce que l'on dénomme aujourd'hui « Loi Godfrain » correspond en réalité au chapitre III du titre II du livre III du code pénal consacré aux systèmes de traitement automatisé de données. Cela démontre que cette loi demeure la référence.
[20] TGI Créteil, 21 fév. 2013
[21] CA Paris, 30 oct. 2002, *Kitetoa c.Tati.*

maintien irrégulier dans le système de traitement automatisé de données visité où il a réalisé des opérations de téléchargement de données à l'évidence protégées ». S'agissant du maintien frauduleux, la Cour de cassation[22] qualifie ainsi le fait de se connecter gratuitement avec son personnel avec un code d'accès après une période d'essai (le code n'étant plus demandé).

### *B. L'entrave au fonctionnement d'un STAD*

L'article 323-2 du code pénal réprime le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données. Constitue, par exemple, une entrave au fonctionnement d'un système de traitement automatisé de données, le fait de procéder à une attaque par « mailbombing » adressant simultanément 12 000 messages identiques[23] qui vont ralentir ou bloquer le fonctionnement par saturation. Cette action peut consister également en une attaque par déni de service (DOS[24]) qui met en action plusieurs milliers d'ordinateurs « zombies ». En janvier 2012, à la suite de la fermeture du site Megaupload par le FBI, de nombreux sites officiels ont fait l'objet d'une telle attaque par les Anonymous. L'intention de nuire doit être prouvée, comme le précise la cour d'appel de Bordeaux, dans un arrêt du 15 novembre 2011[25]. L'injection d'un ver ou d'un virus est aussi constitutive de cette infraction.

### *C. La protection pénale des données*

L'article 323-3 du code pénal réprime l'introduction, la suppression ou la modification frauduleuse de données dans les systèmes de traitement automatisé. Ces données peuvent être modifiées par défiguration (ou défacement ou « tag numérique ») de sites dans lesquels l'attaquant s'introduit pour changer le contenu des pages web. Cette action a pour objectif de nuire à l'image d'une personne (la photo d'une personnalité politique est remplacée par celle d'Hitler) ou à la réputation d'une entreprise. La modification peut consister en un remplacement de données (changement des notes d'un candidat à un examen, modification des prix pratiqués par un service de commerce en ligne).

L'article 323-3, modifié par la loi du 13 novembre 2014 (art. 16), réprime désormais l'extraction, la détention, la reproduction, la transmission de données contenues dans le système. Ainsi répond-on à un vide juridique que la jurisprudence avait tenté de combler relativement au vol de données. Selon l'article 311-1 du code pénal, le vol est la soustraction frauduleuse de la chose d'autrui. Cette chose est un

---

[22] Cass. Crim., 3 oct. 2007, n° 07-81.045.

[23] TGI Nanterre, 8 juin 2006, *Sté Amen c. Michel M*, n° 06-13971065.

[24] Il s'agit notamment d'attaques par déni de service (*Denial off Service*-DOS), à partir de milliers d'ordinateurs « zombies », dont l'attaquant a pris le contrôle pour adresser à la cible autant de requêtes simultanées qui le saturent. La location d'un botnet de 80 à 120 000 machines revient environ à 200$, ce qui fait du botnet l'arme du pauvre. Un réseau des machines infectées est à l'origine de l'attaque subie par la NSA, le 25 oct. 2013.

[25] La cour d'appel relaxe le prévenu qui, avec un robot générant 1569 connexions en deux heures, avait, selon la plaignante C-Discount, ralenti puis bloqué son site. La cour relève que le trafic du site est de 16.000 requêtes/heure et que, selon un expert, une attaque efficace devrait être de 80 000 requêtes/heure. Elle souligne les moyens dérisoires déployés par le prévenu au regard des capacités informatiques du site.

bien matériel et non immatériel[26]. La copie de données n'est pas une soustraction, puisque le légitime propriétaire les conserve et n'est à aucun moment dépossédé de la chose. Dans un arrêt du 4 mars 2008[27], la Cour de cassation a qualifié de vol une copie de données, mais cette décision s'éloigne du principe selon lequel la loi pénale est d'interprétation stricte. La modification de la loi règle désormais le problème.

### *D. La protection renforcée des systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'État*

La loi assortit chacune des trois infractions précitées d'une aggravation de peine lorsqu'elles sont commises à l'encontre d'un système de traitement automatisé de données à caractère personnel[28] mis en œuvre par l'État. Cette disposition, introduite par la loi relative à la protection de l'identité[29], à notamment pour objectif de protéger la base centrale des titres sécurisés, le casier judiciaire, le fichier des empreintes génétiques (FNAEG), etc.

L'écriture des articles précités semble indiquer que les autres STAD mis en œuvre par l'État ne sont pas concernés. Les plus sensibles sont toutefois pris en compte par l'article 411-9 du code pénal relatif à la protection des intérêts fondamentaux de la nation. On notera que les peines sont alors de quinze ans de détention criminelle, ce qui requiert un degré de gravité particulier quant à l'attaque et à ses conséquences.

### *E. La lutte contre la prolifération*

La loi sur la confiance dans l'économie numérique (LCEN) renforce le dispositif de la loi Godfrain en réprimant l'importation, la détention, l'offre, la cession ou la mise à disposition d'un instrument, d'un programme informatique ou de toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 à 323-3. Par exemple, la Cour de cassation[30] retient l'intention coupable d'un individu ne pouvant ignorer, en raison de son expertise, qu'il diffuse sur le portail interne, accessible à tous, d'une société dont il est le gérant, des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance.

Elle exclut du champ de l'infraction les actes accomplis avec un motif légitime, notion jugée trop vague par le législateur qui la précise, avec la loi de programmation militaire du 18 décembre 2013, en mentionnant la recherche et la

---

[26] Pour le vol d'énergie, bien immatériel, le législateur a créé une incrimination spécifique : art. 311-2 c. pén.

[27] Cass. crim., 4 mars 2008, *X c. Sté Graphibus*, n° 07-84.002.

[28] Selon l'article 2 de la loi « informatique et libertés », « constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

[29] Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité (art. 9).

[30] Cass. crim., 27 oct. 2009, n° 09-82.346, *Bull.* n° 177.

sécurité informatique. Compte tenu de la montée en puissance de la cyberdéfense, il est, en effet, indispensable d'écarter la responsabilité pénale des policiers, gendarmes, membres des armées, ingénieurs, experts, etc. appelés à utiliser ces moyens pour comprendre les attaques, voire pour mener, dans le cadre de la stratégie de cyberdéfense, une action plus « offensive ».

### *F. La pluralité des acteurs*

L'action du hacker isolé demeure d'actualité mais n'est pas de nature à déstabiliser un état, un secteur critique, une entreprise. Dès 1988, la loi Godfrain a prévu la pluralité des auteurs d'attaques informatiques en réprimant l'association de malfaiteurs (art. 323-4). La mise en évidence d'une association de malfaiteurs permet d'agir à titre préventif, au stade de la préparation de l'infraction.

La loi renforçant les dispositions relatives à la lutte contre le terrorisme introduit la circonstance aggravante de bande organisée (art. 323-4-1) qui répond au passage du hacker isolé au groupe structuré, organisé. Par exemple, le groupe appelé Cybervor serait composé d'une douzaine de russes, dont l'activité a été révélée en août 2014. À leur actif, le piratage de 1,2 milliards de données (combinaisons d'email et de mots de passe) sur 420.000 sites web. On est loin du pirate isolé des années quatre-vingt. Cette aggravation ne concerne que les atteintes aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'État.

Les infractions de la loi Godfrain ne figurent pas dans la liste dressée par l'article 706-73 du code de procédure pénale, mais l'article 706-74 du même code dispose que « lorsque la loi le prévoit, les dispositions du présent titre sont également applicables aux crimes et délits en bande organisée autres que ceux relevant de l'article 706-73 ». Dans le nouveau titre XXIV intitulé « De la procédure applicable aux atteintes aux systèmes de traitement automatisé de données », et pour les seules infractions à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, le législateur insère l'article 706-72 qui énumère les articles de procédure applicables aux atteintes aux systèmes de traitement automatisé de données. Il emprunte la plupart des dispositions prévues pour la lutte contre la criminalité organisée (cyberinfiltration, captation de données, etc.), à l'exception de certaines mesures (pas de garde à vue portée à quatre jours et pas de perquisition de nuit). Ainsi une infraction commise en bande organisée peut être confiée à une juridiction interrégionale spécialisée (JIRS).

### *G. Le cyberterrorisme*

Dès la réforme du code pénal (1992-1994), le législateur est dans une démarche d'anticipation lorsqu'il inscrit les infractions en matière informatique prévues par la loi Godfrain parmi celles dont la finalité permet de recevoir une qualification terroriste[31] (art. 421-1 2°).

[31] Les milieux terroristes (Al Qaeda, Hezbollah, Shebabs, Daech, etc.) tirent parti d'Internet. Ils utilisent les réseaux sociaux pour diffuser la terreur (images de décapitation), pour la propagande, la subversion (notamment par défacement de site), le recrutement, la formation, la transmission d'informations ou d'ordres, les transferts financiers, etc. L'attaque contre le tunnel routier du Mont Carmel (oct. 2013), en

Le terme « cyberterrorisme » est souvent utilisé à tort pour qualifier les cyberattaques. Toutes les cyberattaques ne relèvent pas du cyberterrorisme. Seules peuvent être ainsi qualifiées les atteintes aux systèmes de traitement automatisés de données qui ont pour but de troubler gravement l'ordre public, par l'intimidation ou la terreur. L'objectif poursuivi et les effets produits sont plus déterminants que les voies et moyens utilisés, lesquels peuvent servir d'autres finalités.

### *H. L'irresponsabilité pénale des acteurs de la cyberdéfense*

Les agents des services de l'État déterminés par le Premier ministre ne sont pas pénalement responsables des infractions qu'ils commettent au regard des articles 323-1 à 323-3 du code pénal lorsqu'ils répondent par ce biais à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. Ces mêmes services peuvent détenir des équipements, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du code pénale en vue d'analyser leur conception et d'observer leur fonctionnement. Au moment où le Livre blanc sur la défense et la sécurité nationale reconnaît la légitimité d'une action plus « offensive », ces dispositions (article L. 2321-2 du code de la défense) évitent le risque de poursuites pénales, à condition toutefois qu'elles s'inscrivent dans un contexte de légitime défense.

## II. Les infractions liées aux contenus

Les infractions de contenu sont caractérisées par la détention, l'échange, le transfert, la diffusion, etc. de messages illicites. De telles infractions peuvent être commises en dehors du cyberespace, mais elles bénéficient avec internet d'un exceptionnel vecteur d'amplification. Ainsi une information peut atteindre plusieurs millions d'internautes en quelques secondes, connaître une diffusion exponentielle difficile à maîtriser et s'inscrire dans la durée. Diffamation, atteinte à la dignité humaine, à la vie privée, atteinte à l'image, à l'honneur à la réputation ou à la considération sur un réseau de communications électroniques, pédopornographie, provocation à la violence, au suicide, au terrorisme, à la haine raciale, etc. sont les infractions de contenu les plus fréquentes véhiculées notamment par les réseaux sociaux.

### *A. Les délits réprimés par la loi du 29 juillet 1881 et « commis par tout moyen de communication au public par voie électronique »*

La loi sur la presse réprime la provocation suivie d'effets ou d'une tentative d'une action qualifiée crime ou délit, par « tout moyen de communication au public par voie électronique » (art 23 de la loi du 29 juillet). L'article 24 sanctionne aussi la provocation non suivie d'effets à la discrimination, à la haine, à la violence à l'égard d'une personne ou d'un groupe de personnes :

---

Israël, semble relever d'un acte terroriste contre les SCADA. Pour l'heure, aucune attaque majeure sur les STAD n'a été revendiquée par des mouvements terroristes, ce qui ne préjuge pas de leurs intentions futures.

- à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée ;
- à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.

Le même article vise l'apologie des crimes de guerre, des crimes contre l'humanité, tandis que l'article 24 bis réprime la contestation de crimes contre l'humanité.

Ces infractions peuvent être commises en dehors du cyberespace, mais elles y trouvent une « caisse de résonnance », en raison du nombre d'internautes qui peuvent avoir accès à ce type de contenu illicite.

La provocation aux actes de terrorisme et leur apologie relevaient de la loi sur la presse. La loi du 13 novembre 2014 (art.5) opère leur transfert vers le code pénal, notamment lorsqu'elles sont commises avec un moyen de communication en ligne.

### *B. Les atteintes à la dignité ou à la personnalité*

Certains contenus sont de nature à porter gravement atteinte aux personnes, dans leur intégrité physique ou psychique.

#### *1. Le vidéolynchage ou « happy slapping »*

Cette infraction est liée à la démocratisation des smartphones qui peuvent capter et diffuser des images sur la Toile. Souvent le fait d'adolescents, elle consiste en l'enregistrement et la diffusion d'images de violence prises sur le fait, les violences pouvant être commises en vue de leur diffusion. L'article 222-33-3 punit comme complice des faits l'auteur, sauf si celui-ci exerce une profession ayant pour objet l'information du public ou si l'enregistrement est réalisé pour servir de preuve en justice. La loi du 4 août 2014[32] pour l'égalité réelle entre les femmes et les hommes a ajouté le harcèlement sexuel parmi les faits relevant du « happy slapping ».

#### *2. La cyberintimidation par envoi de messages malveillants et harcèlement moral*

La loi du 4 août 2014 (art. 39) assimile aux appels téléphoniques malveillants les envois réitérés de messages malveillants émis par la voie des communications électroniques. Il s'agit de sanctionner les mails, les SMS, etc. qui ont pour but et pour effet de porter atteinte à l'équilibre psychique d'une personne, à la fois par les propos qu'ils contiennent et par la fréquence des envois. Ce genre d'agression pouvait être sanctionné auparavant, malgré le silence de la loi. Ainsi, dans un arrêt du 30 septembre 2009, la Cour de cassation a reconnu des violences par SMS, car la

[32] Loi n° 2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les hommes.

réception de ceux-ci se manifeste par l'émission d'un signal sonore sur le téléphone portable de leur destinataire... La précision est toujours préférable à l'interprétation.

L'article 41 de la loi ajoute une circonstance aggravante au harcèlement moral, lorsque celui-ci est commis par un service de communication en ligne.

### *C. Les contenus à caractère terroriste*

Internet est devenu le principal vecteur de propagation des appels à la commission d'actes de terrorisme. « Les groupes terroristes maîtrisent parfaitement toutes les potentialités de l'espace numérique, diffusant des messages de propagande généralement bien conçus et incisifs, traduits dans toutes les langues, et s'appuyant sur l'ensemble des volontaires ralliés à travers leurs propres pages ou comptes (Facebook, Twitter) qui démultiplient de manière exponentielle l'appel au ralliement »[33]. En 2013, 122 sites ont fait l'objet d'un signalement pour apologie du terrorisme. La diffusion sur internet, depuis août 2014, de la décapitation de plusieurs otages[34], dont celle, en Algérie, du français Hervé Gourdel, en sont les exemples le plus odieux.

Avec la loi du 13 novembre 2014 (art. 5), la provocation aux actes de terrorisme ou leur apologie ne relèvent plus de la loi du 29 juillet 1881 sur la liberté de la presse (art. 24) mais deviennent des infractions terroristes. Ces infractions sont aggravées lorsqu'elles sont commises à l'aide d'un moyen de communication électronique en ligne[35], ce qui souligne la plus grande nocivité du message transmis par cette voie. Un site internet n'a, dans les faits, qu'un lointain rapport avec celui d'un organe de presse, ce qui montre bien l'inadaptation de la loi de 1881 aux contenus véhiculés par internet.

Ce transfert n'a pas qu'une valeur symbolique puisqu'il a des incidences sur la procédure : prescription de trois ans et non plus d'un an pour les mêmes infractions lorsqu'elles étaient sous le régime de la loi sur la liberté de la presse, possibilité de convocation par procès-verbal ou de comparution immédiate, application du régime procédural dérogatoire prévu par le code de procédure pénale en matière de terrorisme sauf en ce qui concerne le délai de prescription, les perquisitions de nuit et les règles particulières de garde à vue[36].

---

[33] Pietrasanta S., rapport n° 2173 sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, Ass. nat., 22 juil. 2014, p. 14.

[34] Le journaliste américaine James Foley, le britannique Alan Henning ont été les premières victimes de Daech en Syrie.

[35] Le Sénat ne voulait opérer ce transfert que dans le seul cas d'un recours à un moyen de communication électronique en ligne, mais il n'a pas été suivi par la commission paritaire.

[36] L'art. 706-24-1 du code de procédure pénale (créé par l'art. 8 de la loi du 13 nov. 2014) dispose que les art. 706-88 à 706-94 du code de procédure pénale ne sont pas applicables aux délits prévus à l'art. 421-2-5 du même code (de même de l'art. 706-25-1). Le Conseil constitutionnel considère que les techniques spéciales d'enquête ne doivent être mises en œuvre que pour les infractions les plus graves : C. const., n° 2004-492 DC, 2 mars 2004 : « Si le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et 'en rechercher les auteurs, c'est sous réserve que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité, proportionnée à la gravité

La loi concerne la provocation non publique : sont donc visés les prêches dans les lieux non ouverts au public, les réunions privées, les réseaux sociaux accessibles à un nombre restreint de personnes agréées. En revanche, l'apologie « privée » n'est pas réprimée.

La loi du 13 novembre 2014 (art. 7), s'alignant sur le régime des contenus à caractère pornographique, incrimine le fait de fabriquer, de transporter, de diffuser, par quelque moyen que ce soit et quel que soit le support, un message incitant au terrorisme (art. 227-24 du code pénal). S'agissant de contenus à caractère terroriste, cette loi ne crée pas une incrimination semblable à celle en vigueur pour les sites pédopornographiques et qui pénalise directement la consultation habituelle de sites. Mais celle-ci fait partie de la liste des faits matériels qui, avec d'autres, sont les indices constitutifs de l'infraction d'entreprise individuelle terroriste définie par le nouvel article 421-2-6 du code pénal.

### *D. Les contenus à caractère pédophile*

La pédopornographie est, hélas !, la forme la plus courante des infractions de contenu. Elle existait avant internet mais elle avait un caractère local et se limitait à une diffusion « sous le manteau ». Aujourd'hui, ce sont de véritables groupes criminels qui exploitent les penchants les plus sordides de l'individu pour en tirer de confortables bénéfices. Cette délinquance internationale dans sa structuration est d'autant plus difficile à contrer que les sites, hébergés le plus souvent dans des « zones grises », se reconstituent aussi vite qu'ils ont été créés. En France, la loi du 5 mars 2007, relative à la prévention de la délinquance, a durci le dispositif répressif. Le code pénal comprend plusieurs dispositions protectrices relatives à la corruption de mineur (art. 227-22), aux propositions sexuelles à un mineur de quinze ans (art. 227-22-1), à l'exploitation de l'image pornographique d'un mineur (art. 227-23). Enfin, l'article 227-24 réprime la fabrication, diffusion d'un message à caractère pornographique lorsque celui-ci est susceptible d'être vu ou perçu par un mineur.

La consultation habituelle de sites pédophiles a été introduite dans le code pénal par la loi précitée. La réitération est nécessaire (ce qui exclut la consultation par erreur), sauf s'il y a eu accès au site après paiement, l'intention coupable étant alors clairement matérialisée.

### *E. Les mesures de retrait ou de blocages des contenus*

Les contenus à caractère terroriste et pédopornographique peuvent, outre les poursuites pénales, entrainer des mesures de retrait ou de blocage prises par l'autorité judiciaire ou au titre de la police administrative. Ces mesures concernent des acteurs qui ont été définis par la loi pour la confiance dans l'économie numérique : les fournisseurs d'accès, les hébergeurs, les éditeurs. À ces trois acteurs, il convient d'ajouter les moteurs de recherche (par exemple Google) et les annuaires qui

---

et à la complexité des i fractions commises et n'introduisent pas de discrimination injustifiée ». Voir également C. const., n° 2013-679 DC, 4 déc. 2013 et n° 2014-420/421 QPC, 9 oct. 2014.

référencent les sites. Ils peuvent se voir imposer un déréférencement, notamment en application du droit à l'oubli consacré par l'arrêt de la CJUE[37].

*1. L'intervention judiciaire relative à un contenu illicite*

Plusieurs textes de lois permettent à l'autorité judiciaire d'agir face à un contenu illicite. Selon le paragraphe 8 du I de l'article 6 de la loi pour la confiance dans l'économie numérique, l'autorité judiciaire peut prescrire en référé ou sur requête, aux hébergeurs ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ». Le référé au civil s'appuie sur l'article 809 du code de procédure civile (ou 145, si le fournisseur d'accès est étranger).

L'article 50-1 de loi du 29 juillet 1881 relative à la liberté de la presse, créé par la loi du 5 mars 2007 relative à la prévention de la délinquance, dispose que, lorsque certains contenus constituent un trouble manifestement illicite, « l'arrêt du service peut être prononcé par le juge de référés, à la demande du ministère public et de toute personne physique ou morale ayant intérêt à agir ». Du fait du transfert dans le code pénal des infractions de provocation et d'apologie du terrorisme, la loi du 13 novembre 2014 (art. 8) introduit une disposition similaire dans le code de procédure pénale (article 706-23). L'article 50-1 s'applique toujours aux autres contenus illicites. Ainsi le TGI de Toulouse a rendu, le 11 avril 2014, une ordonnance de référé concernant un site à connotation antisémite[38].

Enfin, l'article 61 de la loi du 12 mai 2010, relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne[39], autorise le président de l'ARJEL de saisir en référé le président du tribunal de grande instance de Paris en vue d'ordonner l'arrêt de l'accès à un service de jeux en ligne illicites ainsi que toute mesure destinée à faire cesser le référencement de ces services.

Ces dispositions permettent donc au juge d'intervenir dans des cas définis par la loi (terrorisme, jeux d'argent) mais aussi d'une manière très large pour prévenir ou empêcher un dommage. Mais, considérant que la justice est parfois (trop) lente, le législateur a construit progressivement une police administrative des contenus. C'est sur ce point que les discussions sont les plus vives, cette police administrative étant contestée par ceux qui estiment nécessaire l'intervention du juge judiciaire pour protéger les libertés publiques, au premier rang desquelles figure la liberté d'expression.

*2. La fermeture ou le blocage des sites au titre de la police administrative*

Considérant que le juge judiciaire est le gardien des libertés, certains parlementaires et la plupart des acteurs d'internet (Conseil National du Numérique en

[37] CJUE, Grande chambre, 13 mai 2014.
[38] TGI Toulouse, 11 avr. 2014, n° 14/00525.
[39] Loi n° 2010-476 du 12 mai 2010.

particulier) voudraient lui donner le monopole de toute intervention relative aux contenus eu égard à l'atteinte portée à la liberté d'expression par une mesure de retrait ou de blocage. Ils s'opposent donc au développement d'une police administrative des contenus. Ces opposants se sont fait notamment entendre lors des débats relatifs à la loi du 13 novembre 2014 renforçant les dispositions relatives à la loi sur le terrorisme.

Ils ont parfois gain de cause : la loi sur la confiance dans le commerce électronique (art.18) avait autorisé le blocage des sites relatifs au commerce électronique pouvant porter atteinte au maintien de l'ordre et à la sécurité publics, à la protection des mineurs, à la protection de la santé publique, à la préservation des intérêts de la défense nationale ou à la protection des personnes physiques qui sont des consommateurs ou des investisseurs. Cette disposition a été abrogée par l'article 78 de la loi du 17 mars 2014 relative à la consommation. Les parlementaires ont également imposé au gouvernement (article 77 de la même loi) de remettre, dans un délai de douze mois, un rapport sur les effets et la justification des mesures de blocage légales du contenu d'un service de communication au public en ligne. Ces deux articles témoignent d'une opposition, qui transcende les courants politiques, à toute mesure de filtrage ou de blocage des sites par mesure administrative[40]. Celle-ci s'est notamment exprimée à propos des sites relatifs à la prostitution[41].

Pour autant, la police administrative des contenus conserve un champ d'application s'agissant des contenus à caractère pédophile ou relatifs au terrorisme.

2.1. Les contenus à caractère pédophile. La LOPPSI a complété le paragraphe 7 du I de l'article 6 de la LCEN en disposant que « 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 (fournisseurs d'accès) 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 ».

Ces dispositions sont désormais inscrites à l'article 6-1 de la LCEN. Le Conseil constitutionnel a estimé qu'une telle mesure opérait «une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 »[42]. Mais, faute de décret d'application, le dispositif n'est toujours pas entré en vigueur[43].

---

[40] Elle est notamment incarnée par Laure de la Raudière (UMP) et par Corinne Ehrel (PS).

[41] Le blocage des sites relatifs au proxénétisme, initialement prévu dans la loi renforçant la lutte contre le système prostitutionnel (art.1er), a été abandonné sur amendement du gouvernement et d'un député.

[42] C. const., n° 2011-625 DC, 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure.*

[43] Le gouvernement annonce un décret commun avec les dispositions concernant la provocation ou l'apologie du terrorisme.

On notera que le blocage des sites internet illégaux n'est pas une spécificité française. Il est prévu par la directive européenne du 4 novembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants[44].

2.2. Les contenus à caractère terroriste. Parmi les principales mesures de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, l'article 12 est celui qui suscite le plus de critiques. Il modifie, en effet, l'article 6 de la loi sur la confiance dans l'économie numérique en transférant dans un nouvel article 6-1 les modalités qui s'appliquent au retrait des contenus provoquant au terrorisme ou faisant leur apologie et au blocage administratif des sites qui y donnent accès. La procédure est identique à celle prévue pour les sites pédopornographiques (v. *supra*).

L'autorité administrative applique un principe de subsidiarité : elle s'adresse d'abord aux éditeurs et hébergeurs afin qu'ils retirent les contenus dans un délai de 24 heures. En cas d'échec, ou directement si l'éditeur ou l'hébergeur ne peuvent être identifiés, les fournisseurs d'accès sont invités à bloquer l'accès au(x) site(s) incriminé(s). Cette procédure, identique à celle prévue pour la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal fait l'objet d'un contrôle par une personne qualifiée, désignée par la CNIL en son sein, puis, le cas échéant, par le juge administratif. On notera la possibilité donnée à l'autorité administrative de s'adresser directement aux moteurs de recherche ou aux annuaires pour qu'ils cessent de référencer les sites illicites. Cette dernière mesure est déjà appliquée en vertu de l'article 61 la loi du 12 mai 2010, relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne. Mais dans ce cas, l'intervention du juge judiciaire est nécessaire.

### 3. *Un débat révélateur de clivages qui transcendent les courants politiques*

Deux questions sont soulevées : peut-on bloquer ou retirer des contenus sans porter atteinte à la liberté d'expression ? Dans l'affirmative, quel est le juge compétent ?

S'agissant des aspects juridiques, les opposants considèrent que le retrait ou le blocage est une atteinte telle à la liberté d'expression que celle-ci requiert l'intervention du juge judiciaire. La Commission de réflexion sur le droit et les libertés à l'âge du numérique[45] estime, dans sa recommandation de juillet 2014, que

[44] Les États membres prennent les mesures nécessaires pour faire rapidement supprimer les pages internet contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire et s'efforcent d'obtenir la suppression des pages hébergées en dehors de celui-ci. Les États membres peuvent prendre des mesures pour bloquer l'accès par les internautes sur leur territoire aux pages internet contenant ou diffusant de la pédopornographie. Ces mesures doivent être établies par le biais de procédures transparentes et fournir des garanties suffisantes, en particulier pour veiller à ce que les restrictions soient limitées à ce qui est strictement nécessaire et proportionné et que les utilisateurs soient informés de la raison de ces restrictions. Ces garanties incluent aussi la possibilité d'un recours judiciaire » (art.25).

[45] Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, coprésidée par le député (PS) Christian Paul et l'avocate Christiane Féral-Schuhl et composée de 13 députés et de 13 personnalités qualifiées.

« le préalable d'une décision judiciaire apparaît comme un principe essentiel, lorsqu'est envisagé le blocage de l'accès à des contenus illicites sur des réseaux numériques ». Le Conseil National du Numérique, dans son avis rendu le 15 juillet 2014[46], n'a pas de position différente : sans s'opposer au blocage ou au filtrage de contenus quand ils sont illicites, il préconise en de pareils cas de ne jamais déroger au principe du recours à une autorité judiciaire préalablement à l'instauration d'un dispositif de surveillance, de filtrage ou de blocage des contenus sur internet. Le rapport de Marc Robert est plus partagé : il recommande que la décision de blocage d'un site vienne du juge judiciaire saisi par l'administration (juge civil ou juge des libertés et de la détention), compte tenu des effets sur les libertés individuelles, mais qu'une exception doit être faite pour la pédopornographie, cette infraction étant avérée par nature et le dispositif de blocage administratif sans intervention judiciaire ayant été validé par le Conseil constitutionnel.

Du point de vue de l'efficacité, selon les détracteurs du texte, de nombreux sites incriminés (90 à 95 %) sont hébergés au Canada ou aux États-Unis, ce qui rend la procédure de retrait quasi inopérante. 80 % des contenus illicites sont véhiculés par Facebook, Twitter ou Youtube. Les blocages par inspections de contenus (Deep Packet Inspection- DPI) sont attentatoires aux libertés car ils consistent à inspecter l'ensemble des échanges. Les blocages par adresse IP, par nom de domaine ou URL sont les plus aisés à mettre en place mais ils conduisent à des « surblocages » ou sont inefficaces, car contournables. L'abonnement à un réseau virtuel privé (VPN), qui permet de surfer sur internet à partir du pays de son choix, permet, en effet, de ne pas subir un blocage limité aux internautes français. Le logiciel TOR (The Onion Router) offre également une solution qui garantit l'anonymat. L'efficacité du dispositif de blocage serait donc très réduite. Le recours au cryptage par les terroristes viendrait compliquer la tâche des services spécialisés. « On ne coupe pas le téléphone de celui que l'on veut écouter », selon certains de leurs membres qui craignent une perte d'efficacité des enquêtes sur les milieux terroristes. Ainsi le juge anti-terroriste, Marc Trévidic considère que « toutes les personnes arrêtées depuis 2007 l'ont été grâce aux imprudences commises sur internet, à la communication électronique. Si nous les empêchons de surfer, nous aurons plus de mal à détecter leurs agissements. Les sites pratiquant le prosélytisme peuvent toucher un large public, on peut donc souhaiter limiter cette propagande. Cependant la part la plus dangereuse de leurs activités se déroule sur messageries privées et c'est parce que nous visitons ces dernières que nous savons ce qui se passe »[47].

Le gouvernement et ceux qui le soutiennent ne sous-estiment pas l'efficacité limitée du blocage des sites, mais ils considèrent qu'il n'est pas acceptable dans une société libre et démocratique que des contenus mettent en scène des personnes décapitées, violées, crucifiées. Maître Jakubowicz, président de la LICRA, vient en renfort : « les fournisseurs d'accès doivent sortir d'une certaine hypocrisie et épauler les

[46] Avis n° 2014-3 du 15 juil. 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

[47] Marc Trévidic, juge anti-terroriste, audition devant la commission sénatoriale sur le contrôle et l'évaluation des dispositifs législatifs relatifs à la sécurité intérieure et à la lutte contre le terrorisme. Octobre 2012.

avancées permettant de lutter contre les atteintes à la dignité, voire à la vie humaine »[48].

Le retrait et le blocage, certes contournables par les plus experts, doivent prévenir l'accès involontaire du plus grand nombre. Le blocage, jugé attentatoire à la liberté d'expression n'est que l'ultime recours, le retrait étant la règle qui témoigne de l'esprit de responsabilité des hébergeurs.

Sur le recours à une procédure de police administrative, le rapporteur de la loi à l'Assemblée nationale, Sébastien Pietrasanta, considère que « ce que l'autorité administrative peut faire dans la sphère réelle pour protéger l'ordre public, elle doit également pouvoir le faire dans la sphère numérique »[49]. Bernard Cazeneuve renchérit : « si des appels se produisaient sur un autre espace public, un autre espace de liberté, et non sur la Toile, l'espace numérique, je suis convaincu que tous ceux qui siègent dans l'hémicycle me demanderaient les raisons pour lesquelles je ne fais pas cesser le trouble à l'ordre public, et ils auraient toute légitimité à la faire. Mais dès lors qu'il s'agirait d'internet, il ne serait plus possible de procéder ainsi parce que la prévention du risque et la mesure de police en vue de rétablir ou d'assurer l'ordre public serait liberticides ! »[50].

Quand à l'intervention du juge judiciaire, par préférence au juge administratif, Jean-Jacques Hyest, rapporteur de la loi au Sénat, déclare : « certains voudraient que la justice judiciaire s'occupe de tout. Mais le rôle de la justice judiciaire, c'est de réprimer ! Et si l'on commence à tout mélanger, à faire intervenir le juge judiciaires dans les affaires de police administrative, on détruira en partie un édifice auquel beaucoup d'entre nous sont attachés »[51].

Pour éclairer le débat, on peut émettre deux observations : si l'infraction est constituée, rien n'empêche le juge judiciaire de se saisir et de procéder lui-même aux démarches aboutissant au retrait ou au blocage. La crainte de sa lenteur semble motiver le choix du législateur. Il appartient donc au juge judiciaire de faire preuve de réactivité. S'agissant de la technique du blocage, comme le souligne le rapport de Marc Robert, « elle n'est pas la panacée -mais celle-ci n'existe que rarement dans le domaine de la lutte contre la cybercriminalité- elle constitue un outil, parmi d'autres, dont on aurait tort de se priver à condition de le cantonner strictement ».

Faute d'une saisine directe du Conseil constitutionnel, l'Association des services internet communautaires (ASIC[52]) espère que le Conseil d'État fera usage de Questions prioritaires de constitutionnalité lors de l'examen des décrets d'application[53]. Mais la Haute juridiction appréciera sans doute assez peu de n'être pas

[48] AFP, 10 juil. 2014 (à propos du projet de loi relatif au terrorisme).
[49] Débats à l'Assemblée nationale, séance du 15 sept. 2014.
[50] Sénat, séance du 15 oct. 2014.
[51] Hyest J.-J., Sénat, séance du 15 oct. 2014.
[52] L'ASIC regroupe notamment Google, Facebook, Microsoft, eBay, Yahoo ! Dailymotion, Deezer, Spotify, Airbnb, AOL, Skyrock, PriceMinister, Skype.
[53] Le Conseil constitutionnel a rappelé que le blocage d'un site internet constitue une atteinte grave à la liberté d'expression et de communication, tout en déclarant conforme à la Constitution le blocage des sites pédophiles, n° 2011-625 DC, 10 mars 2011.

considérée comme garante des libertés publiques, elle qui a su montrer par sa jurisprudence qu'elle pouvait prendre des positions courageuses[54].

Le cyberespace, contrairement à la terre, à la mer et à l'espace aérien, est entièrement construit par l'homme. Celui-ci porte donc l'entière responsabilité de son développement. Entre une liberté sans limite et une sécurité absolue, le droit qui le régit doit respecter un juste équilibre. La lutte contre la cybercriminalité doit être réactive pour ne pas laisser émerger un non-droit préjudiciable au plus faible. Mais elle doit aussi prendre le recul nécessaire pour éviter la tentation de la surveillance généralisée. « Depuis dix ans, de nombreuses lois comportent des dispositions numériques. Mais nous ne pouvons pas nous satisfaire de cette législation peinte par petites touches, parfois discordantes ». En s'exprimant ainsi, début octobre 2014, lors du lancement de la concertation nationale en vue de la loi sur le numérique, le Premier ministre souligne la nécessité d'avoir une vision d'ensemble sur une transformation numérique de la société porteuse du meilleur comme du pire.

[54] On pense en particulier à l'arrêt Canal (1962).