RAPPORT

CODE PENAL ET LUTTE CONTRE LA CYBERCRIMINALITE :

PROPOSITIONS POUR UNE EFFICACITE JURIDIQUE RENFORCEE

25 janvier 2017

Cyberlex
Association loi 1901
https://www.cyberlex.org/

Centre expert contre la cybercriminalité français
Association loi 1901
https://www.cecyf.fr/

CODE PENAL ET LUTTE CONTRE LA CYBERCRIMINALITE :

PROPOSITIONS POUR UNE EFFICACITE JURIDIQUE RENFORCEE

La présente contribution est le fruit de la réflexion collective de membres de l'association Cyberlex, Association du droit et des nouvelles technologies, et du CECyF, Centre Expert contre la Cybercriminalité Français, lancée à l'initiative d'Éric FREYSSINET et de Corinne THIERACHE afin de concrétiser le partenariat avec la complémentarité des compétences de ces deux organisations, inauguré en juin 2014.

PRESENTATION DE CYBERLEX

Cyberlex réunit, depuis 1996, des juristes d'entreprise, des avocats, des professeurs de droit, des magistrats ainsi que des professionnels du marché d'Internet et des technologies numériques.

Cyberlex ne représente pas une opinion mais des opinions, à l'image de la diversité de ses membres, excluant tout lobbying. L'ambition de Cyberlex est de contribuer à mieux comprendre le monde des nouvelles technologies et l'évolution des usages, appréhender les différents aspects du droit et ainsi participer à sa meilleure lisibilité.

PRESENTATION DU CECYF

Le CECyF est une association créée en 2014 regroupant des services de l'Etat chargés de la lutte contre la cybercriminalité, des établissements d'enseignement et de recherche ainsi que des entreprises de toutes tailles.

Ils ont réuni leurs forces pour mener des actions de prévention, de formation et de recherche et développement contre la cybercriminalité. Le CECyF est le résultat du projet européen 2CENTRE qui vise à développer un réseau de telles initiatives à travers l'Europe. L'association est aussi membre du projet européen SENTER qui perpétue 2CENTRE et de l'association européenne ECTEG de développement de formations contre la cybercriminalité.

METHODOLOGIE ADOPTEE

Un groupe de travail composé de membres de Cyberlex et du CECyF, disposant de compétences juridiques et techniques nécessaires à la compréhension des enjeux sociétaux, juridiques et économiques de la cybercriminalité, a donc été mis en place sous la direction de Corinne THIERACHE, Ancienne présidente et membre de Cyberlex, et d'Eric FREYSSINET, Secrétaire général du CECyF, afin de coordonner les différents travaux (ci-après le Groupe de travail Cyberlex - CECyF.

Les réflexions qui ont alimenté ces travaux et les recommandations qui en ont découlé reprises dans le présent rapport sont proposées par les membres du Groupe de travail Cyberlex – CECyF en

toute indépendance et n'engagent que ces derniers. Elles ne sauraient donc engager leurs employeurs.

Plusieurs réunions mensuelles de réflexion ont été tenues par le Groupe de travail Cyberlex – CECyF entre juillet et décembre 2016, ainsi composé (dans l'ordre alphabétique) :

Membres de Cyberlex contributeurs :

- Carole BUI, Avocat
- Matthieu CAMUS, Expert sécurité des données et vie privée
- Fabrice MATTATIA, Ingénieur et docteur en droit
- Myriam QUEMENER, Magistrat, docteur en droit
- Corinne THIÉRACHE, Avocat associé

Membres du CECyF contributeurs :

- Philippe BAUDOIN, Officier de gendarmerie
- Éric FREYSSINET, Officier de gendarmerie (également membre de Cyberlex)
- Catherine HORNAIN, Inspectrice de la concurrence, de la consommation et de la répression des fraudes
- Alexandre HUGLA, Juriste
- Marc WATIN-AUGOUARD, Général d'armée de gendarmerie (2S)

Sont vivement remerciés Benjamin AMAUDRIC DU CHAFFAUT, Jean-Christophe LE TOQUIN, ainsi que Jean-Sébastien MARIEZ, pour leur soutien au présent rapport.

L'objectif poursuivi par Le Groupe de travail Cyberlex – CECyF a été établi à échéance suffisamment courte afin d'éviter de devoir réactualiser de manière permanente sess analyses et recommandations.

POURQUOI UN NOUVEAU RAPPORT SUR LA CYBERCRIMINALITE ?

Le Code pénal a été modifié au coup par coup, au fil des lois comportant des dispositions pénales ayant trait aux technologies de l'information et de la communication et en particulier suite aux attentats terroristes et à l'émergence de nouveaux comportements facilités par le numérique. Il est particulièrement difficile de corriger la lettre du Code pénal. Aussi, le présent rapport ne sera pas uniquement dédié à une élite juridique ou à des spécialistes du numérique. Il est destiné en toute modestie à apporter un nouvel éclairage et être source de propositions d'aménagement du code pénal. Il vise à une meilleure lisibilité du texte légal, notamment en unifiant les termes [1]après identification des problèmes de définition[2] et de redondances) ; condition essentielle pour mieux appréhender la lutte contre la cybercriminalité.

[1] Annexe **1** – Subtilités sémantiques
[2] Annexe **2** – Pour une définition clarifiée de la terminologie

En outre, le rapport contient des propositions afin d'harmoniser le quantum des peines au regard de la gravité des infractions relatives à la cybercriminalité.

En revanche, le présent rapport ne traite pas de la procédure pénale qui pourra faire l'objet ultérieurement d'un autre rapport.

OBJECTIFS POURSUIVIS PAR CYBERLEX ET LE CECYF

L'inflation des textes concernant la cybercriminalité[3], leur complexité, accompagnée de leur superposition ou juxtaposition voire contradiction ainsi que la multiplication des autorités peuvent avoir pour conséquence de rendre délicate l'appréhension juridique des situations rencontrées dans le monde du numérique.

Pourtant, les acteurs économiques avec l'assistance de leurs conseils (juristes internes, avocats) doivent traduire en droit les faits auxquels ils sont confrontés pour déterminer la réglementation applicable et s'y conformer. Les services d'enquête élaborent des procédures en proposant des qualifications puis les magistrats ont pour missions de caractériser ou non des infractions et de retenir la qualification adaptée. Souvent ces infractions sont complexes en raison des aspects techniques de leurs modes opératoires, et une politique efficace de lutte contre la cybercriminalité passe par l'application effective des textes légaux.

Cette situation est accentuée par l'évolution constante des technologies qui, en quelques années, a profondément transformé les habitudes et les usages des internautes et ouvert une multitude de possibilités de développements. Cette même situation offre aussi un nouveau terrain de jeux particulièrement attractif pour les cybercriminels qui exploitent toutes failles ou faiblesses, à la fois techniques ou juridiques, animés par un sentiment réel d'impunité face à des infractions aux effets les plus souvent dématérialisés. Il existe ainsi un écart important entre la simplicité de la commission des infractions et la gravité de leurs effets et des préjudices qu'elles causent.

La cybercriminalité n'est donc pas une criminalité comme les autres, elle est protéiforme, à l'image des cyber-délinquants dont les profils sont diversifiés et complexes.

Les décisions de justice rendues dans le domaine de la cybercriminalité illustrent les difficultés rencontrées pour qualifier la nature des faits, rattacher leur auteur à des catégories préexistantes, et ainsi déterminer l'infraction applicable, selon les principes d'interprétation stricte et de non rétroactivité de la loi pénale.

Or, il s'agit d'un point majeur. Des qualifications retenues des faits découle, en effet, l'infraction pénale qui leur sera applicable. Il apparaît alors souvent salutaire de se reposer sur des concepts juridiques classiques qui animent le droit positif français depuis des décennies, avant même l'apparition de l'économie numérique, pour raisonner et tenter de qualifier les faits de façon pertinente.

Toutefois, le recours à des infractions classiques peut apparaître par trop artificiel voire inadapté dans certaines situations offertes par les technologies du numérique. Face à la croissance des cyberattaques et aux menaces que constituent notamment le terrorisme et la criminalité organisée, le législateur est ainsi récemment intervenu à plusieurs reprises pour compléter l'arsenal juridique en matière pénale pour mieux appréhender et punir des actes liés à la cybercriminalité[4].

[3] Annexe **3** – Un droit « millefeuilles »

[4] De manière non exhaustive :

Cette méthode d'adaptation réalisée de façon ponctuelle du droit aux faits n'est pas sans inconvénient, créant ainsi un éparpillement dans différents Codes (notamment Code pénal, Code des postes et des communications électroniques, Code de la sécurité intérieure, Code de la défense…), une superposition de textes (« effet mille-feuilles »)[5] et, enfin, un risque d'obsolescence des dispositions pénales par ailleurs parfois sous utilisées par les praticiens du droit.

Ainsi, ce rapport propose d'œuvrer afin que la loi soit plus lisible tant pour les praticiens que pour les justiciables et contribuer à une plus grande sécurité juridique dans l'application des textes. Dans cette perspective, le Groupe de travail Cyberlex – CECyF s'est attaché modestement à relever les éventuelles scories, les redondances des textes et faire le cas échéant des propositions pertinentes afin d'aider le législateur à y voir plus clair et participer ainsi à une meilleure cohérence des textes dans le cadre d'une réforme plus globale de la politique pénale.

EN RESUME, il s'agit ici de contribuer à la clarification de la réglementation applicable à la lutte contre la cybercriminalité. Il ne s'agit pas de faire des modifications massives des dispositions du Code pénal mais plutôt une relecture permettant de relever des lacunes ou des incohérences. Le but est de proposer des pistes de réflexion au législateur pour des évolutions futures y compris ouvrant si nécessaire sur une approche plus globale du droit pénal appréhendé par d'autres codes que le Code pénal. En tout état de cause, l'objectif est d'expliquer le dispositif actuel pour le rendre plus lisible et éventuellement faire des propositions de modification pour finalement constater dans la conclusion de ce rapport que l'essentiel, pour une lutte efficace contre la cybercriminalité, se situe en réalité dans les règles de procédure pénale et dans les ressources qui y sont affectées.

- loi du 15 novembre 2001 relative à la sécurité quotidienne (comportant notamment des dispositions relatives à la lutte contre le terrorisme),
- loi du 18 mars 2003 pour la sécurité intérieure (comportant notamment des dispositions sur la coopération de FAI avec les officiers de police judiciaire),
- loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité,
- loi pour la confiance dans l'économie numérique,
- loi du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle,
- loi du 23 janvier 2006 relative à la lutte contre le terrorisme,
- loi du 5 mars 2007 relative à la prévention de la délinquance,
- lois LOPPSI 1 du 29 août 2002 et LOPPSI 2 du 14 mars 2011,
- loi sur la lutte contre la cybercriminalité du 17 juillet 2014,
- loi du 13 novembre 2014 renforçant la lutte contre le terrorisme,
- loi pour république numérique du 7 octobre 2016.

[5] Annexe 3 – Un droit « mille-feuilles »

TABLE DES MATIERES

1 LES MULTIPLES DEBATS AUTOUR DES INFRACTIONS D'ATTEINTE AUX SYSTEMES DE TRAITEMENT AUTOMATISE DE DONNEES (STAD)

1.1 LE « VOL DE DONNEES »

Peut-on voler une donnée ? Telle est la question à laquelle la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme[6] voulait répondre en modifiant l'article 323-3 du Code pénal.

La réponse est-elle satisfaisante ou faut-il préciser davantage le texte qui en résulte ?

1.1.1 Peut-on voler une donnée ?

C'est une question tout à fait légitime eu égard au sens courant donné au terme « vol » qui est défini comme « *le fait de s'emparer du bien d'autrui par la force ou à son insu* » et « *l'action qui consiste à soustraire frauduleusement le bien d'autrui* »[7].

En l'espèce, ne sera pas ici évoqué le vol d'un support (clé USB, disque dur, etc.) qui répond à la qualification classique du vol[8]. Seul est envisagé le « vol » de données, le support n'étant pas l'objet de l'action du prédateur. Dans cette hypothèse, on confond souvent la soustraction de la donnée qui échappe ainsi à la *« volonté du maître du système »* et la copie de données, malgré la *« volonté du maître du système ».*

C'est bien la copie qu'évoquait M. Sébastien Pietrasanta, rapporteur de la loi précitée du 13 novembre 2014, en affirmant, lors des débats, que :

> *« L'article 331-1 du code pénal définissant le vol comme la soustraction frauduleuse de la chose d'autrui pose deux conditions qui s'avèrent inadaptées au vol de données : d'une part, une donnée n'est pas une chose, mais un élément immatériel distinct de tout support de stockage ; d'autre part, une donnée extraite d'un STAD à la suite d'un accès ou d'un maintien frauduleux n'est pas nécessairement soustraite de celui-ci mais seulement extraite par sa reproduction sur un autre support*[9] *».*

Pour le vol d'énergie, bien immatériel, le législateur a dû recourir à une incrimination spécifique (article 311-2 du Code pénal).

La copie de données n'est pas, en effet, une soustraction, puisque le légitime propriétaire les conserve et n'en est à aucun moment dépossédé. En ce qui concerne les données à caractère personnel, les constituants de la propriété (usus-abusus-fructus) sont aussi inadaptés : peut-on parler de propriété sur ces données, puisque, tout en étant éventuellement exploitées commercialement, elles ne peuvent faire

6 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id

7 Définition donnée par le dictionnaire LE PETIT ROBERT

8 L'article 311-1 du Code pénal qualifie le vol comme « la soustraction frauduleuse de la chose d'autrui ».

9 Rapport n°2173 CL. AN, 22 juillet 2014, M. Pietrasanta rapporteur.

l'objet d'un abandon de la part de leur détenteur[10] ? Pour éviter cet écueil, plusieurs voies étaient possibles avant la loi : accès ou maintien frauduleux à un STAD, poursuites pour atteintes aux droits du producteur de bases de données, pour abus de confiance[11], pour collecte déloyale ou frauduleuse de données personnelles etc. Mais elles ne couvraient pas toutes les hypothèses.

La jurisprudence a tenté de remédier à cette difficulté en reconnaissant le vol de données :

- Dans un arrêt du 4 mars 2008[12], la Cour de cassation avait déjà qualifié de vol une copie de données, mais cette décision s'écartait du principe selon lequel la loi pénale est d'interprétation stricte.

- Plus récemment, par un arrêt du 20 mai 2015 (postérieur à la loi du 13 novembre 2014 mais pour des faits qui lui sont antérieurs), la chambre criminelle de la Cour de cassation a confirmé l'arrêt du 5 février 2014 de la Cour d'appel de Paris en considérant que le vol était bien constitué. En l'espèce, la Cour d'appel avait condamné pour vol de données (7,7 giga-octets) un bloggeur qui s'était introduit dans le site extranet de l'ANSES. A cette occasion, il a téléchargé des données qu'il a fixées sur plusieurs supports et partiellement publiées pour un article sur la légionellose, sans l'autorisation de l'Agence. En première instance, le Tribunal correctionnel de Créteil avait considéré que, l'ANSES n'ayant jamais été dépossédée de fichiers qui sont restés accessibles et disponibles sur son site, il n'y a pas eu, selon le tribunal, de soustraction de données et donc de vol. Dans ses conclusions, l'avocat général Frédéric Desportes s'est ainsi exprimé[13] :

  « Tout en respectant le principe d'interprétation stricte de la loi pénale, vous avez toujours su adapter les incriminations aux évolutions technologiques, veillant à ce que soient atteints les objectifs du législateur et donc à ce que la loi soit appliquée

---

10 Nicolas Ochoa, *« Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement la principe de libre disposition», RFDA* 2015, p.1157. Voir également Fabrice Mattatia et Morgane Yaïche, « Etre propriétaire de ses données personnelles ? », 1ère partie « Peut-on recourir aux régimes traditionnels de propriété », RLDI, avril 2015 ; 2e partie « Peut-on envisager un régime spécifique ? », RLDI, juin 2016.

11 Cass.crim, n°13-82630 du 22 octobre 2014. « *Le prévenu ayant, en connaissance de cause, détourné en les dupliquant, pour son usage personnel, au préjudice de son employeur, des fichiers informatiques contenant des informations confidentielles et mis à sa disposition pour un usage professionnel, la cour d'appel, qui a caractérisé en tous ses éléments, tant matériel qu'intentionnel, le délit d'abus de confiance, a justifié sa décision*».

Alors qu'il rejoint une société concurrente, un salarié démissionnaire d'un **cabinet de courtage d'assurances** s'adresse en 54 messages, via sa messagerie personnelle, 305 fichiers informatisés. A **la suite du contrôle interne, u**ne perquisition à son domicile permet de découvrir 13 clés USB portant la dénomination de son ancien employeur et refermant 9824 fichiers et documents de la société. Pour se justifier, il prétend que c'est pour son fonds documentaire personnel et pour travailler à son domicile. Il avait signé le 22 mai 2003 une « *charte pour l'utilisation des ressources informatiques et des services Internet »* lui rappelant l'interdiction d'extraire ces données ou de les reproduire sur d'autres supports informatiques sans l'accord préalable d'un responsable de service et de les détourner enfin de leur utilisation normale à des fins personnelles. La Cour de cassation qualifiant de **« biens » des données informatiques, confirme l'arrêt de la cour d'appel de Bordeaux qui avait condamné le prévenu pour abus de confiance (art. 314-1 du Code pénal), car les fichiers informatiques ne lui avaient été remis qu'à charge d'en faire un usage déterminé, conforme à la charte informatique interne proscrivant l'extraction de ces documents de l'entreprise.**

12 Cass.crim., n°07-84.002, 4 mars 2008, X/ Société Graphibus non publié.

13 Avis non publié.

> *conformément à la fois à sa lettre et à son esprit. Cela est particulièrement vrai s'agissant du vol dont la définition a révélé une certaine plasticité. […]* ***Il serait paradoxal que la soustraction frauduleuse d'un document papier sans intérêt soit passible de trois ans d'emprisonnement mais non celle de milliers de fichiers stratégiques alors même que ces fichiers ne sont jamais que des documents numériques ou numérisés pouvant être imprimés et donc matérialisés*** *».*

1.1.2 L'extraction (avec et sans copie des données) sanctionnée

Pour éviter les difficultés liées à la définition même du vol, le Parlement a décidé, à l'occasion de l'examen de la loi du 13 novembre 2014, de modifier l'article 323-3 du Code pénal. Celui-ci, sans jamais évoquer le « vol » (ni le recel), réprime désormais **l'extraction**, **la détention**, **la reproduction**, **la transmission frauduleuses de données contenues dans le système**.

La notion d' « extraction » de données apparaît dans l'article 2 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés qui qualifie de traitement de données à caractère personnel comme étant *: « 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. »*

Il est possible de s'interroger sur le fait de savoir si le terme *« extraction »* permet de sanctionner la copie de données qui demeurent à la disposition du « maître du système ». Les définitions ou les usages du mot « extraction »[14] impliquent généralement en effet un transfert, un changement de lieu (extraction d'un détenu, d'une dent, d'un minerai, extrait d'un texte ou d'un reportage etc.).

Le transfert est ainsi bien défini juridiquement par l'article L.342-1 du Code de la propriété intellectuelle[15] qui dispose que le producteur d'une base de données a le droit d'interdire :

> *« 1° L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;*
>
> *2° La réutilisation, par la mise à disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme. »*

Toutefois, cette première interprétation est contredite par la pratique. En effet, certes, la copie de ces données est hors du contrôle du « maître du système », mais les données sources, quant à elles,

---

[14] Le dictionnaire LE PETIT ROBERT définit l'extraction comme *« l'action d'extraire, de retirer (une chose) d'un lieu où elle se trouve enfouie ou enfoncée».*
Datamining : le fait d'extraire des informations à partir de fichiers afin de transformer ces données en une structure compréhensible.
ETL (extract, transform, load) : transférer des données d'un système source et les envoyer vers une base de données

[15] Venant en application de l'art .7 de la directive n°96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données (JOCE 27 mars, n°L77).

demeurent au sein dudit système. Par ailleurs, le terme « reproduire » tel que visé dorénavant à l'article 323-3 du Code pénal permet à notre sens de couvrir les actes de copie. C'est d'ailleurs bien ce même terme qui est utilisé par le législateur pour adapter certaines dispositions au numérique. Tel est le cas par exemple de l'apologie publique des actes de terrorisme ou leur provocation telles que réprimées par l'article 421-2-5-1 du Code pénal.

RECOMMANDATION N°1 – Le statu quo en matière de vol de données

Au regard de ce qui précède, les actuelles dispositions de l'article 323-3 du Code pénal semblent suffisantes pour couvrir l'ensemble des comportements délictueux en la matière connus à ce jour, sous réserve bien entendu de l'absence d'interprétation restrictive des tribunaux.

1.2 LES ACTIONS BIENVEILLANTES ASSOCIEES AUX INFRACTIONS D'ATTEINTES AUX SYSTEMES DE TRAITEMENT AUTOMATISE DE DONNEES (STAD)

Aux côtés de l'offre régalienne proposée par les institutions et de la stratégie de cybersécurité menée par des acteurs privés de la sécurité des systèmes d'information se sont glissés les « hackers éthiques », ou « éthico-hackers » et « hackers blancs » internautes agissant généralement seuls. Contribuant de manière collaborative et originale à la sécurité des systèmes en détectant les failles, la question de leur statut au regard de la loi pénale se pose.

Il convient donc de s'interroger sur le fait de savoir si la réponse récente du législateur pour encadrer l'action d'une certaine catégorie de hackers est satisfaisante.

On peut d'ores et déjà écarter le cas des hackers agissant dans le cadre d'un contrat de « bug bounty ». En effet, ils sont sollicités par des entreprises pour détecter des failles dans la sécurisation de leurs systèmes ou de leurs produits. Ils sont recrutés (inside) ou agissent par contrat (outside) pour effectuer des tests d'intrusion, « entraîner » le personnel des SOC (Security Operation Center), effectuer des audits de sites, de produits. Dès lors que le contrat délimite clairement dans le temps et dans l'espace le périmètre des investigations permises sur l'infrastructure, les sites ou les logiciels tout en excluant toute altération du système et toute destruction de données, le cocontractant agit dans les limites autorisées par l'entreprise pour découvrir ses propres failles et formuler des recommandations.

Ainsi, si le contrat de « bug bounty » offre un cadre juridique clair, il n'en est pas de même du lanceur d'alerte.

D'après le Conseil d'État[16], les lanceurs d'alerte seraient des personnes qui « *signalent, de bonne foi, librement et dans l'intérêt général, de l'intérieur d'une organisation ou de l'extérieur, des manquements graves à la loi ou des risques graves menaçant des intérêts publics ou privés, dont ils ne sont pas l'auteur* ». Ainsi, selon cette définition, le lanceur d'alerte au regard du Code pénal n'est

[16] Etude « Le droit d'alerte : signaler, traiter, protéger » adoptée le 25 février 2016 par l'assemblée générale plénière du Conseil d'Etat, La documentation française, p.11

pas l'auteur des faits qu'il dénonce ou signale. Il leur est extérieur. Le lanceur d'alerte ne participe pas à un ou plusieurs actes matériels de l'infraction, sinon il serait auteur, coauteur ou complice.

Sont donc clairement exclus les chasseurs de prime.

Le lanceur d'alerte peut également saisir l'opinion publique quand il a échoué en tant que déontologue de l'entreprise ou de l'administration, voire de son supérieur hiérarchique, et que les autorités régaliennes ne prennent pas sérieusement en considération les manquements dénoncés.

Pour les agents publics qui se retrouveraient dans cette situation, l'article 40 du Code de procédure pénale les oblige à porter à la connaissance du Procureur de la République les faits susceptibles de constituer un crime ou un délit.

Outre les hackers contractuels et lanceurs d'alerte, existent les « hackers autonomes » qui occupent une toute autre place au regard du Code pénal.

Ces hackers sont autonomes dans la mesure où ils agissent sans concertation avec le « maître du système ». Ils testent les systèmes et, pour ce faire, y pénètrent ou s'y maintiennent le plus souvent sans droit ni titre. Ils commettent donc des actes matériels qui entrent dans la définition des infractions à la loi Godfrain.

Après avoir envisagé, dans le cadre des différents débats parlementaires autour de l'adoption de la loi « Sapin II » et la loi pour une République numérique, une exemption de peine en cas d'avertissement immédiat, par le hacker autonome mais de bonne foi, de l'autorité administrative, judiciaire ou du responsable de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système en évitant ainsi toute atteinte ultérieure aux données, le législateur a préféré se diriger vers une autre solution.

Désormais, après adoption de la loi 2016-1691 du 9 décembre 2016 dite Loi Sapin II, la définition donnée à l'article 6 du lanceur d'alerte est la suivante :

> *« Un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.*
>
> *Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre. »*

Dans un but de protection du lanceur d'alerte, il ne fallait pas provoquer un risque de confusion avec le « statut » de repenti dans le « monde réel » (cf. la loi « Perben II » du 9 mars 2004[17] qui avait pour objectif d'empêcher la concrétisation d'une menace imminente et non un risque potentiel, ou de limiter les effets d'une infraction consommée). Or une faille dans un logiciel est un risque et non une menace, tant qu'une personne mal intentionnée ne l'a pas exploitée. L'amendement qui a été proposé en ce sens

[17] Article². 132-78 du Code pénal

au cours des débats parlementaires aurait remis en cause l'équilibre de l'article 323-1 du Code pénal et l'aurait même fortement affaibli.

La solution récemment retenue peut donc paraître d'un prime abord raisonnable et plus sage, car sans risque de déstabiliser les principes fondamentaux des règles pénales et d'entraîner des confusions ou des mélanges de genre. Mais il apparaît qu'elle ne résout pas complètement le problème.

Est désormais instaurée, à la suite de l'adoption de l'article 47 de la loi pour une République numérique du 7 octobre 2016 une dispense des obligations prévues par l'article 40 du Code de procédure pénale au profit de l'ANSSI, dès lors que celle-ci est saisie par un hacker ayant agi de bonne foi, sans avoir donné une publicité à sa découverte :

> « *Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données* ».

L'ANSSI préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. Elle peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace qui lui est présenté pour avertir l'hébergeur, l'opérateur ou le responsable du système d'information.

On notera toutefois que l'expression « *de bonne foi* » est restée dans le texte, alors qu'il eût été préférable de mentionner l'absence de volonté de nuire.

Pour autant, la dispense ainsi reconnue ne fait pas obstacle à l'exercice de l'action publique qui demeure une prérogative du parquet. Libre à lui de poursuivre s'il estime que l'infraction est constituée et, en particulier, en cas de plainte de la victime. On peut éventuellement espérer qu'un «blanc-seing» de l'ANSSI entraîne, pour des motifs d'opportunité, un classement sans suite par le Parquet.

Mais il convient de noter les réserves exprimées sur la solution finalement adoptée, par les professionnels et hackers blancs eux-mêmes, qui s'interrogent à bon droit sur la réelle marge de manœuvre dont disposera l'ANSSI pour juger de la bonne foi et préserver la confidentialité. Ils ont parfaitement compris que la nouvelle loi n'offrait *in fine* aucune garantie absolue à celui qui trouve et signale une faille. Quid également du délai dans lequel les failles seront effectivement traitées si l'objectif poursuivi est bien celui de contribuer à la détection puis résolution des failles ?

Reste également ouverte la question des personnes qui ne sont pas des hackers et qui découvrent une faille par un pur hasard. Fort est à parier qu'elles n'auront jamais l'idée de contacter l'ANSSI. Plutôt que l'affaire « Bluetouff », qui avait concentré et égaré les débats, il faudrait se référer à l'affaire « Kitetoa », dans laquelle un internaute, qui avait découvert par hasard une faille de sécurité dans un site web et l'avait signalée au propriétaire du site, avait été attaqué en justice par ce dernier pour accès frauduleux au système. L'internaute avait été condamné en première instance avant d'être relaxé en appel. Un tel précédent n'incite pas l'internaute moyen à signaler les failles qu'il peut découvrir par hasard.

Enfin, il est à nouveau regrettable que cette disposition soit intégrée dans le Code de la défense (art. L. 2321-4), ce qui affaiblit une fois de plus l'unité de la loi « Godfrain » dont les dispositions (notamment article 323-1) sont insérées dans le Code pénal.

Compte tenu de la solution actuellement adoptée, ne convient-il pas de travailler sur des règles d'éthique à mettre en place par les professionnels et les hackers blancs, et de chercher une solution simple pour le cas (pas si hypothétique) de l'internaute moyen qui découvre une faille par hasard, et qui n'a connaissance, ni du Code de la défense, ni même de l'existence de l'ANSSI ?

RECOMMANDATION N°2 – Positionnement éthique des professionnels et création d'un statut de repenti pour les cas les plus graves

Aux côtés des règles actuellement applicables mises en place récemment par le législateur, il convient de favoriser un positionnement éthique de la part des professionnels et le cas échéant prévoir la création d'un statut de repenti pour les situations les plus graves (systèmes d'importance vitale, risques de mise en danger des personnes…)

1.3 LA BANDE ORGANISEE

Il convient également de s'interroger sur le fait de savoir si les règles applicables en matière de criminalité organisée sont pertinentes dans le cadre d'une lutte efficace contre la cybercriminalité.

Le Code pénal prévoit deux cas relevant de la criminalité organisée s'appliquant aux infractions d'atteinte aux systèmes de traitement automatisé de données :

- l'association de malfaiteurs (article 323-4), permettant de poursuivre des personnes s'entendant pour commettre ensemble une atteinte à un STAD ;

- la commission d'une atteinte à un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, en bande organisée (article 323-4-1).

Or seul ce dernier cas permet d'appliquer les dispositions procédurales spécifiques résultant de l'application combinée des articles 706-72 et 706-73-1 du Code de procédure pénale. Ainsi, la diffusion en bande organisée de logiciels malveillants (virus informatiques) ne peut faire l'objet d'une enquête sous pseudonyme, alors même qu'une telle infraction est souvent facilitée par des échanges électroniques sur des plates-formes réservées à ces criminels. Cette technique pourrait faciliter l'identification des auteurs de ces infractions, en particulier au moment des premières étapes de leur commission.

Il est en conséquence dommage qu'une des dispositions les plus emblématiques introduites pour lutter contre certaines formes de cybercriminalité ne puisse s'appliquer aux infractions qui sont au cœur de cette cybercriminalité.

RECOMMANDATION N°3 – Etendre les dispositions de la bande organisée aux infractions de cybercriminalité dont le mode opératoire et la complexité le justifient

Il est proposé la définition d'une infraction d'atteintes aux systèmes de traitement automatisé de données en bande organisée :

- **Option 1 :** Pour tous les types de systèmes de traitement automatisé de données, avec une peine maximum de 7 ans (contre 10 ans en ce qui concerne les systèmes de l'Etat traitant des données à caractère personnel) ;

- **Option 2 :** Pour les systèmes de traitement automatisés de données de l'Etat, des collectivités locales, de leurs établissements publics et des personnes privées exerçant une mission de service public ;

- **Option 3 :** Pour les atteintes aux systèmes de traitement automatisé de données permettant de faciliter la commission des infractions visées aux articles 706-73 et 706-73-1 du Code de procédure pénale

2 REFERENCES AUX COMMUNICATIONS ELECTRONIQUES

2.1 REFERENCES SIMPLES AUX TECHNOLOGIES NUMERIQUES

Certaines références simples viennent uniquement rappeler que des responsabilités spécifiques peuvent résulter des dispositions particulières aux communications électroniques, ou que certains outils numériques peuvent être utilisés. Il convient d'harmoniser ces différentes dispositions entre elles.

Dans un certain nombre de cas, il est proposé d'ajouter une mention explicite aux formes numériques de réalisation des infractions pour souligner l'importance de leur répression et permettre le cas échéant leur comptabilité disjointe dans les systèmes de statistiques judiciaires (classification NATINF[18]).

RECOMMANDATION N°4 – Harmoniser et étendre les références aux technologies numériques

Il est proposé :

- d'harmoniser toutes les références aux technologies numériques, pour faciliter leur compréhension et leur mise en œuvre ;
- d'étendre de façon explicite les infractions qui peuvent s'appliquer dans un contexte numérique pour améliorer leur répression et leur comptabilité.

Ces propositions sont regroupées dans le Tableau 1 ci-après.

Tableau 1 – Références aux technologies numériques

Article du code pénal	En rouge texte ajouté, en gras texte modifié	Commentaire
226-8	« Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention. Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite, ~~**ou**~~ audiovisuelle **ou de la communication au public en ligne**, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »	Harmonisation avec la rédaction issue de l'alinéa 2 de l'article 227-24 du code pénal (ou de l'alinéa 3 de l'article 421-2-5 du code pénal). Applicable également aux articles : 223-15, 226-2, 227-28, 412-8, 413-3, 413-4, 433-10, 434-16 et 434-25.

[18] NATINF : nature d'infraction

Article du code pénal	**En rouge texte ajouté, en gras texte modifié**	**Commentaire**
313-1	« L'escroquerie est le fait, soit par l'usage ~~**d'un faux nom**~~ **d'une fausse identité, ou d'une ou plusieurs données de toute nature permettant d'identifier une personne**, ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende. »	Harmonisation avec la rédaction issue de l'article 226-4-1 du code pénal.
411-3	« Le fait de livrer à une puissance étrangère, à une entreprise ou une organisation étrangère ou sous contrôle étranger ou à leurs agents des matériels, constructions, équipements, installations, appareils**, systèmes de traitement automatisés de données ou leurs composantes** affectés à la défense nationale est puni de trente ans de détention criminelle et de 450 000 euros d'amende. »	Cet ajout permet d'intégrer explicitement les systèmes d'information affectés à la défense nationale dans les objets protégés.
411-9	« Le fait de détruire, détériorer ou détourner tout document, matériel, construction, équipement, installation, appareil, dispositif technique ou système de traitement automatisé ~~**d'informations**~~ **de données** ou d'y apporter des malfaçons, lorsque ce fait est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de quinze ans de détention criminelle et de 225 000 euros d'amende. […] »	Harmonisation avec la rédaction issue des articles 323-1 et suivants du code pénal.
413-13	« La révélation de toute information qui pourrait conduire, directement ou indirectement, à la découverte de l'usage, en application de l'article L. 861-2 du code de la sécurité intérieure, d'une identité d'emprunt**, d'un pseudonyme** ou d'une fausse qualité, de l'identité réelle d'un agent d'un service mentionné à l'article L. 811-2 du même code ou d'un service désigné par le décret en Conseil d'État prévu à l'article L. 811-4 dudit code ou de son appartenance à l'un de ces services est punie de cinq ans d'emprisonnement et de 75 000 € d'amende. […] »	Le pseudonyme est un cas particulier d'identité utilisé sur les réseaux de communication électronique.
432-9	« Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de	Harmonisation avec les termes utilisés dans l'article 100 correspondant du code de procédure pénale

Article du code pénal	**En rouge texte ajouté, en gras texte modifié**	**Commentaire**
	correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de ~~**télécommunications**~~ **communications électroniques**, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des ~~**télécommunications**~~ **communications électroniques**, l'utilisation ou la divulgation de leur contenu. »	modifié par la loi n°2016-731 du 3 juin 2016. En outre, le terme « télécommunications » subsiste encore dans de nombreux autres articles du code pénal et devrait la plupart du temps être substitué par « communications électroniques ».
434-4	« Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, en vue de faire obstacle à la manifestation de la vérité : 1° De modifier l'état des lieux d'un crime ou d'un délit soit par l'altération, la falsification ou l'effacement des traces ou indices, **y compris les données informatiques ou leurs supports** soit par l'apport, le déplacement ou la suppression d'objets quelconques ; […] »	En référence à l'article 56 alinéa 5 du code de procédure pénale sur les perquisitions
434-23	« Le fait de prendre ~~**le nom d'un tiers**~~ **l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier**, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. […]	Harmonisation avec la rédaction issue de l'article 226-4-1 du code pénal.
441-1	« Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée**, y compris numérique**, qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. […] »	Référence explicite aux supports d'expression numérique.
444-3	« Sont punies de cinq ans d'emprisonnement et de 75 000 euros d'amende :	Référence explicite à la commission de cette infraction par le biais des communications au public en ligne.

Article du code pénal	En rouge texte ajouté, en gras texte modifié	Commentaire
	1° La contrefaçon ou la falsification des sceaux, timbres ou marques d'une autorité publique, ou l'usage de ces sceaux, timbres ou marques, contrefaisants ou falsifiés ; 2° La contrefaçon ou la falsification des papiers à en-tête ou imprimés officiels utilisés dans les assemblées instituées par la Constitution, les administrations publiques ou les juridictions, la vente, la distribution ainsi que l'usage de ces papiers ou imprimés ainsi contrefaisants ou falsifiés ; 3° La contrefaçon ou la falsification d'estampilles et de marques attestant l'intervention des services d'inspection ou de surveillance sanitaire de la France ou d'un pays étranger. **Les infractions visées au présent article s'appliquent lorsqu'elles sont commises sur un service de communication au public en ligne.** »	

2.2 LES CIRCONSTANCES AGGRAVANTES LIEES A L'UTILISATION D'INTERNET

L'utilisation d'Internet ne saurait en tant que telle constituer une circonstance aggravante. En effet, il s'agit d'une modalité particulière de commission de l'infraction, mais ne porte pas en soi une dimension aggravante ou péjorative comme le sont l'usage d'une arme pour accompagner des menaces ou la commission d'une infraction à l'encontre d'une personne vulnérable.

En revanche, certaines techniques disponibles sur Internet permettent effectivement de renforcer, dans des proportions non négligeables, la portée de la publication d'un message ou d'une information. La portée d'une publication sur un site Web est potentiellement plus importante qu'un simple échange entre plusieurs personnes, même prononcées en public.

Ainsi, l'article 227-23 du Code pénal relatif aux incriminations ciblant la pédopornographie prévoit que :

> « *Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques*. »

On y précise donc l'action concernée, le média utilisé (un réseau de communications électroniques) et la façon de l'utiliser (à destination d'un public non déterminé). Etait alors visée par exemple la diffusion sur un site Web librement accessible ou sur un réseau pair à pair où les informations sont partagées avec toute personne s'y connectant.

RECOMMANDATION N°5 – Des circonstances aggravantes liées à l'utilisation d'Internet

Il est proposé d'harmoniser les dispositions prévoyant des circonstances aggravantes liées à Internet en reprenant chaque fois qu'elle est appropriée la terminologie utilisée par l'article 227-23 du Code pénal. Par ailleurs, dans quelques cas nouveaux, ces circonstances aggravantes pourraient être introduites.

Ces propositions sont regroupées dans les Tableaux 2 et 3 ci-après.

Tableau 2 – Harmonisation des mesures de circonstances aggravantes

Article	En rouge texte ajouté, en gras texte modifié
225-12-2	« 2° Lorsque la personne a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication **électronique** ; »
421-2-5	« Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende. Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis ~~**en utilisant un service de communication au public en ligne**~~ **par la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique**. » *Il s'agit ici simplement d'harmoniser la rédaction avec celle utilisée par ailleurs dans le Code pénal. [Cf. recommandation de la commission Paul]*

Tableau 3 – Extension des mesures de circonstances aggravantes

Article	En rouge texte ajouté, en gras texte modifié *En italique après, justification de la circonstance aggravante proposée*
226-4-1	« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. **Lorsque cette infraction est réalisée par l'utilisation, pour la diffusion de messages ou la publication de données permettant**

Article	En rouge texte ajouté, en gras texte modifié *En italique après, justification de la circonstance aggravante proposée*
	d'identifier une personne à destination d'un public non déterminé, d'un réseau de communication électronique, les peines sont portées à deux ans d'emprisonnement et 30 000 euros d'amende. » *Lorsque ces données sont publiées sur un média qui sera lu par un grand nombre de personnes, telle une petite annonce dans un contexte de recherche de contacts ou de rencontre amoureuse, l'effet démultiplicateur peut être réel.*
226-8	« Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention. […] **Lorsque l'infraction prévue au premier alinéa est réalisée par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique, les peines sont portées à deux ans d'emprisonnement et 30 000 euros d'amende.** » *Cette proposition d'aggravation est plus discutable, puisque l'infraction vise déjà la diffusion par la voie des médias audio-visuels qui pourraient tout autant être considérés comme une circonstance aggravante par leur portée.*
226-13	« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. **Lorsque l'infraction prévue au premier alinéa est réalisée par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique, les peines sont portées à deux ans d'emprisonnement et 30 000 euros d'amende**. » *Ici, la diffusion de secrets par un mode de communication qui en démultiplie la reproduction et donc le nombre de personnes susceptibles de recueillir ce secret est clairement plus importante qu'une simple diffusion dans un cercle fermé. Il existe même une théorie de « l'Effet Streisand » qui décrit le fait qu'une information qu'on souhaite cacher suite à sa diffusion serait ensuite reproduite sur Internet par des personnes ayant été témoin de sa diffusion.*
227-24-1	« Le fait de faire à un mineur des offres ou des promesses ou de lui proposer des dons, présents ou avantages quelconques, ou d'user contre lui de pressions ou de contraintes de toute nature, afin qu'il se soumette à une mutilation sexuelle est puni, lorsque cette mutilation n'a pas été réalisée, de cinq ans d'emprisonnement et de 75 000 € d'amende.

Article	**En rouge texte ajouté, en gras texte modifié** *En italique après, justification de la circonstance aggravante proposée*
	Est puni des mêmes peines le fait d'inciter directement autrui, par l'un des moyens énoncés au premier alinéa, à commettre une mutilation sexuelle sur la personne d'un mineur, lorsque cette mutilation n'a pas été réalisée. **Lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique, les peines sont portées à sept ans d'emprisonnement et 100 000 euros d'amende**. » *On reprend ici la rédaction d'articles tels que le 227-26, relatifs à la façon dont la mise en relation entre l'auteur des faits et la victime mineure a eu lieu.*
312-2	« L'extorsion est punie de dix ans d'emprisonnement et de 150 000 euros d'amende : […] **6° Lorsqu'elle est commise par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique**. » *Il s'agit ici de viser les messages utilisés pour menacer la personne (visibles d'un grand nombre d'autres personnes et donc avec un impact plus fort), ou alors lorsque les menaces permettant l'extorsion sont portées à destination d'un large public par les outils utilisés (comme lors de la diffusion d'un rançongiciel).*
313-2	« Les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende lorsque l'escroquerie est réalisée : […] **6° Lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique**. » *On reprend ici la rédaction issue de l'article 227-26 pour souligner la mise en relation potentielle d'un grand nombre de victimes par l'utilisation des moyens de communication électronique à destination d'un public non déterminé (publication d'une petite annonce par exemple).*
322-12	« La menace de commettre une destruction, une dégradation ou une détérioration dangereuses pour les personnes est punie de six mois d'emprisonnement et de 7 500 euros d'amende lorsqu'elle est soit réitérée, soit matérialisée par un écrit, une image ou tout autre objet.

Article	**En rouge texte ajouté, en gras texte modifié** *En italique après, justification de la circonstance aggravante proposée*
	La peine est portée à un an d'emprisonnement et 15 000 euros d'amende lorsqu'elle est commise par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique. » *Il s'agit ici de viser l'impact de la menace auprès d'un large public.*
322-13	« La menace, par quelque moyen que ce soit, de commettre une destruction, une dégradation ou une détérioration est punie d'un an d'emprisonnement et de 15 000 euros d'amende lorsqu'elle est faite avec l'ordre de remplir une condition. La peine est portée à trois ans d'emprisonnement et 45 000 euros d'amende s'il s'agit d'une menace de destruction, de dégradation ou de détérioration dangereuses pour les personnes **ou lorsqu'elle est commise par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique**. » *La menace ainsi portée concerne non seulement le gestionnaire d'un établissement mais éventuellement l'ensemble de ses occupants ou par exemple l'ensemble des clients d'une entreprise. On touche ici à des infractions qui peuvent sembler proches de celles relatives au terrorisme, mais sans qu'on en remplisse tous les critères d'une action réalisée « intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ».*
322-14	« Le fait de communiquer ou de divulguer une fausse information dans le but de faire croire qu'une destruction, une dégradation ou une détérioration dangereuse pour les personnes va être ou a été commise est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Est puni des mêmes peines le fait de communiquer ou de divulguer une fausse information faisant croire à un sinistre et de nature à provoquer l'intervention inutile des secours. **La peine est portée à trois ans d'emprisonnement et 45 000 euros d'amende lorsque l'infraction prévue au premier alinéa est commise par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique.** » *Même discussion que ci-dessus.*

Article	**En rouge texte ajouté, en gras texte modifié** *En italique après, justification de la circonstance aggravante proposée*
433-3	« Est punie de deux ans d'emprisonnement et de 30 000 euros d'amende la menace de commettre un crime ou un délit contre les personnes ou les biens proférée à l'encontre d'une personne investie d'un mandat électif public, d'un magistrat, d'un juré, d'un avocat, d'un officier public ou ministériel, d'un militaire de la gendarmerie nationale, d'un fonctionnaire de la police nationale, des douanes, de l'inspection du travail, de l'administration pénitentiaire ou de toute autre personne dépositaire de l'autorité publique, d'un sapeur-pompier professionnel ou volontaire, d'un gardien assermenté d'immeubles ou de groupes d'immeubles ou d'un agent exerçant pour le compte d'un bailleur des fonctions de gardiennage ou de surveillance des immeubles à usage d'habitation en application de l'article L. 127-1 du code de la construction et de l'habitation, dans l'exercice ou du fait de ses fonctions, lorsque la qualité de la victime est apparente ou connue de l'auteur. […] La peine est portée à cinq ans d'emprisonnement et 75 000 euros d'amende lorsqu'il s'agit d'une menace de mort ou d'une menace d'atteinte aux biens dangereuse pour les personnes**, ou lorsqu'elle est commise par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique.** » *Même raisonnement que plus haut sur l'impact plus fort d'une telle menace.*
433-5	« Constituent un outrage puni de 7 500 euros d'amende les paroles, gestes ou menaces, les écrits ou images de toute nature non rendus publics ou l'envoi d'objets quelconques adressés à une personne chargée d'une mission de service public, dans l'exercice ou à l'occasion de l'exercice de sa mission, et de nature à porter atteinte à sa dignité ou au respect dû à la fonction dont elle est investie. Lorsqu'il est adressé à une personne dépositaire de l'autorité publique, l'outrage est puni de six mois d'emprisonnement et de 7 500 euros d'amende. […] Lorsqu'il est commis en réunion **ou par l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique**, l'outrage prévu au premier alinéa est puni de six mois d'emprisonnement et de 7500 euros d'amende, et l'outrage prévu au deuxième alinéa est puni d'un an d'emprisonnement et de 15 000 euros d'amende. » *Même raisonnement que plus haut sur l'impact plus fort d'une telle menace.*

RECOMMANDATION N°6 – Des critères pour l'application de la circonstance aggravante

Une série de critères simples pourraient être pris en compte dans l'application de cette circonstance aggravante, qui cible la notion de public non déterminé (c'est-à-dire non déterminé au moment de la publication du message ou de l'information) :

- Le média électronique utilisé est ouvert à tous les publics ;
- ou visible par un public dont le nombre est nettement supérieur à l'entourage immédiat de la victime (famille proche, collègues de travail, amis) ;
- ou le protocole utilisé est destiné à la diffusion à un large public (site Web librement accessible, protocole de communication pair à pair).

En outre, lors de l'évaluation du quantum de peine réclamé, l'utilisation de techniques de camouflage ou d'anonymisation des actions et des transactions pourrait être prise en compte.

2.3 INFRACTIONS DE CONSULTATION HABITUELLE DE CONTENUS PROHIBES

Deux infractions du Code pénal prévoient à ce jour la notion de « consultation habituelle » de contenus prohibés. La première est contenue dans l'article 227-23 du Code pénal qui traite de pédopornographie. Cette disposition a été introduite par la Commission des affaires culturelles de l'Assemblée nationale dans un amendement 302 rectifié[19] qui reprenait les motifs suivants :

> *« Il est proposé de compléter le code pénal avec deux nouvelles dispositions :*
>
> - *Aujourd'hui, seul le fait de détenir sur un disque dur d'ordinateur ou tout autre support une image à caractère pornographique est puni par la loi de deux ans d'emprisonnement et de 30 000 euros d'amende. Il est proposé d'élargir cette incrimination non plus seulement à la détention mais également à la consultation de telles images qui est aujourd'hui pratiquée par les pédophiles via internet.*

En effet, l'évolution des technologies et en particulier la possibilité d'être connecté en permanence à Internet (câble, puis ADSL) a amené de nombreux adeptes de tels contenus à ne plus les télécharger et les stocker (par exemple pour ne pas être découverts par leurs proches), mais à les consulter au moment qui leur convenait. Les données illégales étaient alors éventuellement stockées (parfois en grandes quantités) dans le cache du navigateur, mais ne constituaient pas forcément aux yeux du magistrat le délit de détention d'images pédopornographiques. Il s'est donc ici agi de réprimer une action qui porte autant atteinte aux mineurs qui en sont indirectement victimes que la simple détention

[19] http://www.assemblee-nationale.fr/12/amendements/3184/318400302.asp

(par la démarche de recherche de nouveauté). L'aspect commercial fut du reste ajouté ultérieurement à ce même alinéa :

> *« Article 227-23 alinéa 4 du code pénal : Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende. »*

C'est la même démarche qui a conduit le législateur à créer une disposition similaire en matière d'accès à des contenus relatifs à l'apologie du terrorisme, dans l'article 421-2-5-2 :

> *« Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende.*
>
> *Le présent article n'est pas applicable lorsque la consultation est effectuée de bonne foi, résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice. »*

L'infraction est ici limitée aux services comportant des images montrant la commission d'actes d'atteintes volontaires à la vie.

De façon liminaire, certaines modifications de texte ont pu entraîner des changements de référence ou l'utilisation de termes qui ne sont plus appropriés. Ainsi, dans l'article 227-33 du Code pénal, la référence au sixième alinéa de l'article 227-23 doit être remplacée par une référence au cinquième alinéa. En effet, cet article a été modifié pour la dernière fois le 27 mars 2012 (loi 2012-409 de programmation relative à l'exécution des peines). Or, lors de la modification en août 2013 de l'article 227-23 relatif à la pédopornographie, le sixième alinéa qui faisait référence aux circonstances de commission en bande organisée est devenu le cinquième alinéa.

RECOMMANDATION N°7– INFRACTIONS DE CONSULTATION HABITUELLE

Il apparat pertinent de ne recourir à d'autres cas d'infractions de consultation habituelle que pour les contenus les plus graves et s'il est démontré que cette nouvelle infraction pourra apporter une véritable contribution à la lutte contre l'infraction principale et à sa prévention.

(et de façon liminaire, il est recommandé de remplacer, dans l'article 227-33, la référence au sixième alinéa de l'article 227-23 par une référence à son cinquième alinéa).

2.4 INFRACTION SE DEROULANT EXCLUSIVEMENT SUR INTERNET

L'article 227-22-1 du Code pénal décrit une infraction qui se déroule exclusivement par un moyen de communication électronique :

> *« Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.*
>
> *Ces peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende lorsque les propositions ont été suivies d'une rencontre. »*

En effet, l'objectif du législateur était de couvrir les circonstances dites de « *grooming* » (sollicitations sexuelles à l'encontre d'un mineur de quinze ans) qu'on couvrait auparavant de façon imprécise par la notion de corruption de mineurs. Il ne s'agit donc pas de stigmatiser Internet en tant que tel mais de décrire une situation très précise. Cette infraction permet aussi, en parallèle avec les dispositions du Code de procédure pénale autorisant l'enquête sous pseudonyme (article 706-47-3 du Code de procédure pénale), d'autoriser son constat par des enquêteurs prenant temporairement l'identité d'un mineur.

RECOMMANDATION N°8– INFRACTION SE DEROULANT EXCLUSIVEMENT SUR INTERNET

En l'état du droit positif et des usages, il apparaît que le dispositif déjà mis en place par le législateur répond aux exigences requises en matière de lutte contre la cybercriminalité.

3 PEINES COMPLEMENTAIRES

Le droit pénal comporte un certain nombre de mesures relatives au prononcé de la peine et à son application. Ces mesures peuvent être des peines stricto sensu (peines complémentaires, peines de substitution, suivi socio-judiciaire) ou des obligations imposées par la juridiction de jugement ou de l'application des peines.

3.1 CONFISCATION DE RESSOURCES IMMATERIELLES

Dans certains cas, les ressources immatérielles utilisées pour faciliter la commission d'une infraction constituent non seulement un outil indispensable à sa réalisation (et donc ne doit pas retomber entre les mains de délinquants), mais aussi un moyen de communication qui peut être utilisé pour sensibiliser le public (les utilisateurs d'un service cybercriminel, ceux qui cherchent à s'informer à son sujet ou ceux qui pourraient en être victimes). Enfin, dans certains cas, ces ressources pourraient faciliter la collecte de preuves numériques. Ainsi, un nom de domaine (et le site Web associé) ou un compte de réseau social pourraient-ils être utilement placés sous-main de justice au moment de l'enquête judiciaire et au-delà ?

C'est par exemple ce que réalisent régulièrement les autorités américaines lors d'opérations relatives à la lutte contre la contrefaçon ou à des escroqueries.

Il est intéressant de noter que des biens immatériels ont déjà fait l'objet de confiscation et, en particulier, les crypto-monnaies lors d'une affaire judiciaire dont ont été saisis le tribunal correctionnel de Foix et la gendarmerie en juillet 2014.

RECOMMANDATION N°-9 – CONFISCATION DE RESSOURCES IMMATERIELLES

Il est proposé la création d'une peine complémentaire de **confiscation de ressources immatérielles** (noms de domaines, comptes de réseaux sociaux ou de courrier électronique, etc). Cette peine complémentaire pourrait aussi trouver à s'appliquer comme peine de substitution à l'emprisonnement (art. 131-6).

Cette disposition trouvera écho dans l'application des dispositions correspondantes du Code de procédure pénale en matière de saisie conservatoire et s'agissant du rôle de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC).

3.2 CONTRAINTES VISANT A EVITER LA REITERATION DE L'INFRACTION

Comme peine complémentaire ou comme mesure d'application des peines, plusieurs dispositions du Code pénal apportent des contraintes supplémentaires à la personne condamnée pour éviter la réitération de l'infraction.

Certaines trouvent à s'appliquer plus particulièrement en matière de cybercriminalité telle l'interdiction d'entrer en contact avec certaines catégories de personnes (visée au 13° de l'article 132-45). Toutes ces mesures peuvent trouver une application numérique et il pourrait être explicitement prévu qu'elles soient applicables y compris par un procédé de communication électronique.

L'interdiction d'accéder à Internet de façon générale a été explicitement écartée par le Conseil constitutionnel dans sa décision 2009-580 DC du 10 juin 2009 (loi favorisant la diffusion et la protection de la création sur internet) :

> *« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme […] : en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services ».*

RECOMMANDATION N°10–CONTRAINTES VISANT A EVITER LA REITERATION DE L'INFRACTION

Au vu de ce qui précède, il n'est pas proposé d'explorer à nouveau la question de l'interdiction de l'accès à Internet, mais il est en revanche recommandé la pleine application des mesures existantes, en exploitant systématiquement leur effectivité dans le cyberespace.

Toutefois, dans tous les cas où un juge d'application des peines souhaiterait s'assurer de l'interdiction qui est faite à une personne condamnée d'entrer en contact via Internet avec certaines catégories de personnes, il faudrait qu'il puisse s'en assurer à l'aide de mesures d'enquête appropriées (ex : investigations numériques) pour vérifier le respect des mesures prononcées

CONCLUSION

L'étude effectuée pendant plusieurs mois par les membres du Groupe de travail Cyberlex – CECyF aboutit à une première conclusion somme toute assez rassurante : l'arsenal pénal de lutte contre la cybercriminalité existe d'ores et déjà et ne demande plus qu'à être appliqué dans les faits. Alors pourquoi ce sentiment d'inefficacité, voire de frustration, ressenti par les acteurs de la lutte contre la cybercriminalité ? Répondre à cette interrogation nous conduit à développer des réflexions complémentaires en guise de seconde conclusion pour aboutir à d'autres pistes de réflexions.

À l'issue de nos réflexions, il apparaît que les modifications qui sont proposées dans la présente contribution, allant de la simple coquille à rectifier jusqu'à quelques changements plus substantiels, ne changeront pas en réalité de manière profonde l'efficacité de la lutte contre la cybercriminalité. En effet, le droit rien que le droit, en particulier dans un domaine à haute implication technique et à l'évolution constante, peut rapidement montrer ses limites. Au-delà de la règle de droit applicable et de son efficacité, la question de l'efficience des disposions légales doit être au centre de tout dispositif mis en place.

La tenue annuelle du FIC est l'occasion idéale pour souligner l'urgence qu'il existe à mettre la question de la lutte contre la cybercriminalité au cœur des débats politiques et de la volonté de l'ensemble des acteurs impliqués qui doivent être concentrés sur un objectif commun. Cela signifie une prise de conscience de chacun face à la montée croissante des cyberattaques. Cela concerne les enquêteurs, les magistrats du Parquet et du siège, les pouvoirs publics, la gendarmerie nationale et la police judiciaire, les partenaires publics et privés, les auxiliaires de Justice (dont les avocats) et ce jusqu'au plus haut sommet de l'Etat en passant par les ministères de l'Intérieur, de la Justice, de la Défense nationale, de l'Economie.

Des dispositions du Code pénal peuvent avoir un effet totalement neutre sur le terrain de la lutte contre la cybercriminalité si les personnes en charge de cette mission ne sont pas formées, et convaincues de la nécessité de fournir les efforts nécessaires pour assurer l'efficience de l'ensemble de cet arsenal pénal et protéger les citoyens. La question de la mise à disposition des moyens nécessaires (humains, financiers et techniques) et de leur pérennité doit être posée avec l'inscription de la lutte contre la cybercriminalité comme une priorité nationale.

Par nature transverse et protéiforme, la lutte contre la cybercriminalité ne peut enfin se concevoir que de manière globale et ne saurait se contenter que d'une vision nationale. La recherche d'une coopération toujours plus étroite entre Etats, certes dans un domaine par nature régalien (et l'on connaît les difficultés d'application de la convention de Budapest), est le moyen pour permettre une meilleure collecte de preuves et éloigner de plus en plus l'impunité derrière laquelle se retranchent trop souvent à raison les cyberdélinquants.

Le présent rapport ne constitue qu'une première étape dans la réflexion du Groupe de travail de Cyberlex – CECyF pour une lutter contre la cybercriminalité renforcée. Les travaux du Groupe de travail vont en effet se poursuivre dans les mois qui viennent pour se concentrer sur l'élaboration de recommandations en matière de procédure pénale et pour l'ensemble des textes de loi et règlements qui concourent à la lutte contre la cybercriminalité.

ANNEXES

ANNEXE 1 - SUBTILITES SEMANTIQUES

En se reportant à la qualification d'infractions (notamment celles qui font l'objet d'aggravations), on notera que le législateur n'est pas constant dans la formule : selon les articles, il est fait référence à *« l'utilisation, pour la diffusion de messages à destination d'un public non déterminé d'un réseau de communication électronique »*, à *« un réseau de télécommunication à destination d'un public non déterminé », à un « réseau de télécommunication*[20] *»* ou, enfin, à l'utilisation d'un *« service de communication au public en ligne »*…

L'article 227-22-1 du Code pénal qui réprime le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle évoque l'utilisation d'un *« moyen de communication électronique ».*

Les nuances sont-elles volontaires ? Malheureusement, elles résultent souvent d'un empilement de textes sans reprise et analyse globales du corpus. Peuvent-elles s'expliquer en se reportant aux définitions de l'article 1er de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) ou à l'article L.32 du Code des postes et télécommunications électroniques qui portent pour les premières sur le mode d'échange avec le public (unilatéral ou réciproque) et, pour les secondes, sur des critères techniques (procédé de communication, réseau)?

Selon l'article 1er de la LCEN: *« On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public par un procédé de communication électronique de signes, de signaux, d'écrits, d'images ou de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ».*

Le même article définit la communication au public en ligne comme *« toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque entre l'émetteur et le récepteur ».* La différence repose donc sur l'échange, tandis que la communication au public par voie électronique serait *unilatérale*. La communication au public en ligne est une communication par voie électronique…

S'agissant de l'article L.32 du Code des postes et communications électroniques, on notera l'emploi du pluriel qui n'est pas fortuit, si l'on considère que le singulier caractérise l'échange de contenus, tandis que le pluriel s'applique aux émissions, transmissions ou réceptions de ces contenus.

Selon cet article, *« on entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique »*. Il y a cohérence avec la définition de la communication au public en ligne (cf. art 1er supra).

[20] L'expression « réseau de télécommunication » a été abandonnée au profit de « réseau de communication électronique ». Ainsi la loi du 5 mars 2007 relative à la prévention de la délinquance a toiletté l'article 227-23. L'article L. 5421-13 du code de la santé publique, pourtant créé par l'ordonnance du 19 décembre 2012, se réfère encore au « réseau de télécommunication ».

S'agissant du réseau de communications électroniques, la loi le définit comme *« toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage. Sont notamment considérés comme des réseaux de communication électroniques : les réseaux satellitaires, les réseaux terrestres, les systèmes utilisant le réseau électrique pour autant qu'ils servent à l'acheminement de communications électroniques et les réseaux assurant la diffusion ou utilisés pour la distribution de services de communication audiovisuelle »*.

Quant au réseau ouvert au public, il s'agit *de « tout réseau de communications électroniques établi ou utilisé pour la fourniture au public de services de communications électroniques ou de services de communication au public par voie électronique »*.

Enfin, on entend par services de communications électroniques *« les prestations consistant entièrement ou principalement en la fourniture de communications électroniques. Ne sont pas visés les services consistants à éditer ou à distribuer des services de communication au public par voie électronique »*.

- Sur la différence entre réseau et service de communication au public par voie électronique : pour quelle raison le viol, le proxénétisme, la pédopornographie sont aggravés si on emploie un « réseau » et le harcèlement moral un « service » ? Un service de communication au public « en ligne » permet, sur demande individuelle, un échange réciproque entre émetteur et récepteur (c'est le cas de forums, des chats, des réseaux sociaux), alors que le réseau est une installation de transport et de diffusion.

L'article 111-7 du Code de la consommation définit une plateforme comme un service de communication en ligne reposant sur :

1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ;

2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service.

- Sur la notion de public indéterminé : le viol, le proxénétisme, la pédopornographie ne seraient pas aggravés s'ils étaient commis avec un réseau de communication électronique à destination d'un public déterminé ?(Si l'auteur rencontre la victime grâce à un réseau de télécommunication tel Internet, il s'agit là d'une circonstance aggravante) Doit-on considérer que le public déterminé est celui qui reçoit une *« correspondance privée », « message exclusivement destiné à une (ou plusieurs) personne, physique ou morale, déterminée et individualisée»* au sens de la circulaire du 17 février 1988, prise en application de l'article 43 de la loi du 30 septembre 1986 ? Le public déterminé est-il un public restreint inaccessible sans un mot de passe ?

-Notons aussi que l'article 421- 1 2° utilise le terme d'infractions informatiques et non d'atteintes aux STAD. Une reformulation pourrait être dès lors proposée.

ANNEXE 2 - POUR UNE DEFINITION CLARIFIEE DE LA TERMINOLOGIE

Contrairement à ce qui est parfois affirmé, la cybersécurité n'est pas l'action, dans l'espace numérique, des services de sécurité (intérieure en particulier) et la cyberdéfense n'est pas la «cyber du ministère de la défense ». Quant à la cybercriminalité elle est trop souvent assimilée à la cyberdélinquance de profit. Ces trois définitions sont erronées. D'où l'importance d'une clarification des définitions.

La cybersécurité

La définition de l'ANSSI doit être retenue : La cybersécurité est un « *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ».

La cybersécurité est donc le fruit d'une trilogie. La cybersécurité concerne l'amont du judiciaire et donc la prévention des risques numériques.

Pour aller plus loin…

La cybersécurité

Avec la sécurité des systèmes d'information, la lutte contre la cybercriminalité et la cyberdéfense contribuent à la cybersécurité.

Une définition de la cybersécurité est contenue dans la recommandation UIT–T X.1205 de l'Union Internationale des Télécommunications, agence de l'ONU: « *On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber-environnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants : disponibilité, intégrité - qui peut englober l'authenticité et la non-répudiation - , confidentialité*».

Plus simple est la définition donnée par l'Autorité Nationale de Sécurité des Systèmes d'Information (ANSSI) : la cybersécurité est un « *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ».

La cybersécurité, ainsi définie, est le fruit d'une pluralité d'actions, dont la sécurité des systèmes d'information constitue un volet préventif ressortissant à l'action quotidienne.

La sécurité des systèmes d'information (SSI) concerne l'ensemble des acteurs publics et privés (administrations, entreprises, collectivités territoriales, etc.) qui l'appliquent par des mesures d'ordre interne. Plus tournée vers la prévention et la protection, elle relève de la responsabilité de chacun d'eux. Disponibilité, intégrité, confidentialité et traçabilité en sont les quatre piliers. Dans toute entreprise disposant d'une informatique de gestion ou de production un responsable de la sécurité des systèmes d'information (RSSI) met en œuvre la politique de sécurité, sous l'autorité de la direction générale ou du directeur des systèmes d'information (DSI). Au sein des ministères, les Hauts fonctionnaires de Défense et de Sécurité (HFDS) et les fonctionnaires de SSI (FSSI) exercent cette mission à l'égard de l'ensemble de la chaîne organique. Les collectivités territoriales, quant à elles, et leurs établissements publics développent de plus en plus la fonction SSI, car, ni les unes, ni les autres ne sont épargnés. La sécurité des systèmes d'information se situe donc en amont de toute autre action. C'est à cet échelon que doit s'opérer la détection des attaques et l'application des mesures d'urgence pour empêcher leur développement, notamment grâce à une capacité de cyberrésilience. Dans les entreprises les plus sensibles, la sécurité des systèmes d'information est complétée par des mesures plus contraignantes relevant de la cyberdéfense.

La cybercriminalité

Le rapport du Procureur général Marc Robert[21] doit être considéré comme la référence : « *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* ».

Sauf application du droit des conflits armés (reconnaissance par la communauté internationale d'un conflit interne ou externe), le droit commun s'applique et donc le droit pénal. Une action relève donc de la cybercriminalité si on peut la caractériser par une infraction pénale.

La trilogie « cybercriminalité, cyberterrorisme, cyberconflictualité » est une hérésie, car elle laisse imaginer que le cyberterrorisme ne relève pas de la cybercriminalité (ce qui contredit l'article 421-1 2° du Code pénal), tandis qu'elle méconnaît le fait que la « cyberconflictualité » n'est qu'une illustration paroxystique de la loi « Godfrain » (art. 323-1 et s. du Code pénal).

[21] Marc Robert, « *Protéger les internautes* », rapport sur la cybercriminalité, février 2014, p12.

Pour aller plus loin…

La cybercriminalité

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 ;**
- **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.**

L'OCDE qualifie de cybercriminel « tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données[22] ».

L'ONU reconnaît explicitement la difficulté d'arrêter une définition : « La façon dont est définie la cybercriminalité dépend le plus souvent de l'objectif visé dans le contexte où ce terme est utilisé. Un nombre limité d'atteintes à la confidentialité, à l'intégrité et à la disponibilité des données ou des systèmes informatiques constitue la quintessence de la cybercriminalité. Cependant, d'autres agissements, tels que l'utilisation d'ordinateurs pour réaliser un gain ou porter un préjudice, financier ou autre, y compris certaines formes d'usurpation d'identité et les atteintes aux contenus informatiques (qui relèvent tous de la « cybercriminalité » prise dans son sens le plus large), ne facilitent pas les efforts visant à définir juridiquement ce terme dans sa globalité. Cependant, une « définition » de la cybercriminalité n'est pas aussi utile dans d'autres contextes, par exemple pour fixer la portée des pouvoirs spéciaux en matière d'enquête et de coopération internationale, où il vaut mieux privilégier les preuves électroniques de l'infraction, quelle qu'elle soit, plutôt qu'un concept étendu et artificiel de « cybercriminalité[23] ».

En France, selon l'ANSSI[24], « la cybercriminalité est constituée des actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un crime ou d'un délit, ou les ayant pour cible. Elle regroupe :

- **Les crimes et délits traditionnels facilités par l'usage des nouvelles technologies : blanchiment d'argent sale, pédophilie, grand banditisme, terrorisme, etc. ;**
- **Les crimes et délits nouveaux directement liés à l'usage des technologies de l'information et de la communication : falsification de cartes bancaires, usurpation d'identité, taggage ou**

[22] OCDE Rapport *La fraude liée à l'informatique, analyse des politiques juridiques*, Paris 1986, p.7

[23] Office des Nations Unies contre la drogue et le crime (ONUDC), Etude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les Etats Membres, la communauté internationale et le secteur privé pour y faire face, UNODC/CCPCJ/EG.4/2013/2, p/2.

[24] Rapport ONDRP 2011, note de Philippe Wolf, chargé de mission auprès du directeur général de l'ANSSI, et Luc Vallée, ingénieur au centre opérationnel de l'ANSSI (COSSI).

défacement de sites officiels, attaque en déni de service ou botnets , vol de données, vol de ressources informatiques, « *phishing* » ou hameçonnage, « *carding* » (vente illégale de numéros de cartes bancaires), etc. ;

- **Le détournement rapide des nouvelles technologies à des fins criminelles et terroristes : usage des téléphones portables pour déclencher des bombes artisanales, GPS de plus en plus accessible et couplé à des moyens de communication pour guider des engins explosifs, drones commerciaux, internet des objets, etc. ».**

L'Office des Nations unies contre la drogue et le crime (ONUDC) définit, quant à lui, les actes de cybercriminalité selon le contexte et l'objectif de ces derniers et aboutit à la classification suivante [25] :

- **les agissements à motivation financière (l'utilisation d'ordinateurs pour réaliser un gain ou porter un préjudice financier, y compris certaines formes d'usurpation d'identité)**
- **les atteintes aux contenus des ordinateurs ;**
- **les atteintes à la confidentialité, à l'intégrité et à l'accessibilité/disponibilité des systèmes informatiques.**

Plus simple et sans doute plus opérante est la définition retenue par le rapport du Procureur général Marc Robert[26] : « 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 [27]». Cette définition retient la cible et l'outil sans risquer de se perdre dans une classification selon les auteurs, les mobiles ou les modes d'action.

La cyberdéfense

La définition de l'ANSSI doit également être prise comme référence : la cyberdéfense est « *l'ensemble des mesures techniques et non-techniques permettant à un État de défendre, dans le cyberespace, les systèmes d'information jugés essentiels*[28] ».

La cyberdéfense, contrairement à une idée parfois répandue par ceux qui ont un regard trop « militaro-centré », n'est pas la cybersécurité du ministère de la défense, car elle a un caractère interministériel et concerne aussi des acteurs privés, opérateurs d'importance vitale (OIV).

25 *« Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face »,* ONUDC, 23 janvier 2013

26 Marc Robert, « *Protéger les internautes* », rapport sur la cybercriminalité, février 2014, pXX.

27 « *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.

28 Tous les systèmes d'un opérateur d'importance vitale ne relèvent pas de la cyberdéfense. Seuls les plus sensibles sont pris en compte, les autres étant protégés au titre de la SSI.

Pour aller plus loin…

La cyberdéfense

Les exigences de la cyberdéfense, énoncées par les deux Livres blancs, se traduisent par des dispositions législatives contenues dans la loi de programmation militaire (2014-2019). Ce texte crée l'article L.2321-1 du Code de la défense qui précise l'architecture sommitale de la cybersécurité en attribuant au Premier ministre la responsabilité de définir et de coordonner l'action gouvernementale, dans le cadre de la stratégie de sécurité nationale et de la politique de défense.

La loi clarifie les relations entre les pouvoirs publics et les opérateurs d'importance vitale. Elle introduit six articles dans le code de la défense (art. L.1332-6-1 et s.), relatifs aux pouvoirs du Premier ministre à l'égard des opérateurs publics et privés qui relèvent de secteurs critiques au regard de la sécurité nationale. Les dispositions de ces articles sont précisées par le décret du 27 mars 2015[29] :

- **Sur proposition de l'ANSSI et après avis des ministres coordonnateurs, le Premier fixe par arrêté les règles de sécurité, éventuellement adaptées à leur spécificité, qui s'imposent aux secteurs d'activité d'importance vitale (article R.1332-41-1 du Code de la défense).**

- **Les opérateurs d'importance vitale désignent en leur sein un correspondant auprès de l'ANSSI. Ils doivent établir la liste des « systèmes d'information d'importance vitale » qu'ils mettent en œuvre qui comprend celle des opérateurs extérieurs (sous-traitants par exemple) qui participent à ces systèmes. Cette liste est contrôlée par l'ANSSI qui peut prescrire des modifications (art. R. 1332-41-2 du Code de la défense).**

- **Les opérateurs doivent installer des systèmes de détection des événements, dont le type figure parmi les règles de sécurité imposées (art. R.1332-41-3 du code de la défense). L'ANSSI établit la liste des systèmes de détection qualifiés ainsi que celle des prestataires de service les exploitant (art. R.1332-41-7 du code de la défense). Cette qualification s'effectue selon les modalités prévues par le décret du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de confiance pour les besoins de la sécurité nationale[30], dont l'ANSSI dresse la liste (art.R. 1332-41-9 du Code de la défense).**

- **Les opérateurs doivent informer l'ANSSI « heure par heure » des incidents de sécurité ou de fonctionnement qui affectent leurs systèmes d'information d'importance vitale (art. R. 1332-41-10 du Code de la défense).**

- **Des contrôles peuvent être prescrits par le Premier ministre et effectué au sein de l'OIV par l'ANSSI, un service de l'Etat ou un prestataire de service qualifié (art. R.1332-41-12 du Code de la défense). En s'appuyant sur une convention qu'il conclut avec lui, l'OIV doit fournir au contrôleur toutes les informations nécessaires à l'accomplissement de sa mission : documentation technique des équipements et logiciels, codes sources, moyens pour accéder aux systèmes, etc. Le rapport, couvert par le secret de la défense nationale, est exploité par l'ANSSI qui en communique les conclusions aux ministres concernés (art. R. 1332-41-13 à R.1332-41-15 du code de la défense).**

[29] Décret n°2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense.

[30] Décret n°2015-350 du 27 mars 2015. Publié le même jour, il est un des deux décrets d'application des articles 22 et suivants de la LPM.

Le non-respect des obligations imposées par la loi, notamment celle de notifier les incidents, peut entraîner des sanctions pénales visant les personnes physiques comme les personnes morales (art. L.1332-7 du Code de la défense).

ANNEXE 3 - UN DROIT « MILLEFEUILLES »

Sans prétendre à l'exhaustivité, l'inventaire ci-après met en exergue une dispersion du droit pénal préjudiciable à une approche globale de la cybercriminalité.

Certaines définitions nécessaires à l'application du droit pénal doivent être recherchées dans le Code des postes et télécommunications électroniques ou dans la loi pour la confiance dans l'économie numérique (LCEN). La loi « Godfrain » a perdu son unité. Des dispositions relatives à la cybercriminalité sont aussi contenues dans le Code de la consommation, le Code monétaire et financier.

Code pénal

- **Art. 226-16 à 226-24 :** infractions à la loi relative à l'informatique, aux fichiers et aux libertés

- **Art. 226-4-1 :** usurpation d'identité sur un réseau de communication au public en ligne

- **Art. 323-1 et s.:** atteintes aux STAD

- **Art. 411-9 :** destruction d'un STAD portant préjudice aux intérêts fondamentaux de la Nation.

Circonstances aggravantes

- Viol (article 222-24 8°), agression sexuelle (article 222-28 6°), traite des êtres humains (article 225-4-2 3°), prostitution de mineurs ou de personnes particulièrement vulnérables (article 225-12-2 2°), corruption de mineur (article 227-22), atteinte sexuelle sur mineur de quinze ans (article 227-26 4°), « *lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique* » ;

- Harcèlement moral (article 222-33-2-2) « *lorsque les faits ont été commis par l'utilisation d'un service de communication public en ligne* » ;

- Proxénétisme (article 225-7 10°) *« grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique.* » ;

- Pédopornographie (article 227-23), *« lorsqu'il a été utilisé pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communication électronique » ;*

- Diffusion de procédés destinés à la fabrication d'engins explosifs (article 322-6-1 2ème alinéa) ;

- Provocation ou apologie du terrorisme (article 421-2-5 alinéa 2 créé par l'article 4 de la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme).

Code de la défense :

- **Art. L 2321-2 :** irresponsabilité des acteurs de la cyberdéfense qui commettent des infractions à la loi Godfrain (323-1 à 323-3 du Code pénal) pour répondre à une attaque informatique.

- **Art. 2321-4 :** non application par l'ANSSI de l'article 40 à l'égard de l'auteur d'une infraction à la « loi Godfrain ».

Code de la sécurité intérieure :

- **Art. L.881-2 :** infractions relatives au refus de fourniture des conventions de déchiffrement.

Code de la propriété intellectuelle :

- **Art. L.341-1 et suivants :** atteinte aux droits des producteurs de bases de données ;

- **Art. L. 122-6 et s. et art. L.335-2 et s :** contrefaçon de logiciels ;

- **Art. L.521-10, L.615-14, L.623-32, L.716-9, L.716-10 :** infractions commises « *sur un réseau de communication au public en ligne »*

Code monétaire et financier

- **Art. 163-3 et 163-4 :** contrefaçon et falsification des moyens de paiement

Code de la santé publique

- **Art. L. 5421-13 4° :** Vente de médicaments falsifiés *« lorsque les délits de publicité, offre ou vente de médicaments falsifiés ont été commis sur un réseau de télécommunication à destination d'un public non déterminé* ».

Code des postes et communications électroniques

- **Art. L32 :** définitions *« communications électroniques », « réseau de communication électroniques », « réseau ouvert au public », « service de communications électroniques ».*

Loi du 21 juin 2004 pour la confiance dans l'économie numérique

- **Art 1er :** *définitions « communication au public par voie électronique », « communication au public en ligne »*

Préconisations : harmoniser ces différentes expressions qui introduisent des confusions regrettables