www.jusletter.ch

Koumba Koné

Cybercriminalité : évolution législative et jurisprudentielle, le cas de la France

La cybercriminalité étant un vaste sujet, il est intéressant d'avoir une vision d'ensemble des infractions pouvant être définies comme étant de « cybercrime », de faire un état des lieux des lois qui sont apparues ces dix dernières années renforçant l'action pénale et visant à lutter face à cette criminalité qui s'est adaptée, de faire un retour sur la jurisprudence qui est venue compléter la loi, puis de voir comment le législateur entend appréhender et lutter efficacement contre la cybercriminalité et au-delà des frontières.

Catégories d'articles: Contributions
Domaines juridiques: Droit pénal et droit de l'informatique; Droit pénal d'autres pays et droit comparé; Droit français

Proposition de citation: Koumba Koné, Cybercriminalité : évolution législative et jurisprudentielle, le cas de la France, in : Jusletter 10 novembre 2014

Table des matières

I. Introduction

[Rz 1] Le dictionnaire Larousse définit la cybercriminalité comme l'ensemble des infractions pénales commises sur les réseaux de télécommunication.

[Rz 2] La doctrine française définit la cybercriminalité comme regroupant les infractions commises via les réseaux de télécommunications et plus particulièrement sur l'espace d'Internet, employant l'usage d'un ordinateur. L'informatique étant tantôt l'objet même de l'infraction, tantôt le moyen.

[Rz 3] Mais il n'existe pour l'heure aucune définition juridique officielle de la cybercriminalité.

[Rz 4] A ce titre, un rapport sur la cybercriminalité[1] a été remis en juin 2014 à la Ministre de la justice, Madame Christiane Taubira. Ce rapport commandé par la garde des sceaux afin d'identifier les aspects à améliorer concernant la cybercriminalité dresse un tableau des lacunes pouvant être corrigées par le législateur pour appréhender ces infractions.

[Rz 5] La première lacune établie dans ce rapport est l'absence de définition juridique de la cybercriminalité. Ainsi, la définition suivante est proposée : « *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* ».

[Rz 6] La cybercriminalité est apparue avec l'essor d'Internet depuis la fin des années 90. En effet, de nouvelles techniques sont apparues, amenant les criminels à s'adapter aux nouvelles technologies et à les utiliser de façon plus élaborée et réfléchie qu'auparavant.

[Rz 7] En effet, l'espace Internet est devenu un lieu d'échange notamment depuis 2005 avec l'arrivée du « web 2.0 ». L'internaute est désormais devenu acteur dans l'espace d'Internet, il peut sans grande connaissance technique utiliser les nouvelles technologies pour interagir, échanger, communiquer, créant ainsi le « web social ». Le web social étant un espace d'interaction illimité entre internaute, créant une nouvelle économie notamment les réseaux sociaux tel que Facebook entre autres ou les web marchands.

[Rz 8] Ce nouvel espace dans lequel chaque internaute échange librement sur des sujets de société est également un espace où l'on communique volontiers des informations personnelles, dites données à caractère personnel, pourtant très sensibles et sans pour autant craindre sur le devenir de ces informations.

[Rz 9] En parallèle du web 2.0, les habitudes de consommation des internautes se sont également développées. Ainsi, on achète énormément sur Internet, et là encore, les informations bancaires circulant sur Internet sont des informations très sensibles, accessibles aux délinquants ayant une connaissance moyenne en informatique. Ces informations échangées de façon anodine par les internautes sont des mines d'or pour les criminels.

[Rz 10] En effet, la criminalité sur l'espace d'Internet s'est développée depuis 2005 de façon considérable, créant des infractions employant des méthodes informatiques de plus en plus sophistiquées.

[Rz 11] Ainsi, dans ce nouvel espace d'Internet, lieu de vie sociale, d'échanges, de communications et de commerce, s'est développée une « cyber-société », ainsi qu'une criminalité, comme dans toute société, une société exempte de crime étant tout à fait impossible[2].

[Rz 12] Criminalité ordinaire donc, mais également une criminalité pouvant être réalisée par tout individu ne connaissant pas les limites sur ce nouvel espace numérique. L'individu victime, mais l'individu également acteur et auteur d'infractions, sans en prendre réellement conscience, comme nous le verrons, notamment en matière de propriété intellectuelle, de diffamation et d'injure.

[Rz 13] Ainsi, le législateur s'est donc adapté à l'émergence d'une nouvelle forme de criminalité et a prévu en conséquence une série d'infractions couvrant les crimes et délits s'opérant désormais avec l'utilisation des nouvelles technologies, dites de cybercriminalité.

[Rz 14] La France fait partie des pays en Europe dans lesquels la lutte contre la cybercrimina-

1 Rapport sur la cybercriminalité intitule « Protéger les internautes », Groupe de travail interministériel, février 2014.

2 «*Le crime est normal, parce qu'une société qui en serait exempte est tout à fait impossible ; telle est la première évidence paradoxale que fait surgir la réflexion sociologique*», Emile Durkheim1894.

lité est la plus active, grâce à un arsenal législatif de plus en plus répressif, notamment envers l'obligation de filtrage imposée aux fournisseurs d'accès à Internet et hébergeurs de contenus.

[Rz 15] Précurseur, la France, dès 1978, prévoyait une loi relative à l'informatique et aux libertés visant à protéger les personnes physiques de tout traitement automatisé de données (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Puis, près de dix années plus tard, fut adoptée une loi relative à la fraude informatique (loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique). Face aux avancées technologiques, une série de normes est venue compléter ces deux lois, qui ne laissaient en rien penser qu'elles serviraient de socle en matière de lutte contre la criminalité informatique dans son ensemble. Dans cette continuité normative, et compte tenu des techniques que nous connaissons maintenant, le législateur français a mené un grand nombre de réflexions visant à renforcer l'action pénale. Ont ainsi été adoptées toute une série de lois, dont, pour ne citer que les plus importantes :

- la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne imposant aux personnes proposant un service de cryptographie de devoir fournir aux autorités les algorithmes de chiffrement.
- La très controversée loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, dite LOPSI 1, qui prévoit notamment la conservation pendant un an d'informations entourant les contenus échangés sur Internet, telles que les adresses IP, les pseudonymes, les login et mots de passe, et qui fait monter au créneau les fervents défenseurs des libertés individuelles.
- La célèbre loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), transposant la directive européenne 2000/31/CE du 8 juin 2000 sur le commerce électronique, ainsi que certaines dispositions de la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques. La loi avait entrainé de longs débats en France, car elle faisait peser sur les fournisseurs d'accès à Internet un certain nombre d'obligations, dont notamment une vérification *a priori* du caractère légal des comptes hébergés par leurs soins, ce qui, techniquement, s'avérait difficile à mettre en place. Difficile mais pas impossible, puisqu'après avoir menacé de suspendre toutes les pages personnelles qu'ils hébergeaient, les fournisseurs d'accès a Internet sont aujourd'hui, 10 ans après l'entrée en vigueur de la loi, acteurs de la lutte contre la cybercriminalité.

[Rz 16] Ainsi, en vingt ans, la France s'est dotée de lois et mesures pénales visant à créer de nouveaux délits, aggravant les peines encourues, renforçant ou octroyant de nouveaux pouvoirs aux forces de l'ordre, dans l'objectif de répondre à cette nouvelle forme de délinquance.

[Rz 17] Toutes ces mesures seraient sans grand intérêt si l'on ne se préoccupait pas d'appréhender les menaces en provenance de l'extérieur de nos frontières. Telle est malheureusement la force de la cybercriminalité ; elle évolue de façon mondiale sans aucune difficulté. Ainsi, la France doit se focaliser également sur une nécessaire coopération internationale, visant à harmoniser les législations et à adapter la mise en œuvre de procédures permettant des actions pénales efficaces. C'est dans cet objectif qu'est entrée en vigueur, le 1er juillet 2004, la Convention du Conseil de l'Europe sur la cybercriminalité.

[Rz 18] La cybercriminalité étant un vaste sujet, il est intéressant d'avoir une vision d'ensemble des infractions pouvant être définies comme étant des « cybercrimes », de faire un état des lieux des lois apparues ces quinze dernières années, renforçant l'action pénale et visant à lutter face à cette criminalité qui s'est adaptée, de faire un retour sur la jurisprudence qui est venue compléter

la loi (II), puis, dans un second temps, de voir comment le législateur entend appréhender et lutter efficacement contre la cybercriminalité en France et au-delà des frontières (III).

[Rz 19] Il est incontestable que la majeure partie des infractions dites de cybercriminalité existaient déjà avant l'apparition de l'Internet. Comme rappelé précédemment, les criminels se sont adaptés aux nouvelles technologies et ont développé de nouveaux moyens, appréhendant les systèmes d'informationd et ayant une longueur d'avance sur les pouvoirs de police.

[Rz 20] Ainsi, il convient de lister toutes ces infractions, les nouvelles méthodes employées par les criminels, mais également le dispositif législatif qui s'est non seulement adapté, mais renforcé, devenant parfois plus répressif.

II. Etat des lieux des infractions et des lois réprimant la cybercriminalité — retour sur les infractions, les lois et la jurisprudence réprimant la cybercriminalité

[Rz 21] Comme indiqué précédemment, les crimes et délits existaient déjà avant l'arrivée des réseaux de communication dans leur ensemble ; le législateur n'a fait qu'adapter les textes en fonction des nouveaux modes de réalisation des infractions.

[Rz 22] Ainsi, il convient de traiter les infractions commises grâce à l'informatique et les réseaux de communication et de distinguer le mode d'utilisation de ces moyens.

A. L'informatique comme objet même du crime ou du délit

1. La criminalité informatique

[Rz 23] Bien avant l'ère d'Internet, l'usage de l'informatique, et notamment du minitel, a entraîné des agissements tels qu'il a fallu prévoir des dispositions afin de protéger les personnes.

[Rz 24] Le législateur français a prévu, dans sa loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « loi informatiques et liberté », de réprimer les infractions relatives aux traitements automatisés de données. En effet, Internet n'existait pas, mais c'est bien l'informatique qui est concernée dans cette loi qui vise à interdire tout traitement de données.

1.1. Les atteintes aux traitements de données

[Rz 25] Ainsi, le Code pénal, en son article 226-16, dispose que :

> « *Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi. La peine encourue est de 3 ans d'emprisonnement et de 45'000 euros d'amende* ».

[Rz 26] L'article 226-17 du Code pénal dispose que :

> « *Le fait de procéder ou de faire procéder à des traitements automatisés d'informations sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment qu'elles ne soient déformées, endommagées ou communiquées à des tiers non*

autorisés. La peine encourue est de 5 ans d'emprisonnement et de 300'000 euros d'amende ».

[Rz 27] Ces deux infractions visent l'usage d'un ordinateur, sans l'utilisation d'un réseau de communication, et tendent à protéger les individus de toute collecte de leurs données à caractère personnel sans leur autorisation ou, s'agissant de la seconde infraction, le fait de ne pas sécuriser l'accès aux fichiers qui contiennent lesdites informations obtenues cette fois-ci avec le consentement de la personne.

[Rz 28] Avec l'arrivée de l'Internet, le législateur s'est adapté et a prévu le cas d'infractions commises ou pouvant être commises au moyen de l'informatique et du réseau Internet.

[Rz 29] Ainsi, l'article 226-18 du Code pénal dispose que :

« *Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique s'y opposant pour des raisons légitimes. La peine encourue est de 5 ans d'emprisonnement et de 300'000 euros d'amende* ».

[Rz 30] L'article 226-19 du Code pénal dispose que :

« *Le fait de mettre ou de conserver en mémoire informatisée sans l'accord expresse de l'intéressé des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques, religieuses ou les appartenances syndicales ou les mœurs des personnes . La peine encourue est de 5 ans d'emprisonnement et de 300'000 euros d'amende* ».

[Rz 31] Ainsi, par un jugement de septembre 1997[3], le Tribunal de Grande Instance de Privas a condamné un prévenu à huit mois d'emprisonnement avec sursis et au versement de la somme de 20'000 francs pour préjudice moral et 3'000 francs aux frais de procédure, pour, d'une part, avoir mis sur Internet des photographies à caractère pornographique de la victime, pour les avoir enregistrées sur un support informatique (une disquette) sans le consentement de la victime, et, d'autre part, pour avoir annoté sur ces photos les tendances sexuelles de cette dernière.

[Rz 32] Dès les années 90, les sanctions sont claires. On ne peut procéder à un traitement de données sans l'autorisation de l'intéressé, même si les données ont été récoltées de façon régulière. Dans le cas d'espèce, les photos avaient été prises avec le consentement de la victime du traitement. La jurisprudence est conforme à la volonté du législateur.

[Rz 33] Ces deux infractions se sont multipliées depuis l'évolution d'Internet avec l'ouverture des forums de discussion notamment. Nous pourrons rapprocher cette décision aux atteintes à la personnalité, lorsque nous aborderons les atteintes au droit à l'image, à la vie privée et la diffamation sur Internet.

1.2. Les atteintes et intrusions aux systèmes de traitement automatisé de données

[Rz 34] Le 28 novembre 1984, des journalistes de l'hebdomadaire satirique français, Le Canard Enchaîné, publiaient un article dans lequel ils expliquaient de quelle manière ils avaient réussi à pénétrer dans une base de données sensibles, à l'aide d'un simple minitel. Le législateur a donc voulu prévoir tout un dispositif législatif visant à sanctionner cette nouvelle forme de délinquan-

3 TGI Privas, 3 septembre 1997, legalis.net.

ce par la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « loi Godfrain ».

[Rz 35] Résulte de cette loi les articles 323-1 al. 1 du Code pénal qui dispose que :

> « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données. La peine encourue est de deux ans d'emprisonnement et de 30'000 euros d'amende* ».

[Rz 36] Cette disposition vise à sanctionner non seulement l'accès frauduleux, mais également le maintien frauduleux dans un système. Si bien que, si une personne a pu avoir l'autorisation par des codes d'accès (le cas d'un salarié par exemple) pour une durée ou une mission déterminée à un système, dès lors que cette autorisation a pris fin, sans même que les codes d'accès aient été modifiés ou supprimés par l'employeur, l'infraction est tout de même caractérisée, même s'il s'agit du poste de travail habituel de la personne qui accède au système[4].

[Rz 37] En effet, la fraude résulte dans la conscience de la personne qui accède au système, alors qu'elle sait pertinemment que l'autorisation qu'elle avait d'accéder au système a été supprimée.

[Rz 38] Enfin, l'article 323-1 al.2 du Code pénal qui sanctionne :

> « *Le fait de supprimer ou de modifier des données contenues dans le système, soit de procéder à une altération du fonctionnement de ce système. La peine encourue est de trois ans d'emprisonnement et de 45'000 euros d'amende* ».

[Rz 39] La Cour de Cassation, dans un arrêt du 8 décembre 1999, vient préciser la différence entre l'article 323-1 al. 2 du Code pénal, qui vise des modifications ou suppressions involontaires, et l'article 323-3 du Code pénal, qui vise des modifications ou suppressions volontaires, sans rechercher la volonté de nuire de l'auteur. En l'espèce, le comptable d'une société avait un droit d'accès au système et a volontairement modifié les données. La Cour dispose « *qu'en effet une écriture comptable constitue bien une information mais qu'à partir du moment où elle est validée et introduite dans un système comptable automatisé, elle devient une donnée dont la suppression et la modification est prohibée ; que le caractère frauduleux de cette suppression ou modification pour exister ne requiert pas la volonté de nuire ou de causer à autrui un préjudice mais seulement que l'opération soit interdite* ».

[Rz 40] « *En effet, le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé caractérise le délit prévu à l'article 323-3 du Code pénal, sans qu'il soit nécessaire que ces modifications ou suppressions émanent d'une personne n'ayant pas un droit d'accès au système ni que leur auteur soit animé de la volonté de nuire* ».[5]

[Rz 41] La loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité a ajouté un alinéa 3 et dispose que lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine encourue est portée à cinq ans d'emprisonnement et à 75'000 Euros d'amende.

[Rz 42] Cette dernière disposition vise les actes d'intrusion dans les systèmes automatisés de données de la préfecture pour faire de fausses cartes d'identité et englobe par conséquent les nouvelles atteintes qui sévissent de plus en plus d'usurpation d'identité sur Internet. A ce titre, nous aborderons ultérieurement la création du nouveau délit d'usurpation d'identité.

---

4 CA Paris, 5 avril 1994, D. 1994, IR, p. 130

5 Cour de Cassation, 8 décembre 1999, Bulletin criminel 1999 N° 296 p. 917

[Rz 43] La cybercriminalité englobe les infractions « traditionnelles », déjà existantes avant l'essor des nouvelles technologies, et qui se commettent au moyen d'Internet, mais également de nouvelles façons de procéder pour caractériser les infractions qui ont vu le jour avec les nouvelles technologies et l'utilisation de l'informatique.

B. L'informatique et/ou Internet comme moyen du crime ou du délit

[Rz 44] Il convient de distinguer les infractions relatives aux atteintes aux biens et celles relatives aux atteintes à la personne.

1. Les infractions relatives aux atteintes aux biens

1.1. L'escroquerie

[Rz 45] L'article 313-1 du Code pénal dispose que :

> « *l'escroquerie est le fait, soit par l'usage d'un faux nom 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. La peine encourue est de cinq ans d'emprisonnement et de 375'000 euros d'amende* ».

[Rz 46] Intéressons-nous dans un premier temps aux conditions de qualification de l'escroquerie pour voir ensuite sous quelle forme elle s'opère sur Internet.

1.1.1. Les conditions de qualification de l'infraction

[Rz 47] Elément matériel : l'escroquerie suppose une tromperie, la remise d'un bien et un préjudice subi.

[Rz 48] La tromperie se manifeste par le mensonge, mais le mensonge seul ne suffit pas à caractériser l'infraction. En effet, le mensonge oral ou écrit visant à se faire remettre un bien ou un service ne suffit pas à être sanctionné. L'article suppose en plus du mensonge, l'usage d'un faux nom, d'une fausse qualité ou l'emploi de manœuvres frauduleuses.

[Rz 49] S'agissant de la remise du bien, il faut que celle-ci ait été réalisée postérieurement à la tromperie, aux moyens tout juste énoncés et que ces moyens aient déterminé ladite remise.

[Rz 50] Et enfin un préjudice, préjudice pouvant être matériel (la remise d'une somme d'argent) ou moral (l'inquiétude lié au sort d'un bien remis, comme par exemple un bijou de famille).

[Rz 51] Elément moral : l'escroquerie étant une infraction intentionnelle, il sera nécessaire de prouver la volonté du présumé escroc de profiter de la victime. Par conséquent, dans l'hypothèse où un présumé escroc a cru de bonne foi pouvoir utiliser un nom qui a déterminé la remise du bien, l'infraction ne sera pas caractérisée. En effet, les juges du fond apprécieront la bonne ou la mauvaise foi de l'accusé.

1.1.2. Les différentes formes d'escroquerie pouvant s'opérer sur Internet

a. Transaction virtuelle, achat ou vente d'un bien

[Rz 52] L'escroc propose un bien onéreux à vendre. Il adresse à la victime un mail lui montrant les photos du bien à acquérir et lui proposede régler par le biais d'un service de transfert d'argent. L'argent est très rapidement retiré par l'escroc mais le bien n'est jamais envoyé.

[Rz 53] A l'inverse, la victime propose la vente d'un bien qu'elle adresse à l'escroc, mais la somme d'argent n'est ensuite jamais réglée à la victime.

b. Le « phishing »

[Rz 54] Le « *phishing* » est une technique qui consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance, comme une banque ou une administration, afin de lui soutirer des informations personnelles, par exemple un mot de passe, un numéro de carte de crédit, une date de naissance. Le « hameçonnage » peut se faire par l'envoi d'un courrier électronique ou de liens vers des sites Internet falsifiés ou autres moyens électroniques.

[Rz 55] Généralement, les escrocs envoient un mail avec le logo d'une société digne de confiance à plusieurs victimes, prétextant une mise à jour de leurs données ou une opération de maintenance, les invitant souvent à se connecter sur un autre site par le biais du lien hypertexte qui leur a été envoyé. Une fois sur le site Internet falsifié, les victimes entrent leurs informations personnelles. Le site falsifié comporte le logo de la société de confiance, mais l'adresse URL (le nom de domaine) est erronée, créant ainsi la confusion chez la victime.

[Rz 56] Très souvent le numéro de carte de crédit avec le nom sont communiqués par la victime qui constate par la suite un ou plusieurs retraits sur son compte bancaire ou que plusieurs achats ont été réalisés par l'escroc.

c. L'escroquerie dite « à la nigériane »

[Rz 57] La victime reçoit un courriel d'un inconnu qui lui propose de servir d'intermédiaire financier. Il se présente comme étant bénéficiaire d'un héritage conséquent, mais qu'il ne peut toucher, faute de moyens suffisants pour avancer les frais de succession ou, parfois, étant victime de persécutions par sa famille souhaitant vouloir le spolier de son héritage. Il demande à la victime de lui avancer la somme et lui propose en retour de toucher un pourcentage de l'héritage. Très souvent, le « hameçonnage » se réalise au moment où la victime envoie l'argent par virement bancaire ou par transfert d'argent à l'auteur. Une fois le versement effectué, le contact est rompu et la victime ne reçoit pas la commission promise.

1.2. La contrefaçon

[Rz 58] Le délit de contrefaçon est prévu par le Code de la propriété intellectuelle, qui le définit comme étant la violation d'un droit de propriété intellectuelle par le fait de reproduire ou d'imiter un titre de propriété industrielle ou une œuvre de l'esprit relevant du droit d'auteur, sans en avoir le droit, ou en affirmant ou laissant présumer que la copie est authentique.

[Rz 59] Il peut s'agir de la contrefaçon de la propriété littéraire ou artistique, prévue à l'article L335-2s du Code de propriété intellectuelle, de la contrefaçon de dessins et modèles, prévue à l'article L521-2s du Code de la propriété intellectuelle ou encore de la contrefaçon de brevet d'invention, prévue à l'article L615-14s du Code de la propriété intellectuelle. Les peines encourues sont identiques, trois ans d'emprisonnement et 300'000 euros d'amende à l'encontre des personnes physiques.

[Rz 60] Il peut également s'agir de la contrefaçon de marques de fabrique, de commerce et de service. L'article L716-9 du Code de la propriété intellectuelle puni de quatre ans d'emprisonnement

et de 400'000 euros d'amende le fait :

> « *Pour toute personne, en vue de vendre, fournir, offrir à la vente ou louer des marchandises présentées sous une marque contrefaite : a) d'importer, d'exporter, de réexporter ou de transborder des marchandises présentées sous une marque contrefaisante ; b) de produire industriellement des marchandises présentées sous une marque contrefaisante et c) de donner des instructions ou des ordres pour la commission des actes visés aux a et b* ».

[Rz 61] L'article L716-10 du Code de la propriété intellectuelle puni de trois ans d'emprisonnement et 300'000 euros d'amende le fait :

> « *pour toute personne : a) de détenir sans motif légitime, d'importer ou d'exporter des marchandises présentées sous une marque contrefaisante ; b) d'offrir à la vente ou de vendre des marchandises présentées sous une marque contrefaisante et c) e reproduire, d'imiter, d'utiliser, d'apposer, de supprimer, de modifier une marque, une marque collective ou une marque collective de certification en violation des droits conférés par son enregistrement et des interdictions qui découlent de celui-ci* ».

[Rz 62] S'agissant des infractions commises par des personnes morales, l'amende est égale au quintuple de celle prévue pour les personnes physiques, sans compter les sanctions de la dissolution, la fermeture ou placement sous surveillance électronique, conformément aux dispositions de l'article 131-38 et 131-39 du Code pénal.

[Rz 63] La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure durcit les sanctions lorsque le délit est commis par voie de communication au public en ligne et prévoit désormais une peine de cinq ans d'emprisonnement et de 500'000 euros d'amende. Comme pour les crimes et délits commis sur mineurs, le délit de contrefaçon commis au moyen d'Internet est désormais une circonstance aggravante, au même titre que le fait de commettre l'infraction en bande organisée.

2. Les infractions relatives aux atteintes à la personne

2.1. Corruption d'un mineur

[Rz 64] L'article 227-22 du Code pénal sanctionne :

> « *Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur* ». *La peine encourue est de cinq ans d'emprisonnement et de 75'000 euros d'amende.*
>
> *Ces peines sont portées à sept ans d'emprisonnement et 100'000 euros d'amende 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 communications électroniques* ».

[Rz 65] L'article 227-22-1 du Code pénal sanctionne :

> « *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. La peine encourue est 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* ».

2.2. Pédopornographie

[Rz 66] L'article 227-23 du Code pénal sanctionne :

> « *le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique. La peine encourue est de cinq ans d'emprisonnement et de 75'000 euros d'amende.*
>
> *Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.*
>
> *Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.*
>
> *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.*
>
> *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.*
>
> *Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500'000 euros d'amende lorsqu'elles sont commises en bande organisée.*
>
> *La tentative des délits prévus au présent article est punie des mêmes peines.*
>
> *Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image* ».

[Rz 67] Intéressons-nous à l'alinéa 4, dans sa version actuelle, qui dispose que « *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 punissable.

[Rz 68] Sa rédaction avant la promulgation de la loi n° 2013-711 du 5 août 2013 portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne et des engagements internationaux de la France était la suivante : « *Le fait de détenir une telle image ou représentation est puni de deux ans d'emprisonnement et 30'000 euros d'amende* ».

[Rz 69] La question à l'époque était de savoir si le fait de consulter une image pédopornographique pouvait tomber sous le coup de la loi.

[Rz 70] En effet, lorsque l'on se connecte sur Internet pour visionner des images, ces dernières s'enregistrent de façon automatique sur la mémoire de l'ordinateur mais de façon temporaire, et ne sont pas enregistrées définitivement. Cela ne signifie pas pour autant qu'elles sont détenues

par celui qui les visionne.

[Rz 71] C'est en tout cas ce qu'avait estimé la Cour d'appel de Lyon, suivie par la Cour de cassation[6] qui, respectant le principe d'interprétation restrictive qui prévaut en droit pénal, avait répondu à la question par la négative.

[Rz 72] Ainsi, aussi dur que cela puisse paraître, elle n'avait pas condamné, sur les dispositions de l'article 227-23 al. 4, un homme qui avait dépensé, à l'époque, la somme de 5'610 francs sur une période de 6 mois pour le visionnage de plusieurs milliers d'images à caractère pédopornographique.

[Rz 73] La Cour retient que « *pour renvoyer le prévenu des fins de la poursuite, les juges retiennent que les images observées n'ont été ni imprimées ni enregistrées sur un support et que la simple consultation de sites pornographiques mettant en scène des mineurs ne suffit pas à caractériser le délit prévu par l'article 227-23, alinéa 4, du Code pénal* ». Pour la Cour de cassation, la Cour d'Appel avait légalement justifié sa décision en raisonnant ainsi.

[Rz 74] Comme indiqué plus haut, la loi n° 2013-711 du 5 août 2013 est venue corriger cela en modifiant l'alinéa 4 de l'article 227-23 du Code pénal, qui désormais précise et sanctionne la simple consultation habituelle ou une consultation moyennant contrepartie financière sur Internet.

[Rz 75] Cette loi est la transposition de la directive 2011/93/UE[7], visant à harmoniser au sein de l'union européenne les infractions pénales relatives notamment à la pédopornographie, particulièrement sur Internet.

[Rz 76] Ainsi, « *les Etats membres doivent faire en sorte que les sites à caractère pédopornographique hébergés sur leur territoire soient rapidement supprimés et s'efforcer de faire supprimer ceux hébergés à l'étranger. Par ailleurs, ils ont, sous certaines conditions de transparence et d'information des internautes, la possibilité de bloquer l'accès à ces sites sur leur territoire* ».

[Rz 77] Pour ce dernier point, la France prévoyait déjà, en partie, de telles mesures dans sa loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). La loi prévoit que les fournisseurs d'accès Internet et les personnes, physiques ou morales, mettant à disposition du public par des services de communication au public en ligne, doivent, d'une part, mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Et d'autre part, ils ont l'obligation d'informer promptement les autorités judiciaires de toutes activités illicites, et notamment en vertu de l'article 227-23 du Code pénal, qui leur seraient signalées et qu'exerceraient les destinataires de leurs services ; ils doivent enfin rendre publics les moyens qu'ils consacrent à la lutte contre ces activités illicites, sous peine d'un an d'emprisonnement et de 75'000 euros d'amende. S'agissant de ce dernier point, nous verrons en seconde partie l'intervention des acteurs privés dans la lutte contre la cybercriminalité.

[Rz 78] L'article 227-24 du Code pénal sanctionne :

> « *Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message. La peine encourue est de trois ans d'emprisonnement et de 75'000 euros d'amende lorsque ce message*

6 Cour de cassation, 5 janvier 2005, n°G04-82.524 FS-PF N°214.

7 Directive2011/93/UEdu 17 décembre 2011, JO L335.

est susceptible d'être vu ou perçu par un mineur.

Lorsque les infractions prévues au présent article sont soumises 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 ».

[Rz 79] Il s'agit ici de l'application des dispositions relatives à la presse, que nous aborderons plus en détails ultérieurement.

[Rz 80] L'article 227-25 du Code pénal sanctionne :

« *Le fait, par un majeur, d'exercer sans violence, contrainte, menace ni surprise une atteinte sexuelle sur la personne d'un mineur de quinze ans. La peine encourue étant de cinq ans d'emprisonnement et de 75'000 euros d'amende* ».

[Rz 81] L'article 227-26 al. 4 du Code pénal dispose que :

« *L'infraction définie à l'article 227-25 est punie de dix ans d'emprisonnement et de 150'000 euros d'amende, 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* ».

[Rz 82] L'article 227-27-1 du Code pénal prévoit :

« *le cas où les infractions prévues par les articles 227-22, 227-23 ou 227-25 à 227-27 sont commises à l'étranger par un Français ou par une personne résidant habituellement sur le territoire français, la loi française est applicable par dérogation au deuxième alinéa de l'article 113-6 et les dispositions de la seconde phrase de l'article 113-8 ne sont pas applicables* ».

[Rz 83] En effet nous étudierons en seconde partie le cas de la procédure pénale, puisqu'en matière d'Internet, il est souvent difficile d'identifier précisément le lieu où l'infraction a été commise, les serveurs ou la connexion pouvant être basés ou effectuée à l'étranger. Nous verrons ainsi comment s'opère alors la saisine de la justice et les coopérations pénales européennes et internationales.

2.3. Viol

[Rz 84] Il est à noter également qu'en matière pénale, la commission de certaines infractions au moyen d'Internet constitue une circonstance aggravante.

[Rz 85] Ainsi, l'article 222-23 dispose que :

« *tout acte de pénétration sexuelle, de quelque nature qu'il soit, commis sur la personne d'autrui par violence, contrainte, menace ou surprise est un viol* ». *Le viol est puni de quinze ans de réclusion criminelle* ».

[Rz 86] La peine encourue passe à 20 ans de réclusion criminelle « *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* », conformément aux disputions de l'article 222-24 al. 8 du Code pénal.

[Rz 87] Il en est de même pour les autres agressions sexuelles autres que le viol ; la peine est aggravée lorsque l'infraction aura été commise au moyen d'Internet (articles 222-27 et 222-28 al. 6 du Code pénal).

[Rz 88] Abordons dès maintenant les infractions relatives à la vie privée.

2.4. Atteinte au secret des correspondances

[Rz 89] L'article 226-15 du Code pénal dispose que :

> « *Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45'000 euros d'amende.*
>
> *Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions* ».

[Rz 90] De même que la loin° 91-646du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques dispose que « *le secret des correspondances émises par la voie des communications électroniques est garanti par la loi.*

[Rz 91] *Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci* ».

[Rz 92] Il en est de même pour toute administration publique, conformément aux dispositions de l'article 432-9 du Code pénal :

> « *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 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, 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, l'utilisation ou la divulgation de leur contenu* ».

[Rz 93] Ainsi, sur la base de ces dispositions, le Tribunal de Grande Instance de Paris a condamné, le 2 novembre 2000[8], au délit de violation de correspondances effectuée par voie de télécommunications par personne chargée d'une mission de service public prévu et puni par l'article 432-9 alinéa 2 du Code pénal, des enseignants et responsables d'un laboratoire de l'Ecole Supérieure de Physique et de Chimie Industrielle de Paris, qui avaient surveillé la messagerie d'un étudiant, pris connaissance de ses mails et supprimé certains d'entre eux. Ils évoquaient pour leur défense qu'ils voulaient préserver la sécurité du réseau, au motif que l'étudiant abusait de l'utilisation du réseau et de la messagerie à des fins privées.

[Rz 94] Le tribunal assimile le courrier électronique communément appelé e-mail, à de la correspondance privée, en application de la loi précitée, en énonçant ainsi « *Il convient donc de considérer que la messagerie électronique de la partie civile, à laquelle il n'était, en l'occurrence, possible*

8 Tribunal de Grande Instance de Paris 17ème chambre, chambre de la presse Jugement du 2 novembre 2000, legalis.net.

d'accéder qu'en utilisant son mot de passe, était protégée par le secret de la correspondance émise par voie de télécommunications, dont la violation tombe sous le coup de la loi pénale ».

[Rz 95] Dans le même sens, la Cour d'appel d'Angers[9] relaxe un prévenu au motif que « l*e courrier électronique est assimilable à une correspondance privée. Il est protégé par un mot de passe personnel et confidentiel qui est composé par l'usager au moment de sa connexion à internet ou à sa boîte aux lettres électronique. Son titulaire est le seul à y avoir accès et il est responsable de son utilisation. Ce n'est que par sa volonté ou sa négligence qu'un mineur peut la consulter* ».

[Rz 96] En l'espèce, le prévenu, qui était un artiste reconnu par ses pairs, avait envoyé des courriers électroniques contenant un lien vers un site Internet sur lequel on pouvait consulter des photographies à caractère pornographique, voir violent et morbide. Ces courriers électroniques avaient été adressés à une trentaine de destinataires bien précis et adeptes de son culte. Mais ce n'est que bien plus tard que le prévenu s'est aperçu que l'un des courriers électroniques avait été adressé à un destinataire qu'il ne connaissait pas, malgré les demandes de ce dernier de cesser l'envoi desdits messages, qui ont été malencontreusement visionnés par un mineur, faisant ainsi l'objet d'un dépôt de plainte au titre de l'article 227-4 du Code pénal.

[Rz 97] Le délit de corruption de mineur n'est pas retenu, *« l'élément moral de l'infraction n'existe donc pas en l'espèce* », le courrier électronique étant considéré comme une correspondance privée, peu importe son contenu.

[Rz 98] Nous l'avons vu plus haut, en matière d'atteinte à la personnalité sur Internet, il y a bien entendu l'atteinte à la vie privée, mais également l'atteinte au droit à l'image, que nous avons rapidement abordée lorsque nous avons traité de l'intrusion dans un système automatisé de données. En effet, le fait de conserver des données nominatives a été traité et, nous l'avons vu, les images sont également incluses dans la définition des données.

[Rz 99] Cela nous amène à traiter des cas d'atteintes au droit à l'image, puis ensuite des atteintes à l'honneur de la personne pouvant être réalisées au moyen d'Internet, telles que la diffamation et l'injure notamment, et les atteintes aux droit d'auteur. En effet, le droit d'auteur est une branche du droit de la propriété intellectuelle. Les titres de propriété industrielle, que nous avons abordés dans le chapitre consacré au délit de contrefaçon, ont, à juste titre, été traités dans les atteintes aux biens. S'agissant du droit d'auteur, il contient un droit personnel qui permet à l'auteur de se voir reconnaitre la paternité de son œuvre et d'en protéger son intégrité. Il y a donc une atteinte à la personnalité de l'auteur.

[Rz 100] Intéressons-nous en premier lieu aux infractions d'appel à la haine et à la violence sur Internet.

[Rz 101] Ces dispositions ne sont pas, en droit français, prévues dans le Code pénal, mais relèvent des infractions en matière de presse.

[Rz 102] Nous envisagerons ces infractions uniquement dans l'hypothèse où elles ont été commises par Internet.

[Rz 103] S'agissant des crimes et délits contre les personnes, il faut distinguer le cas particulier des infractions liés au propos tenu sur des sites internet. En France, ces infractions sont régit par la loi relative à la liberté de la presse et relève de dispositions particulières quant à leur mises en œuvre.

9 Cour d'appel d'Angers Chambre correctionnelle 10 juin 2003, legalis.net.

3. Les infractions relatives à la loi du 29 juillet 1881 sur la liberté de la presse

[Rz 104] On compte exactement 30 infractions sanctionnées par les articles 23 et suivants de la loi du 29 juillet 1881 sur la liberté de la presse ; nous citerons ici les plus courantes sur Internet, à savoir la diffamation, l'injure, l'injure raciale, l'incitation à commettre des crimes et des délits, et l'incitation à la haine ou à la violence, notamment raciale.

[Rz 105] La particularité de ces infractions nous amène à traiter du mode de leur poursuite et du délai de prescription.

a. De la poursuite et de la répression en matière de presse

[Rz 106] En matière de presse, c'est le régime de responsabilité dite « en cascade » qui s'applique. Ainsi, la loi dispose en son article 42, que seront poursuivis comme auteurs des crimes et délits commis au titre des infractions de la loi du 29 juillet 1881 sur la liberté de la presse, les directeurs de publications ou éditeurs. A défaut, les auteurs ; à défaut, les imprimeurs et à leur défaut, les vendeurs, les distributeurs et afficheurs.

[Rz 107] Le régime de responsabilité « en cascade » prévu par l'article 42 de la loi du 29 juillet 1881 sur la liberté de la presse vise à répondre aux difficultés rencontrées par la victime d'identifier l'auteur d'une infraction pouvant être commise par voie de presse. En effet, comme c'est fréquemment le cas en matière de presse, les auteurs emploient l'anonymat dans les articles qu'ils publient ; le législateur a donc décidé de placer en première ligne, par ce régime de responsabilités, le directeur de la publication ou l'éditeur dont le nom et les coordonnées doivent obligatoirement figurer dans les journaux et toutes publications (ouvrages).

[Rz 108] Il en est de même en matière audiovisuelle, sauf pour les émissions diffusées en direct. Dans ce cas, les auteurs de propos sont directement responsables.

[Rz 109] En transposant cette disposition à Internet, la responsabilité revient au directeur de publication du site Internet puis, à défaut, à l'auteur du message et, à défaut, au producteur.

[Rz 110] En s'adaptant toutefois à la spécificité de la communication électronique et au fait que les messages sont instantanés, la responsabilité du directeur de publication est atténuée, puisque ce dernier ne peut autoriser les messages des internautes avant leur mise en ligne.

[Rz 111] La jurisprudence est venue préciser le cas des messages que le directeur de la publication pouvait contrôler avant leur mise en ligne. C'est le cas de messages ayant fait l'objet d'une fixation préalable, conformément à l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle, qui dispose que « *au cas où l'une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication au public par voie électronique, le directeur de la publication ou, dans le cas prévu au deuxième alinéa de l'article 93-2 de la présente loi, le codirecteur de la publication sera poursuivi comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public* ».

[Rz 112] Dans une affaire mettant en cause un directeur de publication et un journaliste pour le délit de diffamation, la Cour de Cassation[10] a affirmé que « *le directeur de publication a pu exercer son contrôle sur le contenu du message avant sa diffusion, et dès lors que doit être considéré comme ayant fait l'objet d'une fixation préalable à la communication au public, au sens de l'article 93-3 de la loi du 29 juillet 1982, le message qui est diffusé à l'identique et de façon répétitive sur les ondes, la cour d'appel a justifié sa décision* » et rejette ainsi le pourvoi formé.

[10] Cour de cassation 5 octobre 2011.

[Rz 113] La jurisprudence définit donc ce qu'est un message ayant fait l'objet d'une fixation.

[Rz 114] En matière d'Internet, le directeur de la publication, pour voir sa responsabilité engagée, doit pouvoir prendre connaissance des propos litigieux avant leur diffusion ; il peut donc les retirer dès lors qu'il prend connaissance d'un contenu faisant l'objet d'un crime ou d'un délit.

[Rz 115] C'est d'ailleurs ce que vient préciser la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet, qui modifie l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle, en précisant que « *lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message* ».

[Rz 116] Mais en matière d'Internet, *quid* des propos ou des contenus diffusés sur les forums de discussion, où l'auteur ne peut être identifié, et pour lesquels le directeur de la publication n'a pas eu connaissance de la teneur du propos et n'a pas par conséquent pu les retirer de la diffusion au public, faute notamment de modération *à priori* ? Qui sera responsable ?

[Rz 117] C'est à ce vide juridique que la chambre criminelle de la Cour de cassation[11] vient de répondre, par deux arrêts rendus le même jour, en précisant, d'une part, qu'il convenait « *de rechercher si le directeur de la publication avait également la qualité de producteur* » au sens de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle et, d'autre part, quand bien même « *il n'y avait pas eu de fixation préalable des messages, le directeur de la publication, ayant pris l'initiative de créer un service de communication au public par voie électronique en vue d'échanger des opinions sur des thèmes définis à l'avance, pouvait être poursuivi en sa qualité de producteur, sans pouvoir opposer un défaut de surveillance du message incriminé* ».

[Rz 118] Elle définit par la même occasion la qualité du producteur d'un site Internet, d'un forum de discussions ou d'un blog comme celui qui a « *pris l'initiative de créer un service de communication au public par voie électronique en vue d'échanger des opinions sur des thèmes définis à l'avance* ».

[Rz 119] Désormais, il importe peu que les personnes qui organisent des forums de discussions et autres sites de communications au public en ligne, mettant ainsi à la disposition du public des messages adressés par des internautes sur Internet, n'aient pu mettre en place un système de modération, ni pris connaissance des propos litigieux ou des contenus diffusés pouvant faire l'objet d'une incrimination au sens de la loi du 29 juillet 1881 sur la liberté de la presse, avant leur mise en ligne. A défaut de pouvoir incriminer le directeur de la publication ou l'auteur, le producteur sera poursuivi.

[Rz 120] Pèse donc une présomption de culpabilité sur une personne privée pour des faits commis par autrui et dont cette dernière ignorait l'existence. De plus, il semble y avoir une différence de responsabilité entre le directeur de publication et l'auteur, et le producteur. Ce dernier étant responsable, quand bien même il n'a pas pris connaissance du contenu mis en ligne.

[Rz 121] On peut se demander si ces dispositions, visant à protéger les victimes de diffamation ou d'injure, entre autre sur Internet, est conforme notamment avec le principe selon lequel « *tout*

[11] Cour de cassation, le 16 février 2010, pourvoi n° 08-86301et 09-81064.

homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable », ancré à l'article 9 de la Déclaration des Droits de l'Homme et du Citoyen de 1789.

[Rz 122] C'est la question qui a été posée à la chambre criminelle de la Cour de cassation le 21 juin 2011[12]. En l'espèce, un producteur avait été condamné en première et seconde instance pour des faits de diffamation publique envers un particulier. Il demandait à la cour de se positionner sur l'inconstitutionnalité de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982, modifiée par la loi 12 juin 2009 sur la communication audiovisuelle en ce que, d'une part, l'article est contraire aux articles 8 et 9 de la Déclaration des droits de l'homme et du citoyen, en créant une présomption de culpabilité et en permettant d'imputer à une personne qui ne sait rien du contenu des messages diffusés sur son forum ou blog, une infraction à la loi du 29 juillet 1881 sur la presse, en réalité commise par d'autres ; d'autre part, le producteur affirmait que l'article en question méconnaît le principe d'égalité garanti par l'article 6 de la Déclaration des droits de l'homme et du citoyen en traitant différemment le directeur de publication et le producteur sur Internet, sans aucune justification.

[Rz 123] Par son arrêt, la Cour de cassation renvoie au Conseil constitutionnel la question prioritaire de constitutionnalité (QPC) ; ce dernier, dans sa décision du 16 septembre 2011[13], considère « *qu'en principe le législateur ne saurait instituer de présomption de culpabilité en matière répressive ; que, toutefois, à titre exceptionnel, de telles présomptions peuvent être établies, notamment en matière contraventionnelle, dès lors qu'elles ne revêtent pas de caractère irréfragable, qu'est assuré le respect des droits de la défense et que les faits induisent raisonnablement la vraisemblance de l'imputabilité ; qu'en outre, s'agissant des crimes et délits, la culpabilité ne saurait résulter de la seule imputabilité matérielle d'actes pénalement sanctionnés* » et déclare l'article conforme à laConstitution.

b. Sur le délai de prescription en matière de presse

[Rz 124] La loi du 29 juillet 1881 sur la liberté de la presse déroge aux dispositions de droit commun en matière de prescription de l'action publique pour la poursuite des crimes et délits. En effet, l'article 8 duCode de procédure pénale prévoit qu'en matière de délit, la prescription est de trois années révolues. En revanche, l'article 65 de la loi du 29 juillet 1881 prévoit une prescription des délits à trois mois révolus à compter du jour de la commission de l'infraction de presse ou du dernier acte d'instruction ou de poursuite s'il en a été fait. Cette prescription écourtée a été introduite par l'article 6-V de la loi du 21 juin 2004, diteLCEN, qui prend en compte la particularité d'Internet pour la commission des infractions, celles-ci étant continues sur Internet, alors que les infractions de droit commun sont généralement instantanées.

[Rz 125] Alors que pour l'infraction instantanée le délai commence à courir au jour de la commission de l'acte incriminé, pour l'infraction continue, le délai ne débute qu'à partir de la cessation de l'acte.

[Rz 126] Mais s'agissant d'Internet, lorsque des propos ou contenus litigieux sont mis en ligne pour une première fois, il est quasiment impossible de déterminer les fois où ils sont mis à nouveau en ligne sur un autre site Internet, prolongeant ainsi la matérialité de l'infraction dans le temps.

[Rz 127] Deux Cours d'appel, en 2004 et 2005[14], ont reconnu que des publications diffamantes

12 Cour de cassation chambre Criminelle, 21 juin 2011, pourvoi N° 11-800100.

13 Conseil constitutionnel, 16 septembre 2011, décision n° 2011-164 QPC.

14 Cour d'appel, 29 janvier 2004 et 26 mai 2005, Bulletin mensuel des arrêts de la Chambre criminelle janvier 2009.

publiées une première fois sur un site Internet et ayant fait l'objet d'une nouvelle publication à une autre adresse Internet constituaient une nouvelle publication, faisant courir à chaque fois le point de départ de la prescription de trois mois.

[Rz 128] A ce titre, la notion de réédition avait déjà fait l'objet d'un arrêt de la cour de cassation en 1991[15]; cette dernière avait jugé que la réédition d'un ouvrage constituait un nouvel acte de publication. Il semblerait que la Cour d'appel ait suivi la jurisprudence de la Cour de cassation, et ait ainsi transposé ce qui était applicable à la publication d'ouvrage à Internet.

[Rz 129] Mais manifestement, ce n'est pas la position de la chambre criminelle de la Cour de cassation en matière d'Internet. Par un arrêt du 6 janvier 2009[16], la Cour de cassation confirme sa position et réaffirme[17] que « *lorsque des poursuites pour l'une des infractions prévues par la loi du 29 juillet 1881 sont engagées en raison de la diffusion, sur le réseau Internet, d'un message figurant sur un site, le point de départ du délai de prescription de l'action publique prévu par l'article 65 de la loi précitée doit être fixé à la date du premier acte de publication ; cette date est celle à laquelle le message a été mis pour la première fois à la disposition des utilisateurs.*

[Rz 130] *Méconnaît ce principe la cour d'appel qui, pour retarder le point de départ de la prescription de l'action publique, retient qu'en créant un nouveau mode d'accès au site existant, plus accessible par une adresse plus courte et plus simple que la dénomination initiale, l'auteur a renouvelé la mise à disposition du message dans des conditions assimilables à une réédition, alors que la simple adjonction d'une seconde adresse pour accéder à un site existant ne saurait caractériser un nouvel acte de publication de textes figurant déjà à l'identique sur ce site* ».

3.1. Contrefaçons de droit d'auteur

[Rz 131] Ayant rappelé plus haut le délit de contrefaçon dans son ensemble, nous ne citerons ici que les cas liés au délit de contrefaçon se rapportant au droit d'auteur et droits voisins, ainsi que l'atteinte au droit moral de l'auteur. Plus particulièrement depuis les avancées technologiques, les œuvres compressées ou numérisées ont permis une diffusion plus grande sur Internet. cela est généralisé notamment par le « *peer to peer* » et les célèbres plateformes d'échanges qui ont rendu cela possible, à savoir « Emule et Kazaa ».

[Rz 132] Il est désormais de jurisprudence constante que la mise en ligne d'œuvres sans le consentement de l'auteur est caractéristique de contrefaçon. Face à l'ampleur du contentieux depuis la fin des années 90, nous ne citerons qu'un exemple jurisprudentiel récent.

[Rz 133] Vu l'article L. 121-1 du Code de la propriété intellectuelle[18] :

> « *Attendu que pour la condamner à verser à M. Claude X...-Y..., ès qualités, la somme de 30'000 euros en réparation du préjudice né des conditions d'utilisation des œuvres, l'arrêt retient que la société Artprice.com avait fait coexister sur son site les œuvres de l'artiste avec une importante quantité d'autres œuvres, sans avoir sollicité l'accord préalable des ayants droit, et qu'elle s'était comportée en « société anti-droits » d'auteur « puisqu'elle confisque ceux-ci en se les appropriant à grande échelle, grâce aux nouvelles technologies, ceci à des*

15 Cour de cassation, Chambre criminelle, 8 janvier 1991.

16 Cour de cassation, Chambre criminelle, 6 janvier 2009, pourvoi n°05-83.491.

17 Cour de cassation, Chambre criminelle, 16 octobre 2001, pourvoir n°00-85.728.

18 Cour de cassation, 1ère Chambre civile, 10 septembre 2014, legalis.net.

fins capitalistiques » ;

Qu'en se déterminant ainsi par des motifs insuffisants à caractériser l'atteinte au droit moral de l'auteur qu'elle retenait, la cour d'appel n'a pas donné de base légale à sa décision ».

3.2. Droit à l'image

[Rz 134] Le droit à l'image est un droit personnel que détient toute personne physique sur son image. En France, ce droit est consacré à l'article 9 du Code civil, qui dispose que « *Chacun a droit au respect de sa vie privée* ».

[Rz 135] Les sanctions pénales sont prévues aux articles 226-1, 226-2 et 226-8 du code pénal. La jurisprudence a également consacré une position ferme sur les atteintes au droit à l'image sur Internet, à savoir toute diffusion, publication, reproduction ou commercialisation sans l'accord explicite de la ou des personnes dont l'image est diffusée, porte atteinte à son droit à l'image.

3.3. Usurpation d'identité

[Rz 136] Traitons enfin du délit d'usurpation d'identité, une nouvelle infraction qui a été introduite par la loi n° 2002-1094 du 29 août 2002 d'orientions et de programme pour la sécurité intérieure (LOPSI) et la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) prévoyant des dispositions visant à lutter contre la criminalité générale et notamment contre la cybercriminalité. Insérant ainsi un nouvel article 226-4-1 au Code pénal, donnant définition du délit comme étant :

« *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 euros d'amende .*

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne ».

[Rz 137] Il s'agit ni plus ni moins du vol d'identité, qui n'était jusqu'à présent pas prévu par la loi ; mais les pratiques nouvelles que nous avons détaillées plus haut ont nécessité la création d'une nouvelle incrimination. En effet, seul le vol d'identité suivi de la commission d'une infraction pouvant entrainer des poursuites pénales contre la victime du vol d'identité était sanctionné (article 434-23 du Code pénal).

[Rz 138] Avec la création de ce nouveau délit, le vol d'identité seul, sans la commission d'aucune autre infraction, peut désormais être poursuivi.

[Rz 139] Ainsi, et pour ne citer que cet exemple, dans les cas d'escroquerie dits de « *phishing* » par exemple, où l'escroc va obtenir le numéro de carte de crédit ou le mot de passe de carte de crédit afin de pouvoir retirer le contenu du compte bancaire de la victime ou effectuer des achats sur internet, le délit d'usurpation sera caractérisé.

[Rz 140] Précédemment, la victime n'aurait pas pu se retourner puisqu'aucune infraction résultant du vol de son identité ne pouvait être sanctionnée.

[Rz 141] Nous l'avons vu, la France, en une quinzaine d'années, a renforcé son dispositif légal et est devenue de plus en plus répressive face à la cybercriminalité.

[Rz 142] Mais ces dispositions législatives sont-elles suffisantes pour appréhender les cybercriminels ?

[Rz 143] La particularité d'Internet est telle que les infractions sont commises sur des territoires différents, rendant plus difficile la tâche des enquêteurs. Quels sont les moyens dont se dotent la France, et plus généralement les pays, pour lutter efficacement contre la cybercriminalité ?

III. Les moyens mis en œuvre pour appréhender efficacement la cybercriminalité

[Rz 144] Internet n'ayant pas de frontières, comment raisonnablement lutter contre des infractions commises en dehors du territoire français ?

[Rz 145] En matière pénale, l'article 113-1 du Code pénal prévoit que la loi française est applicable pour les infractions commises sur le territoire français. Est réputée être commise sur le territoire une infraction dont l'un des éléments constitutifs a eu lieu en France. En matière d'infraction relative à Internet, le Tribunal de Grande Instance[19] a jugé que la France était compétente dès lors qu'un contenu ou qu'un message est rendu accessible par Internet sur le territoire français. Cela a été confirmé par un arrêt de la Cour de cassation en 2003[20], qui énonce que « *le juge français est compétent quels que soient la situation et le contenu d'un site s'il est accessible en France* ».

[Rz 146] Mais qu'en est-il lorsque des infractions se commettent simultanément dans plusieurs pays ou lorsque des investigations doivent avoir lieu à l'étranger ? L'intervention de plusieurs acteurs mettant en œuvre des moyens d'actions rapides et efficaces semble plus que nécessaire, qu'il s'agisse d'acteurs nationaux ou/et internationaux. Mais surtout l'importance d'établir une politique globale entre tous ces acteurs doit également être prise en compte pour lutter efficacement contre cette criminalité qui semble évoluer sans cesse.

A. L'intervention des acteurs nationaux

1. Les acteurs publics

[Rz 147] On l'aura rappelé à plusieurs reprises, cette criminalité qui sévit sur Internet étant nouvelle, il est naturel de se demander si les acteurs publics sont compétents pour enrayer l'évolution criminelle sur les réseaux. Les forces de l'ordre sont-elles suffisamment spécialisées dans la lutte contre la cybercriminalité ? Les acteurs et notamment les enquêteurs ont-ils su s'adapter sur les technologies et sur les connaissances scientifiques compte tenu de l'évolution rapide de la cybercriminalité ?

1.1. L'ordre judiciaire

[Rz 148] Le premier acteur public luttant contre la cybercriminalité est bien entendu la police judiciaire, qui a pour mission, de manière générale, de lutter contre la criminalité dans son ensemble. Les nouvelles technologies étant une spécialité particulière entraînant une nouvelle

[19] TGI, 17ème chambre, 26 février 2002, legalis.net

[20] Cour de cassation, 9 décembre 2003 arrêt Roederer, legavox.fr.

forme de criminalité, comme nous l'avons vu, il était nécessaire que la police se dote de moyens et services compétents en la matière ; il a donc fallu former les enquêteurs et créer des « brigades » spéciales ayant les moyens de comprendre et d'appréhender un nouveau genre de criminels. Il convient de voir en détails toutes les unités spéciales rattachées soit à la direction centrale de la police judiciaire (DCPJ) ou à la sous-direction de la police judiciaire (SDPJ) de la direction générale de la Gendarmerie nationale exerçant sous la direction et le contrôle des magistrats de l'ordre judiciaire.

1.1.1. Les unités de la police judiciaire

a. La brigade d'enquêtes sur les fraudes aux technologies de l'information

[Rz 149] Cette brigade, plus communément appelé BEFTI, est rattachée au service de la Direction Régionale de la Police Judiciaire de Paris. Elle a été créée en février 1994 avec pour mission de lutter contre les infractions suivantes : intrusion dans un ordinateur ou un réseau ; contrefaçon de logiciels ou de bases de données ; téléchargements illégaux ; piratage de réseau téléphonique ; défiguration de sites sensibles ; modification ou suppression de données ; défaut de sécurisation des données personnelles et collectes frauduleuses, illicites ou déloyales de données à caractère personnel.

[Rz 150] La BEFTI compte aujourd'hui 25 policiers spécialisés dans les nouvelles technologies. Elle est composée de trois groupes « enquêtes et initiative » et d'un groupe « d'assistance ».

[Rz 151] En 2011, la BEFTI[21] a constaté une hausse de 35% des saisines justifiées par l'accroissement très important du e-commerce, de l'e-administration et de l'ampleur du développement des nouveaux modes de communication. Elle a pu traiter 684 faits incriminés constatant une hausse de 27,8 % et procédé à 249 assistances traduites par un soutien aux autres services de police à l'occasion des constatations informatiques et des opérations de récupération de données.

b. La brigade centrale de répression de la criminalité informatique

[Rz 152] Cette brigade, plus communément dénommée BCRCI, est rattachée au ministère de l'Intérieur sous la Direction centrale de la police judiciaire (DCPJ). Créée le 15 mai 2000, elle a pour mission de réaliser les enquêtes à caractère national ou international dans le domaine de la criminalité informatique. La BCRCI est dotée de plusieurs services, notamment régionaux, qui interviennent en soutien dans ces domaines.

[Rz 153] Au sein de cette brigade a été créée une cellule Internet qui travaille en coopération avec la BCRCI et la Direction de la surveillance du territoire (DST) sur tous les sites attaqués présentant des intérêts au regard de la Défense nationale ou concernant les secteurs de pointe de l'industrie.

[Rz 154] Au niveau régional, il existe dix-neuf services régionaux de police judiciaire qui emploient chacun un groupe d'enquêteurs également spécialisés en criminalité informatique. Ils sont les correspondants locaux de la BCRCI.

c. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

[21] Source de la préfecture de police, prefecturedepolice.interieur.gouv.fr.

[Rz 155] L'office a été créé le 15 mai 2000[22]; il est également rattaché à la Direction Générale de la Police Nationale et dépend de la Direction Centrale de la Police Judiciaire. Il s'agit d'une structure nationale à vocation interministérielle. L'office a pour missions de réaliser et/ou de participer aux enquêtes judiciaires liées aux infractions de contrefaçons de logiciels, d'utilisation frauduleuse de cartes de crédit, de toutes les formes d'intrusions dans un système de traitement automatisé ; d'assister de manière technique les enquêteurs et de faire de la recherche technologique, et, enfin, de coordonner les coopérations nationales et internationales. A ce titre et dans le cadre de la réalisation de ces missions, l'office peut intervenir dans des enquêtes nationales en mettant notamment en place un réseau d'investigateurs en cybercriminalité et sur l'international en soutien aux renseignements d'enquêtes tel qu'INTERPOL et EUROPOL.

[Rz 156] L'office est également doté de trois sections spécialisées de 60 policiers et gendarmes, se composant comme suit :

[Rz 157] Une section opérationnelle, qui traite des infractions relatives aux atteintes aux cartes de paiement, des fraudes aux opérateurs de communication électronique et des atteintes aux systèmes virtuels de paiement ; depuis le 1er septembre 2009, cette section s'occupe également d'infractions relatives aux escroqueries sur Internet.

[Rz 158] Une section technique étant spécialement équipée de matériels et de logiciels d'investigations de haut niveau technologique pour assurer une assistance aux services d'enquêtes, mais également pour former les enquêteurs spécialisés en criminalité informatique, qui sont répartis sur l'ensemble du territoire national, se chargeant notamment d'enquêtes liées aux piratages. Cette section se charge également des interceptions judiciaires sur Internet.

[Rz 159] Enfin, une section de traitement des signalements composée des plateformes « PHAROS » et « Info-escroqueries ».

[Rz 160] La plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements (PHAROS), lancée le 6 janvier 2009, permet à tous les citoyens français ou étrangers de signaler un comportement illicite sur Internet, à charge ensuite pour les officiers de rediriger ces signalements vers les services adéquats en France ou à l'étranger. Cette plateforme est censée rendre plus facile le signalement de tout contenu ou comportement illicite pour les particuliers, qui ne savent pas systématiquement vers qui se tourner pour dénoncer les agissements sur Internet. En 2009, les officiers de la plateforme ont traités 52'353 signalements de contenus illicites et 77'646 en 2010[23].

[Rz 161] En ce qui concerne la plateforme Info-escroqueries, il s'agit d'une plateforme téléphonique d'informations et de prévention sur les escroqueries sur Internet, destinée à apporter des conseils aux victimes ou aux potentielles victimes d'escroqueries. La plateforme a enregistré en 2010 plus de 23'695 appels contre 23'608 en 2009[24].

[Rz 162] Quant à savoir si ces chiffres ont augmenté entre 2011 et 2014, aucune communication n'a été faite par les services de la police judiciaire à ce sujet, mais il est à craindre que oui.

---

22 Décret n° 2000-405du 15 mai 2000.

23 Source : police-nationale.interieur.gouv.fr.

24 Même source.

1.1.2. Les unités de la gendarmerie

a. Le service technique de recherches judiciaires et de documentation (STRJD)

[Rz 163] Le STRJD est rattaché au Pôle judiciaire de la gendarmerie nationale (PJGN). Il assure la surveillance du réseau Internet en recherchant la commission d'infractions relatives aux atteintes aux personnes et aux biens ainsi que celles relatives à la transmission de données à caractère illicite sur Internet, notamment sur les sites d'échanges communautaires ou les sites de *peer to peer*. Il met également en œuvre des techniques d'analyse comportementale et facilite le rapprochement judiciaire en constituant une base de documentation criminelle par thématique.

b. L'institut de recherche criminelle de la Gendarmerie nationale (IRCGN)

[Rz 164] L'IRCGN, également rattaché au Pôle judiciaire de la gendarmerie nationale (PJGN, se charge de tout ce qui a trait à l'informatique et l'électronique. A ce titre, il développe des méthodes, des outils et des logiciels qui permettent de détecter automatiquement des images pédophiles connues sur les réseaux ou disques durs ou d'extraire des données. Cet institut, unique en France en matière de preuve scientifique et étant à la pointe dans le domaine informatique, s'est vu confier la création et la gestion du centre national d'images pédopornographiques (CNAIP)[25], en collaboration avec la Police nationale. Le CNAIP, introduit par la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, a créé de nouvelles dispositions autorisant des enquêteurs, formés à cette mission et spécialement habilités, à procéder à des investigations sous pseudonyme sur Internet en matière d'atteintes portées aux mineurs. Créant dans le même temps, les « cyberpatrouilleurs » et précisant le cadre juridique de leur intervention. Il a pour vocation justement de faciliter l'identification des auteurs et des victimes d'infractions de nature sexuelle commises sur des mineurs dont les images ou représentations sont fixées, échangées ou diffusées, notamment par Internet. A ce jour, le centre a pu collecter pas moins de 470'000 images et vidéos saisies au cours des enquêtes judiciaires.

[Rz 165] Afin d'être plus efficace, le PJGN a créé en 2002 la formation N-TECH destinée aux unités de recherches. Cette formation est dispensée au centre national de formation de la police judiciaire (CNFPJ) et vise à former les experts de la gendarmerie aux nouvelles techniques, notamment informatiques, scientifiques et juridiques, sans cesse en évolution, pour lutter efficacement contre la cybercriminalité.

c. La brigade départementale de renseignements et d'investigations judiciaires

[Rz 166] Les BDRIJI sont implantées dans chaque département ; elles constituent le pôle criminalistique départemental de la Gendarmerie nationale. Spécialisées dans les domaines liés aux supports numériques, de la téléphonie mobile ou encore pour déceler les falsifications et contrefaçons de documents sécurisés, elles travaillent en liaison étroite avec le STRJD.

2. Les acteurs privés

[Rz 167] Avec Internet sont apparus de nouveaux acteurs exerçant une activité qui n'existait pas auparavant. Ainsi, les éditeurs et hébergeurs de sites Internet, mais également les fournisseurs d'accès Internet et autres opérateurs télécom fournissent des services qui permettent à la cybercriminalité de progresser dans cet espace numérique, étant des intermédiaires techniques. En

[25] Circulaire interministérielle n° CRIM-2010-7/E6du 22 mars 2010 relative aux investigations sous pseudonyme sur Internet et au rôle du centre national d'analyse des images de pédopornographie.

tant qu'acteur de la cybercriminalité, comment la responsabilité de ces derniers peut-elle être engagée lorsque sont commises des infractions au moyen des services qu'ils mettent à disposition ? Le législateur a décidé de mettre à la charge des personnes privées (personnes morales) des responsabilités au regard du rôle qu'ils occupent dans la cybercriminalité. Ces responsabilités sont rendues possibles par l'introduction de quatre lois. La loi sur la confiance dans l'économie numérique du 21 juin 2004, dite LCEN, relative aux droits sur Internet en matière de communication, d'hébergement, de commerce électronique, de publicité ; la loi relative au droit d'auteur et les droits voisins dans la société de l'information du 1er août 2006, dite DADVSI, qui traite, comme son nom l'indique, de la protection des œuvres et des auteurs à l'environnement numérique ; la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011, dite LOPSSI, qui offre un panel de mesures pour lutter contre les actes criminels sur Internet en vue de la protection des personnes ; et enfin la loi favorisant la diffusion et la protection de la création sur internet du 12 juin 2009, créant une autorité administrative l'Hadopi, Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet chargée d'assurer la mise en place de sanctions et de procédures légales pour tout internaute soupçonné de piratage.

[Rz 168] Cette responsabilité, pénale ou administrative, a été longuement débattue puisque ces acteurs ont avant tout un rôle économique dans la société et constituent un lobbying puissant. Après de nombreux rebondissements judiciaires, le Conseil Constitutionnel appelé à statuer sur la régularité des responsabilités que la loi faisait peser sur ces acteurs, les a déclarées conformes à la Constitution, répondant « *à son objectif d'intérêt général qui s'attache à la sauvegarde de la propriété intellectuelle et de la création culturelle poursuivi*[26] ».

[Rz 169] Dans le même sens, la Cour européenne des droit de l'homme, appelée à statuer sur une affaire de présomption de culpabilité d'un éditeur de forum de discussion[27], rappelle que « *la Convention ne prohibe pas les présomptions de fait ou de droit en matière pénale. Elle oblige néanmoins les Etats à ne pas dépasser à cet égard un certain seuil, ils doivent les enserrer dans des limites raisonnables prenant en compte la gravité de l'enjeu et préservant les droits de la défense* » et que donc « *eu égard à l'importance de l'enjeu, il s'agit de prévenir efficacement la diffusion dans les médias d'allégations ou imputations diffamatoires ou injurieuses en obligeant le directeur de la publication à exercer un contrôle préalable* ». La Cour estime que la présomption de responsabilité de l'article 93-3 de la loi de 1982 reste dans des « *limites raisonnables requises* ».

[Rz 170] Ainsi, ces intermédiaires techniques doivent, dans l'intérêt général, participer à la lutte contre le piratage, la contrefaçon et contre certaines infractions de presse qui s'opèrent sur Internet.

[Rz 171] Voyons maintenant, qui sont ces acteurs et quelles sont les obligations et mesures pénales qui pèsent sur eux, les enjoignant à participer à la lutte contre la cybercriminalité.

2.1. Les FAI

[Rz 172] Les FAIS, fournisseurs d'accès à Internet sont définis par la LCEN comme les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne.

[Rz 173] Les FAI ont l'obligation d'informer leurs abonnés de l'existence de moyens techniques

[26] Conseil constitutionnel, Décision n° 2004-499 DC du 29 juillet 2004.

[27] CourEDH, 30 mars 2004, Radio-France c/France, n° 53984/00.

leur permettant de restreindre l'accès à certains sites Internet, et de leur proposer au moins un dispositif de filtrage, comme le contrôle parental par exemple.

[Rz 174] Ils doivent également informer leurs abonnés des moyens permettant d'éviter que leur connexion soit utilisée pour réaliser des actes de contrefaçons d'œuvres de l'esprit, comme le téléchargement illégal.

[Rz 175] La LCEN ne les soumet à aucune obligation générale de surveiller les informations qu'ils transmettent, ni aucune obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Toutefois, l'autorité judiciaire peut leur demander de réaliser toute activité de surveillance ciblée et temporaire.

[Rz 176] Ils doivent agir promptement pour retirer les informations ou en rendre l'accès impossible dès qu'ils ont pris connaissance d'un fait litigieux, sous peine de voir leur responsabilité pénale engagée.

[Rz 177] Ils doivent également concourir à la lutte contre la diffusion de contenus relatifs aux infractions visées aux cinquième, huitième et neuvième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse (relatif entre autres aux infractions de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale) et aux articles 227-23 et 227-24 du Code pénal (relatif à la pornographie enfantine).

[Rz 178] Pour y parvenir, ils doivent notamment mettre en place un dispositif de signalement facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de contenus. Ils ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes d'un tel signalement et, d'autre part, de rendre publics les moyens qu'ils consacrent à la lutte contre ces activités illicites.

[Rz 179] En matière de répression des activités illégales de jeux d'argent, les FAI ont l'obligation de signaler aux destinataires de leurs services les sites illégaux de jeux en ligne et prévoir un lien vers le site de l'autorité de régulation des jeux en ligne (ARJEL).

[Rz 180] En matière de protection des mineurs, les autorités administratives et judiciaires pourront demander aux FAI de mettre en place des mesures de blocage de contenus pédopornographiques. Il s'agit en fait d'une obligation de filtrage et de surveillance. En pratique, l'OCLCTIC, dont nous avons présenté les missions plus haut, sera chargé d'adresser aux FAI une liste noire des sites pédopornographiques, à charge pour eux de prévoir techniquement les mesures de blocage de ces sites.

[Rz 181] Dans le même sens, tout juge saisi en référé ou sur requête, pourra prescrire aux FAI toutes mesures propres à prévenir ou faire cesser un dommage.

[Rz 182] Concernant les données personnelles, les FAI ont l'obligation de communiquer aux autorités judiciaires, sur demande, dans le cadre d'une enquête pénale ou de toute autorité administrative, toutes données permettant d'identifier l'origine et la durée de connexion d'un abonné à un site illicite.

[Rz 183] Tout manquement à ces obligations est puni d'un an d'emprisonnement et de 75'000 euros d'amende.

[Rz 184] S'agissante de la fourniture de réseau Internet, la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme modifiant l'article L34-1 du Code des postes et des communications électroniques dispose que :

> « *Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un*

accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article ».

[Rz 185] Le législateur a voulu inclure dans la définition de fournisseur d'accès Internet, non seulement la catégorie que nous venons d'étudier, mais également les cybercafés, lieux à partir desquels les cybercriminels peuvent commettre très facilement diverses infractions.

[Rz 186] Sans compter les autres personnes physiques ou morales qui émettent un signal wifi et permettent ainsi à tout public de pouvoir accéder à un réseau Internet de manière gratuite. Peuvent se trouver dans ce cas, les bibliothèques, les hôtels ou les entreprises.

[Rz 187] Conformément à la loi, ces personnes physiques ou morales doivent conserver pendant une durée maximale d'un an les données techniques de connexion permettant d'identifier tout auteur d'une connexion vers un site illicite ou au comportement présumé illicite et les mettre à disposition de toute autorité administrative ou judiciaire, avant de les effacer ou de rendre anonymes ces données.

2.2. Les hébergeurs

[Rz 188] Les hébergeurs sont définis par la loi comme étant « *les personnes physiques ou morales qui assurent, même à titre gratuit, une mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons, de messages de toute nature fournis par des destinataires de ces services* ».

[Rz 189] Tout comme les FAI, la LCEN ne les soumet à aucune obligation générale de surveiller les informations qu'ils stockent, ni à aucune obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Les hébergeurs ont exactement les mêmes obligations que les FAI citées plus haut en matière de lutte contre les infractions prévues à l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse, contre la pédopornographie et les jeux en ligne illégaux.

[Rz 190] Concernant les données personnelles, les hébergeurs ont l'obligation de communiquer aux autorités judiciaires, sur demande, dans le cadre d'une enquête pénale ou de toute autorité administrative, toutes données permettant d'identifier l'origine de la connexion (adresse IP, accès FTP et autres identifiants) de l'auteur de publications à contenus illicites.

[Rz 191] Les hébergeurs encourent les mêmes sanctions que les FAI.

2.3. Les éditeurs

[Rz 192] Les éditeurs sont définis par la LCEN comme étant les personnes physiques ou morales qui mettent en forme, publient et gèrent un site Internet. La LCEN précise que les personnes physiques qui éditent à titre professionnel doivent déclarer leurs nom, prénoms, domicile et numéro de téléphone, et, si elles sont assujetties aux formalités d'inscription au registre des sociétés ou au répertoire des métiers, elles doivent indiquer le numéro de leur inscriptionainsi que le nom du directeur ou du codirecteur de la publication et le cas échéant, celui du responsable de la publication, ainsi que le nom, la dénomination ou la raison sociale, l'adresse et le numéro de téléphone de l'hébergeur.

[Rz 193] En ce qui concerne les éditeurs personnes morales qui éditent également à titre professionnel, ils doivent déclarer leur dénomination ou leur raison sociale et leur siège social, leur

numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social et l'adresse de leur siège social ainsi que le nom du directeur ou du codirecteur de la publication et le cas échéant, celui du responsable de la publication, ainsi que le nom, la dénomination ou la raison sociale, l'adresse et le numéro de téléphone de l'hébergeur.

[Rz 194] Les éditeurs qui éditent à titre non professionnel (particulier éditeur d'un blog) n'ont pas les mêmes obligations, puisqu'ils doivent, avant toute mise en ligne sur un site Internet, déclarer leur identité à leur hébergeur ou à leur fournisseur d'accès en cas d'hébergement direct par le fournisseur d'accès. A charge pour ces derniers de réaliser les surveillances précisées plus haut.

[Rz 195] Ces obligations permettront aux autorités judiciaires d'identifier les auteurs qui enfreignent le droit de la propriété intellectuelle, le droit d'auteur et le droit à l'image ainsi que les infractions l'article 24 de la loi du juillet 1881.

2.4. Les opérateurs télécom

[Rz 196] La loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales instaure l'obligation pour les opérateurs de télécommunication de conserver les données relatives à une communication des abonnés, pour une durée maximum d'une année. Ces données ne concernent en rien le contenu des échanges, mais visent plutôt à identifier les individus.

[Rz 197] Ils encourent la même peine que les FAI.

2.5. Les prestataires en cryptologie

[Rz 198] La loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne modifiant l'article 11-1 de la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications prévoit l'obligation, pour les personnes physiques ou morales fournissant des prestations de cryptologie, de remettre aux autorités judiciaires en charge d'une mission d'interception des correspondances échangées par la voie des télécommunications, les contenus des échanges cryptés ou doivent permettre le déchiffrement des données. Cette obligation concerne également les éditeurs de logiciels de chiffrement.

[Rz 199] La peine encourue en cas de non-respect de ces obligations est de deux ans d'emprisonnement et 30'000 euros d'amende.

B. Les acteurs internationaux et la nécessaire coopération internationale

[Rz 200] La lutte contre la cybercriminalité passe nécessairement par une coopération internationale. La direction centrale de la police judiciaire (DCPJ) est dotée d'une division des relations internationales (DRI) étant en charge de coordonner la coopération policière opérationnelle qui était jusqu'alors disséminée en plusieurs entités.

[Rz 201] Cette division internationale a créé une composante, la section centrale de coopération opérationnelle de police (SCCOPOL) qui constitue l'organe central national chargé de la coopération opérationnelle internationale de police. La SCCOPOL regroupe les trois canaux institution-

nels de la coopération opérationnelle policière internationale auxquels la France participe, à savoir Interpol, Schengen et Europol.

[Rz 202] Interpol étant la coopération policière la plus ancienne, nous la traiterons en premier lieu.

1. Interpol

[Rz 203] De son appellation française Organisation Internationale de Police criminelle (OIPC), Interpol est une organisation internationale créée en 1923 dans le but de promouvoir la coopération policière internationale, plaçant ainsi un bureau central national dans différents pays. Par arrêté ministériel du 18 décembre 1928, la France crée et place à la direction centrale de la police judiciaire (DCPJ) le Bureau central national (BNC) d'Interpol qui sera situé dans la ville de Lyon.

[Rz 204] Le rôle d'Interpol est donc de faciliter pour les pays membres la lutte contre toute forme de criminalité et plus particulièrement pour le cas qui nous intéresse, la lutte contre la criminalité informatique.

[Rz 205] En pratique, le BNC France réceptionne, analyse et diffuse les demandes des pays-membres d'Interpol, ainsi que celles émanant des services français à destination de l'étranger, soit plus 120'000 messages qui transitent ainsi chaque année.

[Rz 206] Nous pouvons citer l'opération de police judiciaire « Cathédrale »[28], lancée en 1998, qui a permis le démantèlement d'un réseau diffusant plus de 750'000 clichés de pornographie enfantine et qui s'est traduite par l'arrestation de 107 personnes dans 12 pays. Il convient également de souligner les efforts d'Interpol en vue de constituer une base de données d'images pédophiles, grâce au logiciel « excalibur » d'analyse et de comparaison automatique par le contenu.

2. Europol

[Rz 207] Europol est une agence européenne ayant pour objectif la lutte contre la criminalité organisée dès lors que deux Etats membres de l'Union européenne ou plus sont concernées. Le domaine de compétence d'Europol couvre toutes les formes graves de criminalité transfrontalière et le terrorisme. Son siège est situé à La Haye (Pays-Bas) et chaque Etat membre dispose d'un correspondant unique.

[Rz 208] La SCCOPOL s'est dotée d'une unité nationale Europol (UNE), ayant pour principale mission l'échange d'informations opérationnelles et stratégiques en provenance de la France et des Etats membres ; d'offrir un soutien opérationnel d'implication des analystes d'Europol ; de valoriser l'information par la confrontation des données dans le Système d'Information d'Europol et la base d'indexation des fichiers d'analyse d'Europol ; d'offrir un soutien aux enquêtes par la traduction en langue française des rapports analytiques opérationnels et stratégiques produits par Europol à destination des services répressifs et enfin de former des enquêteurs français aux différentes applications mises à disposition par Europol.

[Rz 209] Europol a créé en 2013 un centre européen de lutte contre la cybercriminalité, dénommé EC3. Ce centre compte se focaliser sur trois axes, les crimes de haute technologie (cyberattaques,

[28] Source : le guide méthodologique « traitement judiciaire de la cybercriminalité », Direction des affaires criminelles et des grâces du Ministère de la justice.

logiciels malveillants), l'exploitation sexuelle des enfants en ligne et les fraudes aux moyens de paiements.

[Rz 210] Les opérations menées ont déjà données lieux à des arrestations que nous pouvons citer. L'arrestation de 29 suspects qui avaient réalisé un bénéfice de 9 millions d'euros en détournant les codes de paiement de 30'000 titulaires de carte bancaire[29].

[Rz 211] 59 arrestations dans plusieurs États membres menant au démantèlement de deux ateliers illégaux produisant des dispositifs de manipulation des terminaux de paiement et à la saisie d'équipements électroniques illégaux, de données financières, de cartes de paiement contrefaites et d'espèces, faisant 36'000 victimes titulaires de cartes bancaires/de crédit dans 16 pays de l'union européenne.

[Rz 212] 117 arrestations pour 200 transactions frauduleuses d'achat de billet d'avion suite au détournement de cartes de crédit.

3. Système d'information SCHENGEN

[Rz 213] La convention d'application de l'accord de Schengen signée le 19 juin 1990 est entrée en vigueur en France le 26 mars 1995. Elle prévoit, entre autres, la suppression des contrôles aux frontières intérieures et plusieurs outils destinés au renforcement de la coopération policière dans les 28 pays ayant ratifié l'accord. Il faut désormais compter quatre membres associés. L'Islande et la Norvège depuis 1999, la Suisse depuis 2008 et le Liechtenstein depuis 2011.

[Rz 214] Pour pallier aux conséquences de l'accord de Schengen, a été mis en place un fichier informatisé commun aux Etats membres, composé des fichiers nationaux, dénommé système d'information Schengen (SIS). Ce fichier constitue de façon très concrète une nouvelle « frontière électronique dématérialisée » et est composé d'environ 500'000 terminaux d'interrogation dans chacun des Etats membres de l'union. Il faut compter depuis 2011 le Royaume-Uni et l'Irlande pour ce qui concerne uniquement la coopération au SIS.

[Rz 215] En France, cette coopération est mise en œuvre par une unité centrale de coopération policière internationale (UCCPI).

[Rz 216] Un rapport d'étude remis à la ministre de la justice en juin dernier, préconise de créer un « Schengen du numérique » visant à renforcer la coopération actuelle sur le plan de la cybercriminalité. Ce rapport préconise la création d'un centre d'alerte et de réaction face aux attaques informatiques, de renforcer les peines lorsque des infractions seront commises en rapport avec des mineurs, notamment de suspendre la connexion Internet de l'auteur de contenus, tant en France qu'à l'étranger, et de veiller à l'application de la décision.

[Rz 217] Mais également des dispositions visant à sensibiliser au maximum les utilisateurs et les entreprises de l'utilisation des réseaux de communication et les risques en matière pénale, en tant que victime mais également aux risques en tant qu'auteur d'infraction.

[29] Europa.eu (presse).

IV. Conclusion

[Rz 218] Il est incontestable que les pouvoirs publics, en un peu moins de vingt ans, ont répondu à cette nouvelle forme de criminalité. On l'aura vu, les lois se sont renforcées créant tout un dispositif pénal désormais adapté. La jurisprudence est venue compléter les vides juridiques et problème d'interprétation des textes. Toutefois, les chiffres montrent que la cybercriminalité ne cesse d'augmenter, les victimes étant de plus en plus nombreuses.

[Rz 219] L'arsenal répressif et les coopérations internationales sont-ils des moyens suffisants pour enrayer la machine criminelle qui se développe sur Internet ? Ce n'est pas certain !

[Rz 220] Une étude de juin 2014, réalisée par la division de sécurité Intel[30], chiffre à 800 millions le nombre de victimes impliquées dans des attaques numériques.

[Rz 221] Selon cette étude, l'économie numérique mondiale génèrerait 2 à 3000 milliards de dollars et la cybercriminalité s'emparerait de 15 à 20% de cette économie. La cybercriminalité se placerait derrière le crime international et le trafic de drogue avec un impact sur le PIB de 0,8%.

[Rz 222] Toujours selon l'étude, les entreprises des pays développés du G20 seraient considérablement impactées, le secteur bancaire victime de piratage (pertes de données bancaires mais également compte bancaire dévalisé), le secteur pétrolier pour le vol de données d'extraction pétrolière, les pertes en propriété intellectuelle et désavantages commerciaux. Au total, l'étude chiffre à 375 et 575 milliards de dollars le coût de la cybercriminalité pour les entreprises et les individus.

[Rz 223] La cybercriminalité ne cessera d'évoluer. En effet, les pays émergents vont voir l'accès à l'Internet se développer rapidement, notamment en Asie du Sud-Est, en Afrique et en Amérique du Sud. Une nouvelle forme de criminalité va se former sur Internet dans le domaine du grand banditisme, relative aux trafics de stupéfiants, à la vente d'armes, au vol de coordonnées de paiement ou encore à l'exploitation des enfants. Les réseaux mobiles vont également être privilégiés, permettant ainsi la mondialisation de la cybercriminalité en facilitant le déplacement des criminels.

[Rz 224] On l'aura compris, les Etats devront en faire encore plus. Mettre en place des normes de sécurité mondiales en privilégiant une stratégie de lutte globale, notamment pour connaître davantage la cybercriminalité. A commencer par les entreprises, qui devront protéger les résultats de R&D, de propriété intellectuelle et de façon généralisée tous les secteurs économiques devront protéger leurs données et sécuriser davantage les accès aux systèmes, car la cybercriminalité ne cessera de progresser.

[Rz 225] Il faudra également informer les internautes sur toutes les dérives que l'on a observées et ils devront à leur tour devenir acteurs de leur propre sécurité, d'une part, et de la sécurité générale, d'autre part, avec, pourquoi pas, à leur charge une mission de service public au nom de l'intérêt général.

[Rz 226] Le frein à la cybercriminalité sera nécessairement international et généralisé à tous les acteurs de la société.

Madame Koumba Koné, titulaire d'un Maîtrise en droit pénal, mention carrières judiciaires et

[30] « Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II » (www.silicon.fr).

sciences criminelles (2005) et du Master Droit des Nouvelles Technologie (2006) de l'Université Paris Nanterre la Défense — France, sous la Direction de Madame Sylvia Preuss-Laussinotte. Juriste spécialisée en droit des NTIC et Propriété intellectuelle auprès de différents cabinets d'avocat en France (2006—2010), puis responsable des Affaires juridiques Propriété Intellectuelle à la Direction de la recherche de l'Université Paris Nanterre la Défense (2010—2012) et Juriste chargée du portefeuille de Propriété Intellectuelle auprès de l'Institut Polytechnique de Grenoble (depuis 2012).

L'auteure est également consultante en droit des nouvelles technologies auprès du cabinet KONÉ & Associés.

Tous les sites Internet ont été consultés en octobre 2014.