L'applicabilité de la loi pénale à l'endroit de la cybercriminalité dissimulée.

Nadir Ouchene

UNIVERSITÉ PARIS II PANTHÉON-ASSAS
DROIT – ÉCONOMIE – SCIENCES SOCIALES
ÉCOLE DOCTORALE DE DROIT PRIVÉ

Thèse de doctorat

Pour obtenir le grade de

DOCTEUR EN DROIT DE L'UNIVERSITÉ PARIS II PANTHÉON-ASSAS

Discipline: Droit pénal

Présentée et soutenue publiquement le lundi 10 décembre 2018 par

Monsieur Nadir OUCHENE

L'APPLICABILITÉ DE LA LOI PÉNALE À L'ENDROIT DE LA CYBERCRIMINALITÉ DISSIMULÉE

Directeur de thèse

Monsieur Francis BALLE
Professeur émérite à l'Université Paris II Panthéon-Assas (Paris II), Directeur de l'Institut d'études et de recherches sur la communication

Membres du jury

Monsieur Jean-Marie COTTERET
Professeur à l'Université Paris I Panthéon-Sorbonne

Monsieur Bernard VALADE
Professeur à l'Université Paris-Descartes

Madame Valérie DEPADT
Maître de Conférences HDR à l'Université Paris XIII Villetaneuse

Monsieur Jean-Yves MARÉCHAL
Maître de Conférences HDR à l'Université Lille II, codirecteur de l'Institut de criminologie de Lille

La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

Je remercie chaleureusement toutes les personnes qui m'ont aidé pendant l'élaboration de ma thèse et notamment mon directeur Monsieur le Professeur Francis BALLE, pour ses conseils avisés dans la conduite et la poursuite de mes travaux.

Au terme de ce parcours, je remercie également celles et ceux qui me sont chers. Leurs attentions et encouragements m'ont accompagné tout au long de ces années. Je suis redevable à mon père et mes sœurs, pour leur soutien moral et leur confiance indéfectible dans mes choix. Enfin, j'ai une pensée toute particulière pour mon oncle, ma tante et mes amis.

Principales abréviations

ANASSI : Agence nationale de sécurité des systèmes d'information.

Arpanet Advanced Research Projects Agency Network.

BEFTI Brigade d'enquêtes sur les fraudes aux technologies de l'information.

CIA *Central Intelligence Agency*.

CNIL Commission nationale de l'informatique et des libertés.

Cour EDH Cour européenne des droits de l'homme.

CESDH Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales

CJUE Cour de justice de l'Union européenne.

CREDOC Centre de recherche pour l'étude et l'observation des conditions de vie.

DDHC Déclaration des Droits de l'Homme et du Citoyen de 1789.

ENISA European Union Agency for Network and Information Security

Ibid. Référence identique à la précédente.

ICANN *Internet Corporation for Assigned Names and Numbers*.

IRCGN Institut de recherche criminelle de la Gendarmerie nationale.

JORF Journal officiel de la République Française.

LCEN Loi pour la confiance dans l'économie numérique.

MIT Massachusetts Institute of Technology.

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

ONU Organisation des Nations unies.

Op. cit. Opere citato (référence d'ouvrage ou d'article précité).

QPC Question prioritaire de constitutionnalité.

RGPD Règlement général sur la protection des données.

SDLC Sous-direction de lutte contre la cybercriminalité.

STAD Système de traitement automatisé de données.

TGI Tribunal de grande instance.

TOR *The Onion Router*.

GLOSSAIRE

- A -

Adresse IP (Internet Protocol) : Sur Internet, chaque ordinateur est identifié par une adresse numérique, appelée IP, composée d'une suite de quatre nombre séparée par des points. (Ex. : 134.238.47.381).

Adresse URL (Uniform Resource Locator) : Ce terme désigne une méthode d'adressage uniforme de l'information sur Internet, permettant de retrouver un document grâce à l'indication du protocole d'accès au serveur (http, ftp…)

- B -

Big data : La notion de *Big Data* désigne littéralement un ensemble de données massives quasi infinies correspondant à des informations publiées et échangées par les internautes.

Bitcoin : Il s'agit d'une monnaie utilisée sur Internet, et qui fonctionne indépendamment des réseaux bancaires grâce à une décentralisation

Blockchain : Il s'agit d'une technologie de stockage et de transmission d'informations sans organe de contrôle

Botnet : Ce terme vient de la contraction des termes anglais « *robot* » et « *network* ». Ce sont des réseaux de bots informatiques connectés à un réseau Darknet ou à Internet communiquant entre eux afin d'exécuter certaines tâches pouvant être légitimes.

- C -

Cheval de Troie : Programme informatique malveillant comprenant, en plus de ses fonctions officielles et connues, d'autres fonctions, inconnues de l'utilisateur qui consulte à son insu les données inscrites dans le programme de son ordinateur afin d'en prendre le contrôle.

Chiffrement : Le chiffrement ou cryptage est une technique de cryptographie qui permet de limiter la lecture d'un document en l'autorisant qu'aux personnes détentrices de la clé de déchiffrement. Cela permet donc de modifier des données afin de protéger la transmission et la réception des informations dont elles sont porteuses.

Cloud : Il s'agit de services informatiques permettant le stockage de données via Internet.

CNIL : Créée par la loi « *Informatique et libertés* » du 6 décembre 1978 la Commission nationale de l'informatique et des libertés est une autorité administrative indépendante française dont la vocation est de protéger le statut des données personnelles et le droit à la

vie privée face aux risques croissants d'atteintes aux libertés résultant des moyens informatiques.

Cracker : Issu du terme anglais « crack » qui signifie craquer, le mot « *cracker* » désigne les spécialistes du cassage de codes en tout genre. Le terme peut aussi désigner un cryptanalyste dont la spécialité est le cassage de code crytographique

Cryptomonnaie : Il s'agit d'une monnaie utilisable sur un réseau informatique décentralisée peer-to-peer.

Cryptowar : Guerre de la cryptographie opposant les Etats-Unis et d'autres Etats étrangers aux adaptes du chiffrement. Les premiers ont tenté de limiter l'accès du public aux méthodes de chiffrement afin de pouvoir opérer une surveillance mondiale des moyens de communications.

Cyberespace : Il s'agit d'un espace virtuel dont l'accès est possible grâce à une connexion et qui permet d'exercer certaines activités.

Cypherpunks : Le terme « *cypher* » signifie chiffrement. Les Cypherpunks sont des activistes de la cryptographie croyant au respect de la vie privée pour tous.

- D -

Deep Web : le *Deep Web* est le Web accessible librement mais non indexé par les moteurs de recherche.

Darknet : Un darknet est un réseau privé anonyme mis en place entre pairs de confiance. Ce type de réseau, pouvant être établi par une large communauté ou par un petit nombre d'utilisateurs, n'est pas accessible par les logiciels et les protocoles usuels. Le protocole technique pour accéder à un darknet est très simple et les utilisateurs ne trouvent que ce qu'ils sont venus chercher en raison de l'absence de moteur de recherche. Les darknets désignent les infrastructures tandis que le Darkweb désigne le contenu.

DOS : Les attaques DoS ou par « *déni de service* » sont des cyberattaques qui visent à rendre indisponible un service en l'inondant de requêtes. Il s'agit alors de bloquer un serveur de fichiers, un site web ou la distribution de courriel.

Défacement : Il s'agit de la modification non sollicitée de la présentation d'un site web à la suite du piratage de ce site

Déréférencement : Il s'agit de l'opération par laquelle un distributeur supprime un produit des références qu'il commercialise.

- E -

Éditeur : Il s'agit de la personne « dont l'activité est d'éditer un service de communication au

public en ligne.

Europol : Il s'agit de l'agence européenne de police criminelle qui facilite l'échange de renseignements entre polices nationales en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédophilie au sein de l'Union européenne.

- F -

Friend-to-friend (ami à ami ou F2F) : Les réseaux « *d'ami à ami* » ou F2F sont des *« peer to peer* » particuliers qui n'utilisent des connexions directes qu'entre personnes de confiance. D'autres connexions indirectes sont possibles, mais sans que que l'identité des utilisateurs soient dévoilées dans la mesure où un F2F permet un échange automatique et anonyme des fichiers.

- G -

GAFA : L'acronyme GAFA désigne les grandes entreprises *Google*, *Apple*, *Facebook* et *Amazon*.

- H -

Hackeur : Il s'agit d'un Hackeur qui utilise ses connaissances pour démonter des programmes informatiques. Le terme est issu du verbe anglais « *to hack* », qui signifie « *hacher* ».

Hacktivisme : Intimement lié au cybermilitantisme et issu des termes « *hacker* » et « *activisme* », l'hacktivisme désigne le militantisme pratiqué par les hackers. Ainsi, les hacktivistes s'attaquent aux réseaux afin de défendre leurs convictions politiques ou religieuses.

Hébergeur : Personne qui effectue un hébergement de sites c'est-à-dire un service consistant à accueillir les pages web personnelles de personnes privées ou de petites entreprises et à leur offrir ainsi une plus large visibilité.

Hidden Wiki : Le « *Wiki caché* » est un Wikipédia référençant les services cachés du Darknet.

- I -

ICANN : L'ICANN ou *Internet Corporation for Assigned Names and Numbers* est une organisation de droit privé à but non lucratif créée en novembre 1998 et chargée de la gestion des noms de domaine d'Internet au niveau mondial.

IMSI catcher : Littéralement ce terme donne « attrape-IMSI » . Un IMSI est « *International Mobile Subscriber Identity* » c'est-à-dire un numéro de téléphone. Ainsi, le IMSI catcher permet d'intercepter les données transmises par le biais d'un téléphone portable.

Internet : Réseau informatique mondial.

Interpol : L'Organisation internationale de police criminelle est une organisation internationale afin de promouvoir la coopération policière internationale.

- M -

Malware : Un *Malware* ou logiciel malveillant permet de nuire à un système informatique sans le consentement de l'utilisateur

- N -

Nom de domaine : Sur le réseau Internet, chaque ordinateur est identifié par une adresse numérique appelée adresse IP. Afin de pouvoir accéder au contenu des pages d'un site Internet, l'utilisateur doit taper l'adresse IP du site dans un logiciel de navigation. Pour faciliter la mémorisation des sites et mieux identifier les contenus correspondant aux adresses IP, ces dernières ont été doublées par des adresses symboliques alphanumériques. Ces dernières sont les noms de domaines et sont composées d'un préfixe technique (www), d'un radical et d'un suffixe (.com ou .fr par exemple) : www.radical.suffixe.

- P -

Peer-to-peer (pair à pair ou P2P) : Expression employée pour désigner l'échange de fichiers informatiques, via Internet, sans transit par un serveur.

PGP : *Pretty Good Privacy* signifie assez bonne confidentialité. Ce logiciel de chiffrement est créé en 1991 par Philip Zimmermann.

- S -

Silkroad : Il s'agit d'un marché de produits illégaux mis en place sur le Darknet en 2011.

- T -

TCP/IP : De l'anglais *Transmission Control Protocol over Internet Protocol*. Cela désigne l'ensemble des protocoles communs de communication permettant l'interconnexion généralisée entre réseaux hétérogènes.

Token : Ce sont des jetons numériques qui permettent les échanges sécurisés de droits financiers, politiques ou d'usage.

- U -

URL : Il s'agit d'une méthode d'adressage uniforme de l'information sur internet, permettant de retrouver un document grâce à l'indication du protocole d'accès du serveur, du nom du

serveur où se trouve le document et de la référence du document, ces éléments étant séparés par des points.

- V -

Virus : Série de codes créés pour infecter du contenu ou perturber le fonctionnement d'une machine.

VPN : Réseau virtuel privé qui permet de créer un lien entre des ordinateurs distants).

- W -

Web : Ce terme est utilisé comme abréviation de World Wild Web c'est-à-dire « *toile d'araignée mondiale* ». Il s'agit en réalité de l'un des protocoles d'Internet.

UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

SOMMAIRE

« ***L'essentiel est invisible pour les yeux.*** »[1]

Antoine de Saint-Exupéry

[1] Antoine de Saint-Exupéry, *Le Petit Prince*, Gallimard, 18 juin 2000.

INTRODUCTION

Selon l'enquête du CREDOC[2] réalisée en 2015 pour le Conseil Général de l'Economie et l'Autorité de Régulation des Communications Électroniques et des Postes, huit français sur dix disposent d'un ordinateur à domicile, ce taux passe à 97% pour les 12-17 ans et à 91% pour les 18-24 ans. En 2018 ces chiffres se sont accentués dans la mesure où aujourd'hui 73% des français possèdent un smartphone, et 85% ont accès à Internet[3].

Néanmoins, les systèmes d'information offrent de grandes possibilités aux personnes malveillantes, qui s'en prennent ainsi aux internautes les plus vulnérables. Les cibles potentielles peuvent être les enfants ou les personnes âgées mais aussi les administrations et les entreprises privées. Principal axe de la cybercriminalité, Internet a donc révolutionné le comportement de la majorité des français, au point de devenir universel en n'étant plus réservé aux seules relations professionnelles. Véritable espace de liberté, il supprime les frontières et permet des multitudes d'échanges.

Dans ce contexte, la frontière entre ce qui est illégal et légal est influencée par le contexte social dans lequel la société se développe. La morale varie selon la culture et le contexte d'une époque et d'un pays. Un acte peut être déviant par rapport à la morale, sans pour autant l'être par rapport à la loi. En revanche la définition de ce qui est licite ou non dépend de la loi applicable dans le pays concerné.

De manière générale, le droit national et le droit international reconnaissent comme étant illégales la plupart des atteintes aux personnes, aux organisations et aux Etats, qu'elles soient commises sur Internet ou non. Toutefois, l'ubiquité permise dans le monde virtuel d'Internet complique fortement la tâche des autorités quant à la détermination des règles de compétences législatives et juridictionnelles. Les États se sont demandés s'il fallait adapter à la cybercriminalité les règles de droit commun ou s'il fallait adopter des règles spécifiques. La

[2] Centre de recherche pour l'étude et l'observation des conditions de vie.
[3] COEFFE T., *Baromètre du numérique 2017 : équipement, usages et compétences numériques des Français*, 28 novembre 2017.
Disponible sur : https://www.blogdumoderateur.com/barometre-numerique-2017-france/, [consulté le 11 décembre 2017].

difficulté réside dans le fait qu'une infraction commise sur Internet est intrinsèquement internationale contrairement aux règles de procédure prévues par le droit national. De plus, cette notion de cybercriminalité n'est pas définie et ne cesse d'évoluer.

En effet, les cybercriminels ont migré vers un nouvel endroit qui leur permet d'agir avec un réel sentiment d'impunité grâce à des techniques de chiffrement et d'anonymisation. Les termes « *Darknet », « Deep Web », « Darkweb », « Web profond » ou encore « Web dissimulé »* sont utilisés pour désigner le nouveau terrain de jeu des pédophiles, pirates informatiques, terroristes et trafiquants de drogue. En réalité ces termes ont des significations différentes qu'il conviendra de préciser. Une fois tous ces aspects pratiques présentés, il conviendra de montrer quel arsenal juridique permet d'appréhender ces phénomènes.

Mais avant tout développement, l'étude de l'applicabilité de la loi pénale à l'endroit de la cybercriminalité dissimulée suppose de définir d'une part, l'applicabilité de la loi pénale (Section 1) et d'autre part, la cybercriminalité dissimulée (Section 2).

SECTION 1
L'applicabilité de la loi pénale

Créé afin de canaliser la vengeance privée, le droit criminel a été imposé par des corps sociaux prééminents capables d'édicter des règles. Sa singularité provient du fait qu'il s'agit d'une discipline politique ayant vocation à organiser la société face à la criminalité qui ne cesse d'évoluer.

Le droit criminel aborde son objet principal, la criminalité, à travers une représentation juridique qui est l'infraction, un comportement antisocial. Toutefois, l'étude de la criminalité est nébuleuse puisqu'il faut être en mesure d'identifier la personne qui a commis le crime. Dans ce contexte, le droit pénal semble parfois démuni puisqu'il est impossible de reconnaître l'ensemble de la criminalité réelle. Un tel phénomène s'accentue sur le web et notamment sur le web dissimulé.

De plus, il n'est pas possible de poursuive un crime sans connaître son auteur. Dès lors, le droit criminel se développe grâce à d'autres matières comme la criminologie ou les sciences criminalistiques telles que la police scientifique et la médecine légale qui ont vocation à découvrir les crimes. Face à la constante évolution et à la complexité de la criminalité, le droit pénal doit s'adapter et s'entourer de ces autres matières ; c'est ce qui s'est passé avec la cybercriminalité.

Le droit pénal décrit et sanctionne le phénomène criminel caractérisé par des comportements antisociaux. Ainsi, il organise la répression par l'Etat et sanctionne des comportements déterminés ; soit un agissement positif, soit un agissement négatif tel qu'une omission ou une abstention.

Ensuite, il y a la procédure pénale qui est une démarche pénale qui commence lors de la commission de l'infraction et qui se termine lorsque la peine est exécutée. Elle est composée de différentes étapes : l'enquête, l'instruction, le jugement, les voies de recours, et enfin l'exécution des sanctions. Lors de ces diverses phases, la personne mise en cause est désignée de différentes manières. Le suspect désigne l'individu qui fait l'objet d'une enquête, le mis en examen celui qui fait l'objet d'une instruction et le prévenu désigne l'individu qui fait l'objet

de poursuite pour un délit ou une contravention lors de la phase de jugement tandis que l'accusé l'individu qui est renvoyé devant la Cour d'Assises pour un crime.

Par ailleurs, il existe le droit pénal spécial qui n'étudie que les infractions unes par unes et la criminologie qui étudie les causes de l'infraction et la personne du criminel. L'étude de la cybercriminalité dissimulée permet d'envisager ces quatre disciplines.

En France, pour qu'une répression soit envisageable, il faut un texte la prévoyant, et le plus souvent que l'infraction ait un lien avec la République, c'est le principe de légalité criminelle souvent synthétisé par la formule latine du 19ème siècle : « *nullum crimen, nulla poena sine lege* » (§1). Lorsqu'un texte prévoit une infraction, l'individu pourra être condamné s'il a sciemment accompli concrètement et matériellement ce qui est abstraitement prévu par la loi (§2).

§1) La légalité criminelle

Le principe de légalité criminelle est inscrit dans la Déclaration des droits de l'homme et du citoyen de 1789, dans le Code pénal français et consacré par la CESDH ainsi que par le Pacte international sur les droits civils et politiques (A).

Par ailleurs, le thème des sources du droit pénal reste essentiel dans la matière répressive dans la mesure où la mise en œuvre du droit pénal touche aux libertés individuelles. Tous les citoyens ont des droits et la rigoureuse procédure pénale française ne facilite pas toujours le travail des enquêteurs, dans un contexte faisant la part belle aux truands. La lutte contre la criminalité dissimulée amène à se demander quel est le prix à payer pour lutter de manière efficace contre les comportements antisociaux. De plus, la loi n'étant ni atemporelle, ni universelle, le juge répressif doit veiller à ce que les faits poursuivis entrent bien dans le champ d'application de la loi pénale, en prenant en compte le moment et le lieu où ils ont été commis (B).

A) Le principe de légalité criminelle

Les constituants révolutionnaires, marqués par l'esprit du siècle des Lumières, ont érigé le principe de la légalité des délits et des peines au rang de principe fondamental et ce, afin de

mettre un terme au caractère arbitraire de la législation pénale de l'Ancien Régime. Désormais, il faut connaître les règles par avance. Ainsi, aux termes de l'article 5 de la Déclaration des Droits de l'Homme et du Citoyen du 27 août 1789, « *tout ce qui n'est pas défendu par la loi ne peut être empêché et nul ne peut être contraint de faire ce qu'elle n'ordonne pas* ». Quant à l'article 8 il prévoit que « *la loi ne peut établir que des peines strictement et évidemment nécessaires et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit et légalement appliquée* ». Originellement, le respect du principe de légalité supposait que les incriminations et les peines fussent définies de manière précise par un texte écrit qui ne pouvait être qu'une loi *stricto sensu* (1). Mais ce principe a également des conséquences pour les différents acteurs pénaux (2).

1. Les origines du principe de légalité criminelle

Le principe de légalité criminelle est consacré au 18ème siècle par Beccaria qui estime que « *les lois seules peuvent faire les peines de chaque délit et ce pouvoir ne peut résider que dans la personne du législateur qui représente toute la société unie par un contrat social*[4] ». On retrouve à la même période une idée semblable chez Montesquieu qui estime que « *le juge n'est que la bouche qui prononce et applique les paroles de la loi*[5] ».

Ce principe se subdivise en deux propositions. D'une part, il y a le principe de textualité selon lequel nul ne peut être poursuivi qu'en vertu d'un texte de droit préexistant à son acte[6]. D'autre part, il y a la légalité *stricto sensu*, qui veut que le texte de droit préexistant soit nécessairement une loi au sens formel du terme, c'est-à-dire un acte émanent du parlement[7]. Pour la CESDH[8], le principe de légalité ne doit pas être entendu uniquement dans un sens formel mais aussi dans un sens matériel c'est-à-dire avec la nécessité pour toute norme pénale même non écrite d'être conforme à un double principe de qualité. Premièrement, elle doit être claire et accessible. Secondement, elle doit être mesurée, c'est la proportionnalité.

En outre, le principe de légalité repose sur deux fondements particulièrement solides. L'un,

[4] BECCARIA C., *Des délits et les peines*, 1764.
[5] MONTESQUIEU, *Les Lettres Persanes*, 1721.
[6] Code pénal art. 111-3.
[7] Constitution art. 34.
[8] Pour cette raison elle est critiquée par une partie de la doctrine et notamment par le Professeur Conte.

politique, tenant à la souveraineté de la loi, expression de la volonté générale. Il permet d'asseoir le droit de punir. L'autre, plus philosophique, qui fait de la légalité criminelle le moyen d'éviter l'arbitraire et de garantir l'égalité devant la répression en avertissant chacun des frontières du permis et de l'interdit. Ainsi, le principe de légalité criminelle a des conséquences pour les différents acteurs du système juridique (2).

2. Les conséquences pour les acteurs du système juridique

Le principe de légalité criminelle a des conséquences pour le législateur ou l'autorité règlementaire (a) ainsi que pour les magistrats (b).

a) Les conséquences pour le législateur ou l'autorité règlementaire

Le législateur est tenu de rédiger des textes clairs et précis (∂) et de respecter le principe de non-rétroactivité de la pénale (ß) qui est l'un des corollaires du principe de légalité. En effet, une personne ne peut être sanctionnée que si le jour des faits son comportement était incriminable.

∂) L'obligation de rédiger des textes clairs et précis

Pour être garant des libertés individuelles et de la sécurité juridique, le principe de légalité des délits et des peines contraint le législateur à définir de manière claire et intelligible les comportements prohibés et les peines qui y sont attachées afin d'éviter l'arbitraire du juge[9]. L'idée est que celui qui commet un acte doit avoir connaissance du caractère délictueux de son acte au moment de sa commission. Cette connaissance effective est garantie par une fiction de connaissance de la loi selon laquelle « *nul n'est censé ignorer la loi* ». Dès lors, il est nécessaire que la loi soit claire, accessible et prévisible. Cette contrainte a valeur constitutionnelle puisqu'elle est prévue à l'article 8 de la Déclaration des droits de l'homme de 1789. C'est d'ailleurs sur ce fondement que le Conseil constitutionnel a précisé la portée du principe de légalité dans sa décision Sécurité et Liberté de 1981: « *aux termes de l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789, nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit et légalement appliquée qu'il en résulte*

[9] DEBOVE F., *L'overdose législative*, Droit pénal, LexisNexis, 2004.

la nécessité pour le législateur de définir les infractions en termes suffisamment clairs et précis pour exclure l'arbitraire ». Ainsi, les dispositions législatives qui ne déterminent pas l'auteur de l'infraction de manière certaine ou qui prévoient des infractions avec des éléments constitutifs qui ne sont ni clairs ni précis, seront invalidées[10]. En outre, la Cour EDH contraint elle aussi le législateur à voter des lois suffisamment accessibles et précises afin que le citoyen sache quelles normes juridiques seront applicables à telles situations. Elle l'exige indirectement sur la base de son article 7 : « *Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou international. De même il n'est infligé aucune peine plus forte que celle qui était applicable au moment où l'infraction a été commise* ».

Dès lors, pour les crimes et délits le juge pénal peut écarter un texte qui ne respecterait pas l'obligation prévue par l'article 7 de la CESDH par le biais du contrôle de conventionnalité. En effet, depuis l'arrêt « *Société des cafés Jacques Vabre*[11] », les juridictions judiciaires sont compétentes pour vérifier la conformité de la loi interne par rapport aux normes communautaires. Cela permet donc d'écarter un texte d'incrimination qui manquerait de clarté ou de précision, ce qui est en pratique très rare. Concernant l'appréciation de la constitutionnalité d'une loi, c'est le Conseil constitutionnel qui est compétent mais le mécanisme de la question prioritaire de constitutionnalité prévu par l'article 61-1 de la Constitution permet d'envisager ce contrôle si une loi manque de lisibilité et de clarté. En matière contraventionnelle, les infractions sont prévues par les règlements, le contrôle peut alors s'effectuer par le biais de l'exception d'illégalité.

En outre, la question de l'application de la loi pénale dans le temps suppose une infraction, une loi nouvelle et un magistrat. Ce dernier se demande s'il doit appliquer la loi nouvelle ou la loi ancienne. De plus, il faut regarder s'il s'agit d'une loi pénale de fond ou de forme. Ces dernières s'appliquent de manière immédiate puisqu'elles n'ont en principe aucune incidence sur la répression. Quant aux loi pénales de fond, il faut regarder si elles sont plus douces ou plus sévères (ß).

[10] Conseil constitutionnel, 19 et 20 janvier 1981, décision n° 80-127 DC ; Conseil constitutionnel, 25 février 2010, décision n° 2010-604. De plus le Conseil constitutionnel a abrogé l'article 222-33 du Code pénal qui ne définissait pas suffisamment les éléments constitutifs du délit de harcèlement sexuel : Conseil constitutionnel, 4 mai 2012, décision n° 2012-240 QPC.
[11] Cour de cassation, chambre mixte Cour de cassation, 24 mai 1975, n°73-13556.

ß) Le principe de non-rétroactivité de la loi pénale nouvelle.

L'article 112-1 du Code pénal dispose que « *seules sont punissables les faits constitutifs d'une infraction à la date à laquelle ils ont été commis* » et que « *peuvent seules être prononcées les peines légalement applicables à la même date* ». Par conséquent, les faits commis antérieurement à un nouveau texte seront soumis à la loi qui était en vigueur au moment de la commission de l'infraction.

Cet article s'applique pour les lois pénales de fond. Une loi pénale de fond peut être une loi d'incrimination qui définit une infraction[12], une loi de pénalité qui fixe une sanction, une loi qui est relative à la responsabilité pénale comme la loi modifiant le régime de la tentative[13] ou une loi qui est relative aux immunités[14] : c'est l'élément légal de l'infraction. Elle sera applicable de sa promulgation au Journal officiel jusqu'à son abrogation.

Il subsiste cependant des difficultés d'application. En cas de changement de loi entre la commission de l'infraction et le jugement, c'est la loi en vigueur au moment de la commission de l'infraction qui s'applique. Elle est applicable un jour franc après sa publication au Journal officiel. Les lois interprétatives qui se contentent de préciser le sens d'une loi ancienne sans y ajouter de règles de fond sont considérées en vigueur à la même date que la loi interprétée. Mais, il faut que cela soit une vraie loi interprétative au risque que les tribunaux refusent d'appliquer ces textes à des situations antérieures.

Il y a une autre difficulté lorsque l'infraction est accomplie sur une longue période de temps si bien qu'il est difficile de déterminer la date de la commission. En effet, entre le début et la fin de l'infraction des lois peuvent se succéder. En principe, la loi nouvelle s'applique si tous les éléments constitutifs de l'infraction sont accomplis sous son empire. Ainsi, il faut effectuer une distinction entre les infractions instantanées qui se consomment en un trait de temps et qui se verront appliquer la loi en vigueur au moment de l'infraction, les infractions complexes, pour lesquelles deux actes matériels différents constituent l'élément matériel, les infractions

[12] Cour de cassation, chambre criminelle, 9 novembre 1966, n° 65-93.832.
[13] Cour de cassation, chambre criminelle,19 juin 2007, Bulletin criminel n°169.
[14] Cour de cassation, chambre criminelle, 14 novembre 2007 : Bulletin criminel n°281.

d'habitude qui impliquent la réalisation de plusieurs actes, et les infractions continues dont le comportement délictueux s'étend sur la durée. Pour ces deux derniers types d'infractions, la jurisprudence admet qu'un acte commis sous l'empire de la loi nouvelle plus sévère suffit à son application.

Par ailleurs, une loi pénale nouvelle plus douce ne porte pas atteinte aux libertés individuelles et c'est la raison pour laquelle l'article 112-1 du Code pénal dispose, in fine, que « *les dispositions nouvelles s'appliquent aux infractions commises avant leur entrée en vigueur et n'ayant pas donné lieu à une condamnation passée en force de chose jugée lorsqu'elles sont moins sévères que les dispositions anciennes* ». C'est le principe de la rétroactivité « *in mitius* » d'une loi pénale nouvelle plus douce. Afin qu'il s'applique, il faut deux conditions.

D'une part, il faut que la loi nouvelle soit plus douce. Lorsqu'une loi s'avère à la fois plus douce et plus sévère, il est nécessaire d'effectuer une application distributive[15]. Dans ce cas le juge ne prend en considération que les dispositions et peines principales. Une loi pénale plus douce peut par exemple supprimer une circonstance aggravante, diminuer une peine encourue, réduire le champ d'incrimination ou même abroger une infraction.

D'autre part, il faut que la personne poursuivie n'ait pas été condamnée définitivement pour les faits poursuivis avant l'entrée en vigueur de la loi nouvelle sauf si ladite loi enlève aux faits leur caractère pénal. En effet, l'alinéa 2 de l'article 112-4 du Code pénal dispose que « *la peine cesse de recevoir exécution quand elle a été prononcée pour un fait qui, en vertu d'une loi postérieure au jugement, n'a plus le caractère d'une infraction pénale* ». Par ailleurs, certaines lois plus sévères ne sont pas visées par le principe de non-rétroactivité de la loi nouvelle. Il en va ainsi des lois interprétatives, qui précisent les dispositions d'une loi sans la modifier, des lois déclaratives, qui ne font que constater une règle existante, et des lois instituant des mesures de police et de sûreté[16].

Enfin, les lois pénales de forme s'appliquent immédiatement pour la répression de faits commis

[15] Si les dispositions sont divisibles, le juge fait rétroagir la partie la plus douce et n'applique pas la partie la plus sévère.
[16] La jurisprudence considère que leur application est immédiate, même pour des faits commis sous l'empire de l'ancienne loi, car elles permettent de faire face à un état dangereux.

avant leur entrée en vigueur. Outre leur côté pratique qui permet aux juges d'appliquer la même procédure pour des faits commis à des dates différentes, ce principe s'explique par le fait que ces lois ne portent pas atteinte aux libertés individuelles. Les différents cas sont prévus par l'article 112-2 du Code pénal. Tout d'abord, « *les lois relatives au régime d'exécution et d'application des peines » peuvent s'appliquer même si le condamné a fait l'objet d'une peine définitive toujours en cours d'exécution. Ensuite, « Les lois de compétence et d'organisation judiciaire* » et celles « *fixant les modalités des poursuites et les formes de la procédure* » sont aussi d'application immédiate aux procédures en cours, et ce pour celles de compétences et d'organisation judiciaire, « *tant qu'un jugement au fond n'a pas été rendu en première instance* ». Toutefois, n'étant pas rétroactive, la loi nouvelle n'a pas d'effet sur la réalisation d'actes antérieurs à son entrée en vigueur. Enfin, depuis la loi du 9 mars 2004, « *les lois fixant les modalités des poursuites et les formes de la procédure sont applicables immédiatement à la répression des infractions commises avant leur entrée en vigueur* ». Le principe de légalité criminelle a également des conséquences pour le juge (b).

b) Les conséquences pour le juge

En pratique, le principe de légalité contraint le juge à s'assurer que le fait poursuivi constitue bien une infraction punissable. Pour ce faire, il doit constater l'existence de tous les éléments constitutifs de l'infraction et s'assurer que la peine prononcée, principale ou complémentaire, est prévue par un texte. Il est alors tenu à une interprétation stricte du droit pénal et a la possibilité d'écarter une disposition contraire à une norme du droit international ou du droit interne si la solution du procès en dépend.

« *En matière criminelle, il faut des lois précises, point de jurisprudence* ». Cette formule proclamée par Portalis lorsqu'il présenta le Code pénal de 1810 illustre parfaitement la méfiance de l'époque à l'encontre de l'autorité judiciaire. Ainsi, inspirés par les philosophes, les constituants révolutionnaires décident qu'il appartient aux juges d'appliquer la loi sans l'interpréter. Toutefois, cette dernière étant générale et impersonnelle, elle ne peut pas tout envisager et il a fallu admettre une interprétation de la loi par le juge mais uniquement afin qu'il puisse en combler les éventuelles lacunes. Le juge doit être capable de s'écarter de la lettre de la loi lorsqu'un respect trop pointilleux du texte amènerait à des situations absurdes. Par exemple, l'article 78, 5° du décret du 11 novembre 1917 interdisait aux voyageurs « *de monter*

et de descendre ailleurs que dans les gares (…) et lorsque le train est complétement arrêté ». Ce texte imposait donc aux voyageurs de descendre lorsque le train était en marche. Cette situation étant illogique, les juges ont interprété le texte en condamnant un individu qui était descendu alors que le train était en marche, conformément à la volonté du législateur[17]. En ce sens, l'article 111-4 du Code pénal dispose que « *la loi pénale est d'interprétation stricte* », ce principe est un corollaire du principe de légalité criminelle.

La procédure législative étant trop lourde, il convient désormais d'utiliser le règlement comme source du droit pénal pour les infractions les moins graves comme le prévoit l'article 111-2 du Code pénal[18], mais aussi le droit international (B).

B) Les sources du droit pénal

La loi *stricto sensu* désigne la norme votée par le parlement après un débat public et contradictoire et promulguée par le Président de la République. Elle fixe les règles concernant « *la détermination des crimes et délits ainsi que les peines qui leur sont applicables et la procédure pénale* » comme le prévoit l'article 34 de la Constitution. En droit pénal, la principale source législative est le Code pénal issu de 4 lois du 22 juillet 1992 entrées en vigueur le 1er mars 1994 et dont la partie législative comporte 5 livres[19]. Toutefois, le Code pénal n'est pas la seule source législative du droit pénal et de nombreuses autres infractions figurent dans des lois non codifiées. En outre, certaines lois peuvent être qualifiées « *de circonstance* » en ce qu'elles sont votées à la suite de faits divers marquant spécialement l'opinion publique. Tel pourrait être le cas pour le web dissimulé, et notamment pour les infractions touchant au terrorisme qui ont connu une certaine frénésie au sein du Parlement depuis les récents attentats que la France a connus[20].

Les contraventions sont régies par le pouvoir réglementaire comme le prévoit l'article 37 de la

[17] Cour de cassation, chambre criminelle, 19 mai 1999, Bulletin criminel n° 99.
[18] Code pénal, art. 111-2, §1 : « *La loi détermine les crimes et délits et fixe les peines applicables à leurs auteurs* » ; Code pénal, art. 111-2, §2 : « *Le règlement détermine les contraventions et fixe, dans les limites et selon les distinctions établies par la loi, les peines applicables aux contrevenants* ».
[19] Les dispositions générales, des crimes et délits contre les personnes, des crimes et délits contre les biens, des crimes et délits contra la nation, l'Etat et la paix publique et des autres crimes et délits.
[20] Il y a notamment eu l'attentat contre *Charlie Hebdo* du 7 janvier 2015, l'attentat du 13 novembre 2015 et l'attentat de Nice le 14 juillet 2016.

constitution. Le terme règlement désigne la règle de droit qui émane du pouvoir exécutif et c'est donc le président de la République ou son premier ministre qui édicte par décret au conseil d'état les contraventions et les peines qui y sont rattachées. Ces dernières ne peuvent être, à titre principal, que des peines d'amende allant jusqu'à 1500 euros, hors récidive. Ce rôle du pouvoir règlementaire est défini dans le Code pénal aux article 111-2 et 111-3.

Enfin, coutume et principe de légalité criminelle semblent manifestement incompatibles. Pourtant en matière criminelle, la coutume joue un rôle effectif non négligeable. D'une part, les usages peuvent permettre de supprimer une infraction. C'est le cas pour les violences commises lors de la pratique de certains sports ou lorsque la coutume intervient par délégation de la loi. À titre d'exemple, les mauvais traitements faits aux animaux sont autorisés à certains endroits si la coutume locale le prévoit[21]. D'autre part, les usages permettent d'envisager une répression sans que le principe de légalité criminelle soit violé puisque c'est toujours sur délégation de la loi que la coutume sanctionne. Tout comme pour la coutume, la jurisprudence semble discutable en tant que source du droit pénal. Toutefois, les décisions de la chambre criminelle de la Cour de cassation sont très nombreuses et peuvent parfois être *contra legem*. Les Hauts magistrats peuvent ainsi contourner la loi dans le dessein d'influencer le législateur.

De même, lorsque la Cour EDH interprète un article de la CESDH, cette interprétation a la même force que l'article lui-même. Par conséquent, ces interprétations s'imposent aux juridictions françaises ainsi qu'au législateur lui-même, qui doit donc veiller à ne pas contredire le Conseil constitutionnel ou la Cour EDH dans un texte nouveau. En matière de QPC, le conseil constitutionnel a le pouvoir d'abroger la loi pénale. C'est pour cela qu'on parle d'une norme jurisprudentielle. C'est une révolution qui a d'autant plus d'impact que ce pouvoir de la jurisprudence s'exerce très souvent à partir de textes vagues. Les juridictions européennes ont donc un pouvoir créateur de la norme. Se présente dès lors le même problème de la légitimité des juges qu'ils créent une norme et se pose la question suivante : lorsqu'ils « *déjugent* » le législateur, que devient leur légitimité au regard de celle du législateur ? Ce pouvoir grandissant du juge constitue une révolution à la fois juridique et politique. La loi est donc désacralisée. Est-il utile de mentionner le Conseil constitutionnel au sein duquel siègent des gens politisés et non des juristes. Cette instance dont le rôle est pourtant capital ne rédige donc pas elle-même

[21] Cour de cassation, chambre criminelle, 8 juin 1994, Droit pénal 1994, commentaire n° 235.

ses solutions. Lorsque des instances comme la Cour EDH ou le Conseil constitutionnel ont été interrogés sur la question de la jurisprudence en tant que source du droit, la réponse majoritaire apportée a été que oui. Donc, ils ont de ce fait décidé d'ériger la jurisprudence comme une source concurrente de la loi. En ce sens, l'article 7 de la CESDH consacre le principe de la légalité criminelle en visant le droit et non la loi. La Cour EDH a interprété le « *droit* » comme visant à la fois le droit écrit et le droit jurisprudentiel. Il va sans dire que ce rôle reconnu à la jurisprudence comme étant une source du droit, indépendamment des interrogations politiques qu'il peut susciter, menace la sécurité juridique. En effet, en matière pénale, la loi édicte d'avance quelle sera la solution. Or, on ne peut pas attendre cela du juge, car il se prononcera le jour où il jugera. Ce pouvoir créateur du juge est celui de l'opportunité : la solution est donnée non pas par avance mais après l'action. Lorsque la loi prévoit une infraction de manière claire et précise, un individu qui a sciemment accompli ce qu'elle prévoit de manière abstraite peut être punissable (§2).

§2) La participation criminelle

Pour qu'une infraction soit constituée il faut un élément matériel (A) et un élément moral (B).

A) L'élément matériel de l'infraction

Pour être punissable, un agent doit avoir accompli concrètement et matériellement ce qui est abstraitement prévu par la loi, il s'agit de l'élément matériel de l'infraction. Pour ce qui est de l'élément moral, l'article 121-3 du Code pénal pose la notion d'intention de manière très claire : « *il n'y a point de crime ou de délit sans intention de le commettre* ».

Par ailleurs, il existe plusieurs étapes qui amènent à la consommation de l'acte antisocial et qui permettent de déterminer à quel point l'individu est impliqué dans son accomplissement : c'est l'*iter criminis*[22]. Ce processus commence par la pensée de commettre une infraction et la volonté de mettre ce projet en œuvre, se poursuit par une étape consistant en l'élaboration matérielle de l'infraction en accomplissant les actes préparatoires, par le commencement d'exécution et se termine enfin par la consommation de l'infraction.

[22] Le chemin du crime.

L'idée de cette décomposition est de déterminer à partir de quel moment l'individu est appréhendable par le droit pénal. En effet, il n'est pas envisageable de sanctionner la simple pensée criminelle mais le législateur n'attend pas pour autant que l'infraction soit nécessairement consommée. Dès lors, la loi punit certains comportements en l'absence de tout résultat. Tel est le cas pour la tentative d'infraction mais aussi pour les délits-obstacles ou les infractions formelles.

A titre d'exemple, l'individu qui souhaiterait se rendre sur le Darknet, en vue d'y commettre un ou plusieurs délits avant d'y renoncer, ne pourra être poursuivi ni pour la navigation sur le réseau sombre qui ne constitue pas une infraction, ni pour la simple pensée criminelle. Par conséquent, une poursuite ne sera envisageable que s'il a tenté une infraction.

La tentative est prévue à l'article 121-5 du Code pénal qui prévoit qu'elle « *est constituée dès lors que, manifestée par un commencement d'exécution, elle n'a été suspendue ou n'a manqué son effet qu'en raison de circonstances indépendantes de la volonté de son auteur* ».

Il existe différentes conceptions doctrinales concernant la nature du commencement d'exécution. Certains auteurs estiment qu'il y a commencement d'exécution lorsque l'agent a accompli l'un des éléments constitutifs de l'infraction ou une de ses circonstances aggravantes. D'autres auteurs estiment en revanche qu'il s'entend de l'acte univoque accompli par l'agent. Cela signifie que le comportement doit être assez clair pour révéler par lui même l'infraction. Ces deux conceptions sont dites objectives mais il existe une conception subjective selon laquelle la tentative punissable résulterait de la volonté de l'agent de commettre l'infraction sans égard à son comportement. Cette dernière conception est problématique dans le mesure où il est difficile de condamner un individu en ne se basant que sur l'aspect psychologique du projet criminel.

La jurisprudence prend quant à elle en compte l'aspect psychologique du délinquant mais également son activité physique. En effet pour la chambre criminelle de la Cour de cassation c'est « *l'acte qui tend directement et immédiatement à la consommation de l'infraction et qui est accompli dans l'intention de la consommer*[23] ». Les actes qui ne correspondent pas à cette

[23] Cour de cassation, chambre criminelle, 3 janvier 1973, n° 71-91820.

définition sont donc des actes préparatoires non punissables. L'idée est de réprimer suffisamment en amont dans le chemin criminel tout en évitant des condamnations arbitraires basées sur de simples suppositions.

La tentative punissable n'est envisageable que si l'exécution de l'acte n'a été suspendue ou n'a manqué son effet qu'en raison de circonstances indépendantes de la volonté de l'auteur. Par conséquent, l'agent souhaite consommer l'infraction et atteindre le résultat, et c'est un élément extérieur qui l'en a empêché. A contrario, si l'individu se désiste volontairement, il ne sera pas punissable car c'est un repentir actif qui interviendrait suffisamment tôt. Tel est le cas lorsque la raison de l'interruption est purement interne[24]. Ces questions relatives au désistement volontaire sont soumises à l'appréciation souveraine des juges du fond et, il convient de garder à l'esprit que, selon la jurisprudence il y a désistement volontaire lorsque les causes pour lesquelles l'agent s'interrompt sont internes.

Le Code pénal prévoit à l'article 121-4 que la tentative des crimes est toujours punissable même si aucun texte ne le prévoit expressément. En revanche pour les délits, la tentative ne sera punissable que si le texte d'incrimination le prévoit. Quant à la tentative de contravention, elle n'est pas visée par l'article 121-4 du Code pénal de sorte qu'elle ne peut pas exister. Dès lors, pour les délits commis sur le Darknet, la tentative ne sera punissable que si le texte le prévoit. Celui qui tente une infraction est aussi dangereux que celui qui la consomme puisqu'il a échoué en raison de circonstances indépendantes de sa volonté. Dès lors, celui qui tente l'infraction s'expose aux mêmes peines que celui qui l'a consommée. De plus tout ce qui s'applique à l'auteur condamné s'appliquera à celui qui sera condamné pour une tentative d'infraction. C'est le cas des règles concernant la récidive, la tentative ou encore la prescription.

De surcroît, la responsabilité pénale est basée sur la commission d'une faute qui peut être intentionnelle ou non. C'est ce qui constitue l'élément moral de l'infraction (B).

B) L'élément moral de l'infraction

En principe, « il n'y a point de crime ou de délit sans intention de le commettre[25] ». L'intention

[24] Cour d'Appel Douai, 6 mai 2003, 2003/573.
[25] Code pénal, art.121-3 al. 1er.

est la conscience et la volonté de l'individu d'atteindre le résultat prohibé par la loi. Il désire donc transgresser la norme pénale. La doctrine qualifie cette disposition psychologique de dol général mais pour certaines infractions il faut également qu'il désire le résultat dans un but particulier : c'est le dol spécial. La faute non intentionnelle permet également d'envisager une répression. C'est également le cas en matière de cybercriminalité (section 2).

SECTION 2
La cybercriminalité dissimulée

Les infractions commises sur Internet sont multiples. Il peut s'agir de manipulation d'opinion, d'espionnage, d'usurpation d'identité, de terrorisme, de harcèlement, d'escroquerie, de fraude financière ou encore de diverses formes de délinquance. Les technologies du numérique facilitent la réalisation d'activités criminelles, et Internet est devenu un vecteur privilégié de celles-ci. La complexité de la technologie joue de surcroît en leur faveur. La qualification de « *criminels en col blanc* » visant à désigner des cybercriminels, personnes éduquées mais commettant des crimes sans même avoir à se salir les mains, en est un exemple probant. Sans être clairement définie, la cybercriminalité (§1) a su profiter des avancées technologies pour évoluer et consolider un sentiment d'impunité régnant sur Internet. Le Darknet en est le parfait exemple (§2).

§1) La notion de cybercriminalité

Le droit interne évoque la cybercriminalité, mais sans en définir le concept. Le terme est pourtant utilisé dans l'article 695-23 du Code de procédure pénale relatif à l'exécution d'un mandat d'arrêt européen[26], dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et dans la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure. Ces deux dernières prévoient des développements pour lutter contre la cybercriminalité. Mais en dehors de ces textes, la notion est introuvable. En réalité, le concept de cybercriminalité est cerné de manière indirecte par le contenu de conventions internationales qui sont dans l'incapacité d'avoir une portée générale. Pour faire face à cette difficulté, certaines instances officielles utilisent les références « *systèmes informatiques* » ou « *ordinateur* » pour viser les instruments utilisés par les cybercriminels[27] ainsi que « *traitement, transmission ou sécurité de données*[28] » pour en désigner le contenu. D'autres instances définissent la cybercriminalité en se basant sur l'accès non autorisé à « un ordinateur, à un réseau ou à des fichiers à données électroniques[29] » ou au regard d'une connexion à un réseau grâce à un système informatique (A).

[26] Code de procédure pénale art. 695-23.
[27] Le fait de frapper une personne en utilisant un outil informatique ne relève pas de la cybercriminalité.
[28] L'OCDE ou l'ONU par exemple.
[29] Les Etats-Unis ou le Royaume Uni ont adopté ce type de définition qui ne prend pas en compte la diffusion de données ou de comportements illicites.

A) La cybercriminalité, une notion polysémique

La multitude de définitions relatives à la cybercriminalité complique la tâche de ceux qui seraient tentés de définir ce qu'est la cybercriminalité dissimulée. Les autorités étatiques sont confrontées à une nouvelle notion qu'ils maîtrisent mal et qui est sujette aux amalgames. Il sera dès lors pertinent de se demander si les définitions relevant de la cybercriminalité classique sont adaptées à la cybercriminalité dissimulée.

La conceptualisation de la cybercriminalité n'est en effet pas évidente en raison de l'absence de définition étatique universelle. Son objet est perçu différemment par chaque Etat qui adopte ses propres critères de définition, si bien que les définitions doctrinales se sont multipliées. Notion d'étymologie anglo-saxonne, la cybercriminalité fait l'objet de nombreuses définitions, sans qu'aucune d'entre elles ne se soit réellement imposée. Fondamentalement, il s'agit d'une manière d'opérer étant donné qu'à distance, un individu peut atteindre une victime potentielle par le biais de l'outil informatique. Ce dernier permet à l'auteur d'agir anonymement et de viser plusieurs cibles simultanément. En ce sens la Commission européenne s'est expliquée dans une communication au Parlement européen du 22 mai 2007 : « *faute d'une définition communément admise de la criminalité dans le cyberespace, les termes cybercriminalité, criminalité informatique, cybercrime ou criminalité liée à la haute technologie sont souvent utilisés indifféremment*[30] ».

L'organisation de coopération et de développement économiques a défini[31] en 1983 la notion d'infraction informatique comme étant « *tout comportement illégal, immoral ou non autorisé qui implique la transmission et/ou le traitement automatique de données* ». Cela ne concerne pas que les activités internet, mais s'étend à tout ce qu'il est possible de faire via l'informatique, les télécommunications, y compris le téléphone fixe ou mobile, à tous les équipements qui intègrent un traitement électronique et informatique de données[32]. Dès lors, tout élément et toute infrastructure qui manipulent de l'information numérique peuvent être concernés par le crime informatique. Le Darknet est logiquement visé par cette définition en tant que moyen qui

[30] La Convention sur la cybercriminalité adoptée le 23 novembre 2001 par le Conseil de l'Europe fait mention de tous ces termes.
[31] Définition disponible à cette adresse : www.ocde.org.
[32] Cartes à puces, distributeurs de billets, etc.

permet aux cybercriminels de s'exprimer. Dans le même registre la Commission européenne donne une définition large du concept en établissant qu'il s'agit de « *toute infraction qui implique l'utilisation des technologies informatiques*[33] ».

Pour l'OCDE la cybercriminalité a trait à « *tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données* » tandis que pour l'ONU, elle renvoie à « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent* ». Ces définitions sont lacunaires puisqu'elles ne prennent pas en compte toutes les infractions concernées comme par exemple la pédopornographie, l'abus de confiance ou l'escroquerie. De plus, l'ONU fait référence au « *comportement illégal* » or, le même comportement peut être légal dans un pays et illégal dans un autre.

Pour définir la cybercriminalité de manière cohérente, il faut prendre en compte tout le panel d'infractions et se focaliser sur le moyen de commission à savoir un système d'information et de communication. Ainsi, il s'agit de « *toute infraction pénale tentée ou consommée au moyen ou à l'encontre d'un système d'information et communication, principalement Internet*[34] ».

Il en résulte que les experts ont plus de facilités à lister les infractions liées à la cybercriminalité qu'à définir le terme lui-même. Ils s'accordent en effet pour dire que le concept recouvre deux catégories d'infractions. La première regroupe les infractions dirigées contre les systèmes d'information. Il y a notamment les attaques contre les STAD[35] par le biais d'une intrusion, d'une entrave ou d'une destruction de données[36]. Les pirates informatiques multiplient les atteintes aux libertés individuelles via un traitements automatisés de données [37] ou les infractions relatives à la création non autorisée de logiciels de cryptologie.

La seconde catégorie regroupe les infractions de droit commun commises grâce aux nouvelles

[33] Définition disponible sur : http://ssi.gouv.fr/archive/fr/reglementation/CrfimeComFR.pdf.
[34] GROUPE DE TRAVAIL INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE, *Rapport sur la cybercriminalité*, février 2014. Disponible à cette adresse : http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf, [consulté le 15 janvier 2016].
[35] Systèmes de traitement de données. Il peut s'agir d'un site Internet, d'une base de données, d'un ordinateur ou même de la puce électronique d'une carte bancaire ou d'un téléphone portable.
[36] Code pénal, art. 323-1 et suivants.
[37] Code pénal, art. 226-16 et suivants.

technologies de l'information et de la communication. Sont alors visées les infractions de contenu illicite commises grâce à l'utilisation des nouvelles technologies : le contenu pédopornographique, l'apologie du terrorisme ou de crimes contre l'humanité ou encore le négationnisme[38]. Sont également visées les infractions facilitées grâce à l'utilisation des technologies. Celles-ci comprennent un large spectre d'infractions aussi diverses et variées que le proxénétisme, le terrorisme, les trafics de stupéfiants et d'armes, les atteintes au secret professionnel, à la propriété intellectuelle et aux droits d'auteur, atteinte à la vie privée, les menace et injures, les escroqueries, les falsifications de cartes de crédit, la destruction de valeurs[39], de ressources, de services, les fraudes et abus en tout genre, le détournement de capacité informatique, les atteintes au secret professionnel, à la réputation et à l'image etc. Lorsque ces infractions de droit commun sont commises via un système d'information et de communication, on y ajoute le préfixe « *cyber* » afin de les différencier des mêmes infractions commises via des moyens plus classiques. L'escroquerie devient alors la « *cyber-escroquerie* » et le terrorisme le « *cyberterrorisme*[40] ». En outre, pour certaines infractions le système juridique français aggrave les sanctions encourues lorsqu'elles sont commises via un système d'information et de communication.

La notion de cybercriminalité est encore une notion aux contours flous, qui peut faire l'objet de plusieurs définitions et interprétations. Le préfixe « *cyber* », du grec « *kubernan*[41] », permet de faire référence à des activités effectuées sur Internet. Cette dernière est une science qui met en relation les principes régissant les êtres vivants et les machines. Désormais, ce préfixe est utilisé dans les domaines des télécoms et du multimédia. Solange Ghernaouti-Hélie dans son ouvrage « *La cybercriminalité le visible et l'invisible* », donne l'exemple du « *cybernaute* », mélange de cyber et d'astronaute, qui est une personne qui « *surfe* » dans le cyberespace. Initialement ce terme est utilisé en 1948, par Norman Wiener le père fondateur de la cybernétique. Associé à la criminalité, il évoque désormais les infractions commises au moyen d'un réseau informatique et un nouvel espace qu'il convient d'encadrer (B).

[38] « *Doctrine niant la réalité du génocide des Juifs par les nazis, notamment l'existence des chambres à* gaz », LAROUSSE.
Disponible à cette adresse : https://www.larousse.fr/dictionnaires/francais/négationnisme/54062.
[39] Données personnelles ou bancaires, mots de passe, numéros de compte en banque, ordinateurs, composants mémoire (clé USB…) etc.
[40] En réalité, le terme cyberterrorisme est utilisé pour désigner des situations bien précises.
[41] Qui signifie « gouverner ».

B) La création d'un nouvel espace : le cyberespace

En 2014, l'ancien ministre de la Défense[42], Jean-Yves le Drian, a conscience[43] du danger que sont les cybermenaces et propose la création d'une « *cyber armée* » au même titre que les armées existantes. Il y aurait alors l'Armée de l'air, la Marine, l'Armée de terre et l'Armée de la cyberdéfense. Cette dernière serait dotée de structures fonctionnelles et organiques, de prérogatives et d'un état-major. Malgré l'intégration des acteurs de la cyberdéfense dans les structures militaires actuelles, une telle proposition n'a rien d'étonnant.

En effet, tout nouvel espace se doit d'être réglementé. A titre d'exemple, pendant longtemps, l'espace maritime était très largement hors de contrôle des Etats. Il dépendait du principe de liberté des mers et a nécessité une phase de réglementation. Cet espace international maritime est comparable au cyberespace qui est aujourd'hui considéré comme le 4ème espace juridique. En effet, dans le cyberespace, il y a une à la fois complexité et une confusion des acteurs, similaires à celles rencontrées dans l'espace maritime qui ont nécessité l'intervention d'autres administrations pour que la souveraineté française soit respectée sur les eaux territoriales et les zones économiques françaises. Les océans et le cyberespace sont ainsi présentés comme étant des espaces fluides, opposés aux espaces solides[44]. « *Lisse, isomorphes et inhabitables par l'Homme*[45] » sont bien des aspects applicables à ce nouvel espace qui en font un monde singulier où les nouvelles techniques et actions de force appellent à l'élaboration de nouvelles règles. Selon Olivier Kempf[46], les attributs du cyberespace permettent une opacité favorisant l'offensive stratégique. Dans un tel contexte, un encadrement législatif des activités du cyberespace semble nécessaire. En effet, l'insécurité générée par l'informatique, qu'elle soit d'origine criminelle ou non, ne peut plus être ignorée. Elle nécessite de revoir la sécurité des individus, des organisations et des nations en tenant compte de ces risques face auxquels, en général, trois attitudes peuvent être adoptées : les mépriser, les transférer, ou les maitriser. Il

[42] Du 16 mai 2012 au 10 mai 2017.
[43] « C'est que les risques concernant le démantèlement ou la pénétration de nos systèmes informatiques sont de plus en plus réels. C'est une menace contre le fonctionnement de notre pays. Il suffirait de s'introduire dans le dispositif qui organise l'électricité ou qui organise le système ferroviaire pour entraîner une perturbation très lourde », DECROIX C., *Cyberguerre : au cœur de la quatrième armée*, 9 octobre 2014, RTL. Disponible à cette adresse : https://www.rtl.fr/actu/justice-faits-divers/cyberguerre-au-c-ur-de-la-quatrieme-armee-7774738194, [consulté le 10 octobre 2017].
[44] HENNINGER L., *Espaces fluides et espaces solides : nouvelle réalité stratégique ?* Revue de Défense Nationale, octobre 2012, page 245.
[45] Ibid.
[46] KEMPF O., *Introduction à la cyberstratégie*, Economica, 2012.

convient donc de les maitriser tout en respectant les valeurs démocratiques de la société.

Néanmoins, une telle réglementation fait face à deux notions antithétiques qui vont compliquer une telle réalisation : la notion de souveraineté d'une part et celle d'espace virtuel d'autre part. En effet, un Etat n'est souverain que sur son propre territoire. Or, le concept de cyberespace, qui présente les attributs d'immédiateté et d'espace virtuel, ne se soucie pas des frontières étatiques. Dès lors, dans ce domaine, les arsenaux juridiques des Etats manquent d'efficacité si bien que le Droit international a dû proposer des solutions relatives à l'organisation des activités opérées dans le cyberespace.

Concrètement, le cyberespace désigne un « *ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs*[47] ». Ce terme apparu dans une nouvelle[48] de William Gibson en 1984 est en réalité de la contraction[49] des termes « *cybernétique* » et « *espace* ». Le premier désigne « *la science des mécanismes autogouvernés et du contrôle*[50] », le second le « d*omaine localisé dans lequel s'exercent certaines activités*[51] ». Il s'agit donc d'un espace virtuel dont l'accès est possible grâce à une connexion et qui permet d'exercer certaines activités. En présentant un tel espace, William Gibson a en réalité imaginé Internet, ce réseau des réseaux qui permet d'interconnecter tous les ordinateurs du monde.

Désormais, sur cet espace quasi infini, il est possible de distinguer de nouveaux espaces qui se superposent les uns aux autres. Un premier espace nommé « *web visible* » ou « *web de surface* », désigne les sites basiques que l'internaute consulte quotidiennement : réseaux sociaux, journaux en ligne, commerce en ligne, etc. Un second espace nommé « *web invisible* » et lui même divisé en deux espaces, il y a le web profond ou « *Deep Web* » d'une part, et le web sombre ou « *Darkweb* » d'autre part. Le web profond représente l'ensemble des données et des sites hébergés sur Internet sans être indexés par les moteurs de recherches. C'est le cas par exemple pour le contenu des boîtes mel qui fait partie du web profond. Le « *Darkweb* » représente quant à lui l'ensemble des sites dont l'accès est permis grâce à des réseaux alternatifs

[47] Dictionnaire Le Robert de poche 2019.
[48] GIBSON W., *Neuromancien*, 1984.
[49] Définition disponible à cette adresse : https://fr.wikipedia.org/wiki/Cyberespace.
[50] GAYARD L., Darknet, GAFA, Bitcoin, *l'anonymat est un choix*, Slatkine & Cie, 2018, Introduction.
[51] Définition disponible à cette adresse : https://www.larousse.fr/dictionnaires/francais/espace/31013.

comme Tor ou Freenet. Ces derniers, appelés darknets, sont cryptés et permettent à leurs utilisateurs de jouir d'un anonymat quasi-total. Initialement ces darknets étaient créés pour faire face aux contrôles mis en place par les Etats et les grandes entreprises. Mais très rapidement, la cybercriminalité classique a évolué pour migrer vers la cybercriminalité dissimulée (§2).

§2) L'évolution de la cybercriminalité

« *La cybercriminalité se teinte désormais d'une coloration mafieuse donnant naissance à de véritables marchés parallèles d'informations piratées, allant des atteintes à l'identité et à la propriété intellectuelles et artistique, aux fraudes à la carte bancaire en passant par la pédopornographie*[52] ».

Les réseaux numériques sont omniprésents et offrent un espace de travail, de liberté ou économique qui n'a pas que des enjeux positifs. Le développement d'Internet a permis au cyberespace de se définir de manière concrète. Les activités humaines et leurs déviances se retrouvent sur ce nouvel espace virtuel et immatériel que les autorités tentent de sécuriser et de maîtriser.

La cybercriminalité est un véritable fléau qu'il faut nécessairement traiter par des moyens efficaces de prévention et d'action. En effet, un cybercrime peut affecter plusieurs cibles en même temps et avoir de lourdes conséquences, qu'elles soient immédiates ou à retardement : on parle de cyberépidémie. De plus, ces attaques peuvent être perpétrées à distance nonobstant les frontières et les lieux géographiques. C'est cette particularité qui fait que les cybercriminels sont difficiles à appréhender sur l'Internet classique (A) et, dans une plus grande mesure sur le Darknet (B).

[52] OMAR F., *Cadre conceptuel et théorique de la cybercriminalité*, Université de Lorraine, 2014, page 6.

A) L'adaptation des délinquants et criminels aux nouvelles technologies

D'après le rapport Norton[53] sur les cyber risques de Symantec[54], 19,3 millions de Français ont été confrontés à la cybercriminalité en 2017, soit 42% de la population pour un coût total estimé à 6,1 milliards d'euros. Ces chiffres sont en hausse et prouvent que la lutte contre les infractions liées aux nouvelles technologies est loin d'être gagnée.

Sur Internet un commerce illégal s'est mis en place. Il permet d'acheter et de vendre toutes sortes de choses. Les délinquants peuvent être très créatifs lorsqu'il s'agit d'inventer de nouveaux usages criminels. Certains proposent des recettes pour fabriquer de la drogue. D'autres proposent des services sexuels en utilisant des sites comme « *Vivastreet* » par exemple. Toutes sortes d'annonces peuvent trouver preneur à l'instar de celles de recherche de partenaires de suicide qui apparaissent régulièrement, sans compter la vidéodiffusion sur Internet de suicides en temps réel.

Les cybercriminels et cyberdélinquants se sont multipliés grâce à la banalisation de la connexion au réseau Internet. Désormais, les cybercafés et les points d'accès Wifi se trouvent à chaque coin de rue. Ainsi, ils peuvent être aisément utilisés afin de commettre des infractions dans un anonymat quasi absolu. Une meilleure lutte contre la cybercriminalité suppose une collaboration entre le secteur public et le secteur privé qui doivent agir ensemble pour, si ce n'est enrayer, au moins limiter ce fléau. Ainsi, opérateurs et fournisseurs d'accès, sont directement visés par la loi. Ils font, depuis la loi du 21 juin 2004 pour la confiance dans l'économie numérique, l'objet d'une responsabilité atténuée qui les contraint à collaborer avec les enquêteurs et magistrats.

Toutefois, la cybercriminalité est toujours une notion abstraite mal assimilée par les enquêteurs et les magistrats. Malgré la mise en place d'une spécialisation des juridictions et des enquêteurs, les acteurs pénaux éprouvent encore des difficultés à appliquer la loi. En effet, en la matière, les textes se sont multipliés, dispersés et n'apportent pas de réelle définition du terme. Une

[53] Rapport Norton sur les cyber risques, Edition 2017. Disponible à cette adresse : https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/rapport_norton_sur_les-cyber_risques_2017_france.pdf, [consulté le 2 octobre 2017].NORTON, *Cybersecurity rapport*, 2017.
[54] Une société américaine spécialisée dans les logiciels informatiques.

définition légale de la cybercriminalité est donc nécessaire, d'autant plus qu'il s'agit d'une notion qui a vocation à évoluer grâce à des nouvelles techniques d'anonymisation et de chiffrement qui se développent sur le Darknet (B).

B) De la cybercriminalité classique à la cybercriminalité dissimulée

La cybercriminalité s'est développée dans les années 80 avec l'apparition d'Internet alors que la cybercriminalité dissimulée fait son apparition dans les année 2000 grâce à la création du Darknet. Dans la continuité de ce qu'avait proposé l'Internet classique dans les années 2000, le Darknet confirme que le progrès peut être synonyme de vice. La nouvelle génération des cybercriminels a su s'adapter à l'évolution d'Internet pour faire du profit via leur ordinateur. Le Darknet effraie les autorités compte tenu des nombreuses activités illicites qu'il permet. Ce cyberespace dissimulé est notamment devenu le repaire des pédophiles, des trafiquants de drogue, des pirates informatiques et des terroristes.

Toutefois, le Darknet ne se résume pas à la cybercriminalité. Il inquiète les Etats qui craignent de perdre le contrôle de leurs citoyens qui forment à eux seuls une véritable communauté internationale d'internautes. Ce nouvel espace de liberté renforce et renouvelle les droits individuels et collectifs des utilisateurs. Il favorise la liberté d'expression, d'information, de communication et véhicule des valeurs universalistes. Il est devenu à l'instar d'Internet, un acquis des peuples démocratiques[55].

Par conséquent, un sujet relatif à la cybercriminalité du Darknet met en exergue des problématiques qui touchent à divers domaines : informatique, physique, économique, sociologique et juridique. À ce titre, il convient de présenter les aspects techniques du Darknet (Partie 1) avant de se demander comment la loi l'envisage (Partie 2).

[55] VINTON G. CERF, *Internet access is not a human right*, New York Times, 4 janvier 2012. Disponible à cette adresse : https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html, [consulté le 18 avril 2016].

1ère PARTIE
LA FACE SOMBRE D'INTERNET, LES ASPECTS PRATIQUES

Jérémie Zimmermann, porte-parole et co-fondateur de la Quadrature du Net[56], définit le Darknet d'un point de vue technologique. Selon lui, le Darknet est la capacité de deux ordinateurs de parler le protocole de leur choix sans être connectés au reste. Ce protocole n'est pas le Web, de sorte que le Darknet serait l'ensemble de l'Internet moins l'Internet public. Il soutient que cet ensemble est constitué de réseaux privés, de réseaux chiffrés et de réseaux anonymes, répondant à des logiques bien différentes, il y aurait donc une infinité de darknets.

En outre, il démontre que le Darknet est une arme efficace pour lutter contre les atteintes à la vie privée sur Internet. En effet, bien que le secret des communications protégé par la loi soit la norme et devrait permettre à chaque utilisateur de choisir ce qu'il rend public, le fonctionnement de *Google* leur impose de tout rendre public. Ainsi, *Google*, *Yahoo* et la NSA[57] sont main dans la main pour combattre la notion même de vie privée alors que l'anonymat, à la portée de tous sur le darkweb garantirait la liberté d'expression. Cette société de surveillance globalisée dont on a vu se dessiner le contenu avec les révélations de Snowden notamment, repose, selon Jérémie Zimmermann, sur trois principes architecturaux majeurs. Le premier est l'hypercentralisation : *Facebook* par exemple, sait tout de ses utilisateurs si bien qu'il est devenu le premier service de renseignements. Le deuxième est le système fermé qui par définition est isolé de son environnement. Dans cette mesure, les utilisateurs qui n'ont pas accès aux codes sources des logiciels peuvent laisser des portes dérobées exploitables par la NSA par exemple. Le troisième est l'architecture de sécurité internet qui est en réalité un trompe l'œil dans la mesure où les utilisateurs ont une fausse impression de sécurité lorsqu'ils naviguent sur des sites avec le petit cadenas. Et d'un autre côté en miroir il y a trois autres principes sur lesquels reposent les darknets et le Darkweb. Tout d'abord les services sont décentralisés de sorte que chaque utilisateur sait où est sa machine et donc où sont ses données. Ensuite, les

[56] Une association qui milite pour la défense d'un Internet libre et ouvert.
[57] L'Agence nationale de la sécurité, *National Security Agency*, est un organisme gouvernemental du département de la Défense des États-Unis, qui est chargé du « *renseignement d'origine électromagnétique et de la sécurité des systèmes d'information et de traitement des données du gouvernement américain* ».

logiciels libres permettent de contrôler chaque donnée afin d'éviter les failles informatiques. Enfin, il y a le chiffrement de point à point dans lequel les individus gèrent leur clé pour s'assurer d'être les seuls à comprendre les données. Tous les logiciels darknets ont en commun ces trois derniers principes. En somme, les darknets seraient « *l'anti-société* » de surveillance où se trouve en réalité la liberté. A cet égard, il condamne les journalistes qui à tort, partent du principe que le Darkweb est une zone de non droit dans laquelle il peut se passer des choses positives alors que c'est l'inverse puisque le Darkweb serait tout simplement le reflet de la société. Ils ont saisi ce nouveau terme et s'y sont engouffrés en répétant les mêmes inepties sans effectuer de recherches approfondies : d'un côté il y a *Google* qui est blanc et d'un autre le darkweb qui est fondamentalement sombre.

Mais qu'est-ce que le Darkweb ? Pourquoi utilisons-nous également le terme Darknet ? Quelle est la différence avec le *Deep Web*, terme fréquemment utilisé par les journalistes ? Est-ce vraiment un endroit dangereux ? Répondre à ces interrogations nous amène à examiner dans les développements le darkweb dans sa forme et dans son fond. Il convient d'étudier successivement la présentation technique du Darknet (Titre I), et ensuite, le contenu du Darknet (Titre II).

TITRE I
PRESENTATION TECHNIQUE DU DARKNET

Qu'il soit visible ou caché, le Web a une place considérable dans notre société actuelle. En 2017, cet espace de liberté rassemble 3.42 milliards d'internautes, soit 46% de la population mondiale.

Concrètement, plusieurs couches composent le Web de sorte qu'on puisse le comparer à un iceberg dont la partie visible serait dérisoire en comparaison à sa taille réelle. Le contenu de la partie la plus connue est accessible par le biais de moteurs de recherche tels que « *Yahoo* » ou « *Google* » qui sont en mesure d'analyser et d'indexer les pages afin d'avoir de rapides résultats. Ce web de surface donne accès à la plupart des sites que la grande majorité des internautes utilisent quotidiennement. Ainsi, il permet de se connecter aux réseaux sociaux, de faire des achats sur les sites de e-commerce, de fréquenter des sites indexés par un moteur de recherche, etc.

Ensuite, il existe le « *web profond* » qui constituerait entre 70 et 99% du web total[58]. Aussi appelé « *web dissimulé* » ou encore « *Deep Web* », c'est l'Internet des contenus non indexés par les moteurs de recherche. Pour y accéder il faut connaître l'adresse précise du site concerné. Cette non-indexation de pages web peut être faite à dessein ou non et concerne également la majorité des internautes. A titre d'exemple, c'est le cas lorsqu'une personne partage avec ses collègues un document en ligne sans que d'autres personnes puissent y accéder. Par conséquent, il n'y a rien d'intrinsèquement illicites sur le web profond, même si le terme est souvent confondu avec le « web sombre » qui est également une composante du web invisible.

Aussi appelé « *Darkweb*[59] », le web sombre est une partie d'Internet difficile d'accès pour l'utilisateur puisqu'il faut d'une part connaître les adresses spécifiques et d'autre part utiliser des outils informatiques particuliers tels que Tor qui est le logiciel le plus connu. L'idée est de

[58] Une estimation précise n'est pas possible puisqu'il est difficile de cartographier l'ensemble du web. Les ratios varient fortement en fonction des études. Une chose est sûre, le web visible ne représente qu'une infime partie du web total.
[59] BIDDLE P., ENGLAND P., PEINADO M., and WILLMAN B., The darknet and the future of content distribution. In Proceedings of the 2002 ACM Workshop on Digital Rights Management, Washington DC, USA, 2002.

naviguer sur cette partie du web, de manière indirecte, en passant par de nombreux nœuds et ce afin d'assurer que les visiteurs soient fondamentalement introuvables. Pour comprendre ce qu'est réellement le darkweb, nous présenterons le web dissimulé (Chapitre 1) et les moyens d'accès au darkweb via un darknet (Chapitre 2).

CHAPITRE 1
LE WEB DISSIMULÉ

Il s'agit de commencer par une description des fondamentaux, en définissant Internet et le Web avant de traiter le cœur du sujet, à savoir le Darkweb. Tout le monde utilise Internet, mais qui peut réellement donner une définition complète de ce qu'est Internet ? Il s'agit d'un réseau de réseau informatique « composé de millions de réseaux aussi bien privés que publics »[60]. Ces réseaux permettent la transmission de l'information par des protocoles HTTP[61], FTP[62], SMTP [63]et TCP/IP[64] de transfert de données qui permettent l'élaboration d'un ensemble de services diverses comme le courrier électronique, la messagerie instantanée, le p2p ou encore le *World Wild Web* plus connu sous le nom Web. Dès lors, l'Internet et le Web sont deux termes qu'il ne faut pas confondre. Le Web, parfois appelé « *la toile* », est une application d'Internet comme une autre qui utilise le réseau Internet comme un support physique pour le transport de données et pour consulter, via un navigateur, des pages accessibles sur des sites. C'est un réseau d'information constitué par des milliards de documents dans le monde, dispersé dans des millions de serveurs reliés entre eux par des liens hypertextes comparables à des toiles d'araignée[65]. Le Web est divisé en deux parties, l'une visible, l'autre invisible.

Le web visible ou web surfacique est le contenu d'internet accessible via les moteurs de recherche classiques comme *Google, Bing* ou encore *Yahoo*. Il comprend tous les sites indexés atteignables en suivant les liens hypertextes. A titre d'exemple, si vous tapez « *Université Paris II Panthéon Assas* » sur *Yahoo*, vous trouverez un lien direct pour accéder au site dédié à l'Université. Il s'agit d'une page indexée sur un site web référencé. Le moteur de recherche interroge une base de données qu'il a lui même créé en indexant toute les pages web qui existent. Cette recherche s'effectue par mot clé : généralement, les moteurs de recherche

[60] Définition disponible à cette adresse : https://fr.wikipedia.org/wiki/Internet, [consulté le 15 avril 2016].
[61] BALLE F., COHEN T., *Dictionnaire du Web*, Dalloz, page 101. Hypertext Transfer Protocol : « *Protocole de communication utilisé pour transporter des pages programmées en HTML sur le web* ». Ce protocole permet de naviguer sur le Web.
[62] Protocole qui permet l'échange de fichiers.
[63] Ce protocole permet d'envoyer des mails.
[64] Le protocole IP est au cœur d'Internet. Il est souvent associé au protocole TCP qui le complète pour corriger les échanges. Nous parlons alors de protocole TCP/IP : Transmission Control Protocol over Internet Protocol. Ce sont alors les protocoles communs de communication qui permettent l'interconnexion généralisée entre réseaux. Pour faire simple, ils permettent la communication entre tous les ordinateurs reliés à tous les réseaux qui constituent internet.
[65] BALLE F., COHEN T., ibid., « *Le lien hypertexte permet d'atteindre les différentes occurrences d'un mot à l'intérieur d'un texte donné. Il permet aussi de passer d'un site à un autre du Web grâce à un simple clic de souris* ».

stockent les mots les plus fréquemment mentionnés, les emplacements de ces mots et toutes les métadonnées[66] lors de l'indexation des pages web. Les bases de données sont mises à jour grâce à des programmes appelés « *Robot d'exploration* » et « *Robot d'indexation* ». En somme, les sites du Web surfacique sont trouvés par les robots d'exploration et indexés par les robots d'indexation pour être référencés par les moteurs de recherches que les internautes utilisent en tapant des mots clés afin d'accéder au contenu souhaité[67]. Toutefois, certains sites ne respectent pas les normes du web visible et ne sont donc pas référencés, ces ressources forment le Web dit « *invisible* ».

Il existe énormément de sites, de pages, de contenus non référencés par les moteurs de recherche, c'est le « *Deep Web »* ou le Web profond. De manière générale ce web est composé de pages isolées du reste du Web, sans hyperliens pour faire leur promotion, de pages protégées par une identification (Web privé), de pages techniquement mal créées ou de pages utilisant des technologies incomprises par les moteurs de recherche. Il s'agit donc du contenu non lié[68], du contenu non indexable[69], du contenu trop volumineux[70], du contenu à accès limité[71] ou du contenu dynamique[72]. Il peut aussi s'agir du contenu privé lorsque l'administrateur du site web souhaite garder le site ou une partie du site afin de protéger l'information. C'est une catégorie connexe à celle du *Deep Web* et qui se rapproche des darknets. Pour y accéder, il faut connaître l'URL de la page en entier[73]. Certains sites cumulent plusieurs de ces contenus. Par conséquent, lorsque vous consultez vos mails, lorsque vous allez sur l'intranet du site de votre entreprise ou

[66] Le titre de la page Web, l'URL de la page Web, les mots clés, etc...
[67] Les robots d'indexation ne sont pas capables de trouver tous les sites indexables de sorte qu'il existe une partie du web appelée par les auteurs « *web opaque* ». Ce web presque invisible se situe entre le web visible et le web invisible.
[68] Ce sont des pages qui ne sont pas liées entre elles par des liens hypertextes si bien qu'elles ne peuvent pas être trouvées par les robots d'indexation.
[69] Les robots ne comprennent pas tous les langages. Mais les moteurs de recherche deviennent plus performants et aspirent à indexer le plus de formats possibles.
[70] Les moteurs de recherche n'indexent qu'une partie des sites et s'arrêtent d'indexer à partir d'un certain volume de données. 500ko pour Google et Yahoo par exemple.
[71] Il s'agit des sites nécessitant une authentification avec un login et un mot de passe pour accéder au contenu. C'est le cas par exemple pour l'Environnement numérique de travail du site d'une Université qui n'est accessible qu'après identification.
[72] Ce sont des liens qui changent en fonction des recherches. Lors de l'achat d'un billet d'avion, une recherche sur le site d'Air France peut être effectuée. Le lien généré variera en fonction de la destination, de la date et du prix.
[73] BALLE F., COHEN T., op. cit., p.28, page 287. Il s'agit d'une « *méthode d'adressage uniforme de l'information sur Internet permettant de retrouver un document grâce à l'indication du protocole d'accès du serveur, du nom du serveur où se trouve le document et de la référence du document, ces éléments étant séparés par des points* ».

lorsque vous consultez vos comptes en banque, vous êtes sur le *Deep Web*.

Certains sites ont un nom de domaine[74] non standard qui n'est pas enregistré chez l'ICANN[75]. Ils sont regroupés dans des réseaux appelés darknets dont fait partie Tor par exemple. Ce dernier est un réseau qui permet l'accès aux URL en «. *Onion ».* A titre de comparaison, en France, les activités du web de surface sont enregistrées auprès de l'AFNIC[76] avec un nom de domaine en « *.fr* » permettant d'établir une adresse unique. Par exemple, l'adresse IP du site journal quotidien régional français « *Le Parisien* » est 95.131.142.225, mais le nom du domaine, plus pratique, est leparisien.fr. Le Darknet est parfois considéré comme une partie du *Deep Web* puisque son contenu n'est pas indexé par les moteurs de recherche. Néanmoins, le Darknet ou plutôt les darknets désignent les infrastructures[77] tandis que le Darkweb désigne le contenu. En somme, les darknets sont les modalités techniques selon lesquelles le contenu est créé et mis à disposition. Ces sous-réseaux ne communiquent pas ensemble puisqu'ils fonctionnent selon des normes différentes : les protocoles utilisés sont différents mais utilisent tous des fonctions d'anonymisation et de confidentialité. Lorsque le terme Darknet est évoqué, il englobe l'ensemble des darknets existants. Il s'agit donc de comparer Internet et Darknet d'un côté et web visible, *Deep Web* et Darkweb d'un autre. Il s'agit également de se demander si ces différentes étiquettes web visible et web invisible ont lieu d'être. En effet, il s'agirait d'un seul et même endroit avec dans certains cas des spécificités techniques différentes. Mais ces termes semblent nécessaires pour démystifier le Darknet. Ce dernier fait encore l'objet de nombreux préjugés et stéréotypes.

Après cette brève présentation, il semble qu'il existe plusieurs web accessibles grâce à plusieurs Internets. Cette mise en évidence implique de confronter dans un premier temps le web visible et le web invisible (section 1), et d'examiner les particularités des darknets dans un second temps (section 2).

[74] Le suffixe se trouvant à la fin de l'adresse web. C'est le cas pour le .fr se trouvant dans une adresse web.
[75] ICANN est l'acronyme de Internet Corporation for Assigned Names and Numbers. Cette organisation de droit privé à but non lucratif a été créée en 1998. Il s'agit d'une autorité de régulation fixant les noms de domaine des sites Internet au niveau mondial. Un domaine est un ensemble de serveurs utilisé pour la mise en ligne de données. Ils finissent par exemple en .com, en .fr. Son travail est fondamental puisqu'il facilite l'accès aux sites Internet en évitant l'utilisation de l'adresse IP qui est une longue série de chiffre.
[76] Association française pour le nommage Internet en coopération.
[77] Ce sont les modalités techniques selon lesquelles sont créés les contenus.

SECTION 1
Web visible VS Web invisible

La télématique, c'est-à-dire l'alliance de l'informatique et d'Internet a engendré une révolution technologique et culturelle en bouleversant le mode de vie des sociétés industrialisés : « *en vertu d'une rhétorique révolutionnaire, propre aux récits de techniques centrés sur l'innovation, Internet est présenté comme une technique majeure, entièrement nouvelle et résolument tournée vers le futur, dont il est prédit qu'elle doit le transformer socialement*[78] ». Cet essor numérique se traduisant par une mise en réseau planétaire a eu un réel impact sur les monopoles en place et sur la vie privée. Ce réseau informatique basé au niveau mondial est composé d'un ensemble de réseaux nationaux, régionaux et privés qui supportent l'échange de documents électroniques de tout type. Cet outil d'avenir a modifié en profondeur les habitudes de chacun ainsi que l'accès à l'information.

Qui a eu cette volonté de relier tous les ordinateurs du monde entre eux ? Quand a été inventé Internet ? Qui a inventé Internet ? Nul ne le sait avec précision mais il est possible d'affirmer avec certitude que son développement a été entamé dans les années cinquante. Ces dernières ont été marquées par des progrès non négligeables dans le domaine de la télécommunication et de l'informatique.

En tant que réseau, Internet est doté d'une topologie atypique et évolutive se basant sur la possibilité de construire un chemin entre deux équipements connectés. Initialement, Internet était un réseau militaire créé à la demande du Pentagone durant la Guerre froide. Paul Baran et Donald Davies, tous deux informaticiens et physiciens, proposent une « *communication sur réseau de données par paquets*[79] » qui ne serait pas à la portée des Soviétiques dans la mesure où il n'aurait aucun centre. Les deux physiciens suggèrent de relier des nœuds les uns aux autres pour que le réseau soit fonctionnel si certains d'entre eux étaient détruits. Ce projet reliant des chercheurs du ministère de la Défense à des chercheurs universitaires et industriels était financé par « l'*Advanced Research Projetcs Agency, ARPA* », une agence du ministère de la Défense. Il a donné naissance en 1969 à l'ARPAnet, un système d'exploitation créant un réseau consacré

[78] BALLE F., COHEN T., *op. cit.* p. 28, page 119.
[79] BBC, *Internet pioneer Paul Baran passes away*, 28 mars 2011. Disponible à cette adresse : http://www.bbc.com/news/technology-12879908, [consulté le 16 décembre 2015].

à la défense et composé de quatre nœuds, le premier à *UCLA*[80], le deuxième au *Stanford Research Institute*, le troisième à *UCSB*[81] et le quatrième à l'Université de l'Utah[82]. Un an après sa naissance est défini le protocole[83] de communication entre ordinateurs du réseau ARPAnet : NCP [84] . Concrètement l'ARPAnet s'est au fur et à mesure transformé en réseau de communication et s'est popularisé grâce aux universités américaines qui s'y sont reliées. En effet, en 1972 un programme de courrier électronique sur réseau distribué est modifié pour être appliqué à Arpanet. Cela marque le coup d'envoi des recherches qui ne cesseront d'être poursuivies durant toute la décennie. En 1974 deux chercheurs de l'ARPA, Vinton Cerf et Robert Kahnn, créent un « *protocole pour l'interconnexion des réseaux à paquets* » : *the Transmission Control Protocol* qui se divise en TCP et IP[85] pour devenir TCP/IP. Par suite, en 1983, le protocole de l'ARPAnet passe de NCP à TCP/IP et ce changement introduit l'une des premières définitions d'Internet comme étant un ensemble de réseaux passerelles entre ARPAnet et CSnet[86], et met fin à la « militarisation » du développement des réseaux. Internet doit son essor à la gratuité de l'accès au réseau et au développement de l'informatique.

Dès 1996, une nouvelle période de l'histoire d'Internet est entamée avec la phase « *commerciale* » qui va permettre son accès au grand public. De nos jours, Internet est démocratisé et présente des avantages pratiques. Cet ensemble de réseaux permet notamment l'accès à trois types de services. Primo, Internet propose l'accès au courrier électronique, c'est-à-dire aux messages écrits et envoyés électroniquement par le biais d'un réseau informatique. Deuxio, Internet permet l'échange de fichiers par *File Transfer Protocol.* Cette méthode permet de copier les fichiers d'un ordinateur vers un autre ordinateur du même réseau. Tertio, Internet offre la possibilité d'accéder au contenu du Web, connu sous le signe www pour *World Wide Web* et développé dans les années quatre-vingt-dix. Ce dernier se divise en deux parties, l'une visible qui serait dérisoire comparée à l'autre qui est invisible. Il convient de traiter d'une part,

[80] L'Université de Los Angeles.
[81] L'Université de Santa Barbara.
[82] Parallèlement à ce projet, un ingénieur français, Louis Pouzin, invente la notion de « *datagramme* », une technique de communication par paquets. Trop coûteux, son projet est arrêté en 1978 mais ses travaux ont inspiré les protocoles utilisés aujourd'hui dans l'Internet contemporain. Outre ces deux projets, d'autres initiatives similaires sont envisagés en Belgique ou en URSS si bien que certains affirment qu'Internet a été créé en plusieurs étapes grâce au travail de différents scientifiques à travers le monde. La multiplication des réseaux ou protocoles différents de TCP/IP explique le succès tardif d'Internet.
[83] Un protocole est une sorte de langage commun qui permet aux équipement de se comprendre.
[84] *Network Control Protocol*, il s'agit du premier protocole *host-to-host* c'est-à-dire serveur à serveur.
[85] *Internet Protocol*.
[86] *Computer and Science Network.*

le Web visible, la partie visible de l'iceberg (§1) et d'autre part, le Web invisible, la partie cachée de l'iceberg (§2).

§1) Le Web visible, la partie visible de l'iceberg

Il existe une confusion récurrente entre le Web et Internet. Elle est intimement liée au fait qu'Internet est une technologie récente qui a mis de nombreuses années à s'imposer au grand public. C'est dans les années 1990 que s'est popularisé Internet, et ce grâce à la démocratisation du Web, le service d'information en ligne le plus utilisé par les internautes.

A l'instar d'Internet, cette application ne s'est pas créée du jour au lendemain et est l'œuvre de plusieurs scientifiques. Pour faire simple, deux informaticiens, Tim Berners-Lee et Robert Caillau, créent le système HTLM en s'inspirant de plusieurs programmes développant l'hypertexte. La popularité du *World Wide Web* va s'accroître de manière exponentielle avec la création de *NSCA Mosaic*, un navigateur web développé au centre de recherche et d'exploitation des superordinateurs de l'Illinois par Marc Andreessen et Eric Bina. Celui-ci permet de consulter et d'afficher le contenu du *World Wide Web*. En 1994, Marc Andreessen commercialise une version améliorée de Mosaic l'annuaire Yahoo ! est créé. Par suite, les choses vont s'accélérer et les technologies web vont évoluer et devenir celles utilisées aujourd'hui par des milliards d'utilisateurs. Les utilisateurs d'ordinateurs accèdent à l'information juste avec un clic de souris.

Ainsi, l'objet de cette sous-section est d'étudier dans un premier temps, le fonctionnement du Web (A) et dans un second temps, le Web et son contenu (B).

A) Le fonctionnement du Web

Le Web est devenu le nouveau standard de l'informatique connecté sur le réseau Internet. En tant qu'application de l'Internet, le Web utilise le protocole TCP/IP qui permet la communication entre machines connectées en utilisant un protocole qui lui est propre : il s'agit de l'HTTP[87]. Ces protocoles fonctionnent selon le mode de communication « *client /*

[87] *Hypertext Transfer Protocol* : c'est un protocole de communication utilisé pour le transport de pages Web programmées en HTML.

serveur[88] » . C'est ainsi qu'un serveur web transmet des données à l'ordinateur client qui a préalablement effectué une demande par le biais du protocole HTTP. Le programme qui permet à l'utilisateur d'avoir accès au contenu du Web écrit en langage HTLM est appelé navigateur ou *browser.* Par ailleurs, ce programme permet à l'utilisateur d'accéder à d'autres protocoles d'Internet, via des URL[89], mais surtout à l'hypertexte puisque les documents circulant sur le Web sont écrits dans un langage commun : HTML[90]. En somme, les liens hypertexte permettent d'accéder au contenu du Web écrit en langage HTLM en passant d'un site à un autre grâce à un clic de souris.

Il existe plusieurs navigateurs Web en fonction du type de matériel utilisé et en fonction du système d'exploitation[91]. Les plus utilisés en 2018 sont Mozilla Firefox, Safari, Opera ou Google Chrome. Sans eux, les internautes ne pourraient pas accéder au contenu du Web (B).

B) Le Web et son contenu

Internet et plus particulièrement le Web ont été des moteurs essentiels dans l'évolution des nouvelles technologies de l'information et de la communication. Le web a joué un rôle fondamental dans la contribution à la dynamisation des industries de la communication : audiovisuel et télécommunications. Son contenu sans limite peut être constitué de textes, d'images, de dessins, de vidéos, de contenu audio… Ainsi, le Web offre la plus vaste des bibliothèques de sons[92], d'informations, d'images et de vidéos[93] de tous les temps. Avec de

[88] Deux machines du même réseau communiquent ensemble. L'une appelée « cliente » demande un service, l'autre appelée « serveur » fournit ce service.
[89] BALLE F., COHEN T., *op. cit.* p.28, page 387. *Uniform Resource Locator* : « *il s'agit d'une méthode d'adressage uniforme de l'information sur internet, permettant de retrouver un document grâce à l'indication du protocole d'accès du serveur, du nom du serveur où se trouve le document et de la référence du document, ces éléments étant séparés par des points* ».
[90] BALLE F., COHEN T., *op. cit*. 28, page 101. *Hypertext Mark-up Language* : « *Language de programmation des pages web, composé d'une suite de signes ASCH dans laquelle sont incluses les commandes concernant le formatage des pages et des images et la définition des liens hypertexte* », Un document HTLM est le principal composant d'une page Web.
[91] Les systèmes d'exploitation sont un ensemble de programmes permettant d'utiliser les ressources de toutes sortes de matériels tels qu'un ordinateur, un smartphone ou une tablette tactile. Les plus connus pour ordinateur sont Linux, Windows ainsi que Mac OS et pour tablette tactile et smartphone, iOS et Android.
[92] Des services de streaming musicale tels que Deezer, Apple Music, Spotify ou encore Napster offrent un accès illimité à la musique. Selon le syndicat national de l'édition phonographique, 28 milliards de titres ont été « *streamés* » en 2016.
[93] Le streaming légal peut être gratuit, comme sur Youtube et Dailymotion, ou payant, comme sur Canalplay Infinity, FilmoTV et Netflix.

nouvelles applications qui semblent futuristes, les utilisateurs passant du statut de consommateur simple à celui d'émetteur d'information.

D'aucuns s'accordent à dire que ce phénomène ne cessera d'évoluer à tel point que les interrogations se multiplient quant à la capacité du réseau en débit. Un utilisateur peut surfer sur le Web à partir de différents accès au réseau Internet : les smartphones, les tablettes tactiles, les appareils photos, les ordinateurs sont des appareils qu'il est possible de connecter au réseau. Dès lors, les usages évoluent et c'est ainsi que l'ordinateur remplace la télévision ou même le téléphone[94]. Selon le site internet Live Stats[95], il existe en 2017 plus d'1,2 milliard de sites Web utilisés par 3,7 milliards d'utilisateurs à travers le monde. Toutefois, ces chiffres qui ne cessent d'augmenter ne représentent qu'une partie du Web qui serait dérisoire en comparaison à la partie invisible (§2).

§2) Le Web invisible, la partie cachée de l'iceberg

Web invisible, et non pas « *sombre* » ou « *profond* ». Le premier terme englobe les deux autres qui ne sont donc pas des synonymes même si l'amalgame sémantique est fréquent. Le Web invisible composé du *Deep Web* et du Darkweb, s'oppose au Web surfacique.

Le *Deep Web* est le Web accessible librement mais non indexé par les moteurs de recherche. Sa taille a été estimée à plus de 500 fois celle du web visible mais avec la démocratisation du *cloud*[96] qui compose le *Deep Web*, cette proportion aspire à évoluer[97]. Quant au Web sombre, il est plus difficilement appréhendable et nécessite des outils spéciaux pour y accéder. Pour avoir une bonne vision, nous examinerons, d'une part, le *Deep Web* (A), et d'autre part, le Web sombre (B).

A) Le Deep Web

Les organisations des secteurs public et privé sont intriguées par le vaste potentiel de récolte de contenu non structuré à l'échelle de l'Internet, de l'identification des entités dans les

[94] Il est possible d'envoyer des SMS et de passer des appels téléphoniques à partir de son ordinateur.
[95] http://www.internetlivestats.com.
[96] Il s'agit de services informatiques permettant le stockage de données via Internet.
[97] SENELLART P., *Comprendre le Web caché*, Université Paris-Sud 11, 2007.

métadonnées et de la synchronisation de ce contenu semi-structuré en intelligence exploitable. Plusieurs questions sont fréquemment posées sur le processus et les possibilités de collecte, d'analyse et de sortie de données *Deep Web*. L'entreprise BrightPlanet [98] propose une explication claire et simple du *Deep Web*. Il s'agit d'une partie de l'Internet qui n'est pas accessible aux moteurs de recherche. Ainsi, le seul moyen d'accéder à cette partie du web est d'entrer une requête dirigée dans un formulaire de recherche web afin de récupérer du contenu dans une base de données qui n'est pas liée. En d'autres termes, l'accès au *Deep Web* ne peut se faire qu'après une recherche sur le site web dont il est question. Les moteurs de recherche web surfacique conduisent alors à des sites web qui ont un contenu *Deep Web* non structuré. A titre d'exemple, en publiant un statut sur Facebook, un internaute crée du contenu sur le *Deep Web*, mais pour ce faire, il est obligé d'accéder au site Facebook dans un premier temps, et d'entrer ses identifiants dans un second temps[99]. Malgré quelques similitudes le Web dissimulé est différent du Web sombre qu'il convient de présenter (B).

B) Le Web sombre

Est-il possible de situer le Darkweb ? La réponse est non. Le Web, qu'il soit visible ou non, est polymorphe, infini, de sorte qu'il est impossible de le cartographier en définissant son ultime frontière, c'est le même principe qui régit le darkweb.

Comment accéder au Darkweb ? L'accès au Darkweb se fait grâce aux darknets qui suppose l'usage d'outils sophistiqués. Un darknet est un réseau privé anonyme mis en place entre pairs de confiance. Ce type de réseau, pouvant être établi par une large communauté ou par un petit nombre d'utilisateurs, n'est pas accessible par les logiciels et les protocoles usuels. Le protocole technique pour accéder à un darknet est très simple et les utilisateurs ne trouvent que ce qu'ils sont venus chercher en raison de l'absence de moteur de recherche. Les darknets désignent les infrastructures (1) tandis que le darkweb désigne le contenu (2).

1. Les darknets

Un darknet est un sous-réseau d'Internet c'est-à-dire un ensemble d'équipements

[98] Le site de l'entreprise est disponible à cette adresse : www.BRIGHTPLANET.com.
[99] *Deep web.*

interconnectés[100]. Durant les années soixante-dix, des réseaux isolés de l'ARPAnet avaient la possibilité de recevoir des données de la part de l'ARPAnet mais pour des raisons de sécurités les adresses des utilisateurs n'apparaissaient pas dans les listes réseau et ne répondaient pas aux requêtes. Ce sont les premiers Darknets. Avec la généralisation de l'informatique et des réseaux de commutation de paquets, les choses de valeur sont de moins en moins tangibles. Cela a engendré de nouveaux défis et de nouvelles opportunités concernant la distribution et la copie du contenu multimédia.

Révélé au grand public français grâce à un reportage[101] et à un article paru dans Télérama[102], le terme Darknet avait déjà gagné l'acceptation des scientifiques à la suite de la rédaction d'un document intitulé « *The Darknet and the Future of Content Distribution*[103] ». Cet article marquant la naissance du terme Darknet a été présenté par quatre employés de Microsoft lors d'une conférence sur la sécurité à Washington le 18 novembre 2002. Les auteurs de cet article, quatre employés de Microsoft, indiquent que la présence de Darknets serait un obstacle majeur au développement des technologies relatives à la Gestion des droits numériques. Personne ne pourra empêcher la diffusion non autorisée de contenus protégés par un droit de propriété du fait de l'existence d'un réseau sombre appelé Darknet. Cet article explique que le Darknet nuira à la protection du droit d'auteur. Quinze ans plus tard, ses prédictions se sont révélées exactes. Ce document énonce que les technologies de l'information seraient de plus en puissantes si bien qu'il sera permis aux individus de partager des informations avec une facilité déconcertante. Mais cet échange d'information ne se restreindra pas à l'Internet usuel, il se fera par le biais de ce que les auteurs du document appellent le Darknet. Ce terme englobe notamment les réseaux P2P qui sont à l'origine du terme et qui ont constitué l'une des premières craintes des autorités publiques en raison des échanges illégaux de contenu culturel. Lorsqu'un contenu, un film, une musique, ou un logiciel, se retrouve dans le web noir, sa propagation devient incoercible ce qui facilite le piratage du contenu nonobstant les droits numériques. L'article a été écrit par Peter Biddle, Bryan Willman[104] avec les contributions de Paul England et Marcus Peinado. D'aucuns estiment que ce sont les premiers à avoir utilisé ce terme. Selon ces informaticiens la gestion

[100] Les connexions peuvent être physiques (par câble) ou sans fil (via le Wifi par exemple).
[101] ENVOYEE SPECIALE, Darknet, *la face cachée du net*, France 2, vendredi 14 novembre 2013.
[102] TESQUET O., *Darknet, immersion en réseaux troubles*, Télérama, n°3322 du 14 septembre 2013.
[103] Le Darknet et l'avenir de la distribution de contenu.
[104] L'inventeur du terme Darknet qui a pour ancêtre les « *sneaker nets* ».

des droits numériques DRM[105] qui contrôle l'utilisation des œuvres numérique est en danger. La technologie DRM ne peut pas empêcher le piratage qui fait perdre énormément d'argent aux industries. Or, cette technologie a été mise en place par Microsoft qui n'a pas apprécié qu'un de ses employés puisse émettre des critiques dessus alors que l'entreprise essayait de convaincre les fournisseurs de contenu de licence d'utiliser cette technologie. La présentation de Biddle a donc créé une polémique à la suite de laquelle il a été licencié sans avoir la possibilité de se défendre. Les quatre informaticiens ont prédit que le Darknet produirait une course à l'armement technologique et juridique. Ce réseau au fonctionnement insaisissable est capable de s'adapter grâce une grande décentralisation pour ainsi échapper aux entreprises de contenu et aux forces de l'ordre. Les efforts visant à créer des systèmes DRM sécurisés dans la stratégie de lutte contre le piratage n'auront pas de réel impact. En effet, le gouvernement a pu fermer des sites de partages tels que Megaupload[106], et porte son attention sur les sites visibles alors qu'il existe d'autres techniques de partage de fichiers. Dans leur document, les quatre informaticiens examinent la pertinence de la protection du contenu et les architectures de distribution du contenu. Ils spéculent sur l'avenir technique et juridique de ce réseau qui tend à devenir de plus en plus efficace. Ils définissent le Darknet comme un réseau sombre qui n'est pas distinct mais qui serait une couche d'applications et de protocoles s'étendant sur les réseaux existants : il s'agit « d'un ensemble de réseaux et de techniques utilisés pour partager du numérique. Le Darknet n'est pas un réseau physiquement à part, mais une couche applicative qui fonctionne sur des réseaux préexistants ». Sa définition ne se limite pas à la copie de contenu via les P2P puisqu'ils envisagent entre autres le réel potentiel du Darkweb.

En tant que système, le système est potentiellement une cible d'attaques juridiques mais également informatiques. En 1998, alors qu'Internet s'est démocratisé, une nouvelle forme de Darknet voit le jour, et ce grâce aux progrès techniques. Biddle explique les raisons pour lesquelles le commerce multimédia se faisait via des réseaux de distribution centralisés légaux. D'une part, le coût des infrastructures était moindre et d'autre part, les commerçants avaient la possibilité d'afficher des publicités sur les sites hébergeurs. Par ailleurs, la gestion et l'audit s'effectuaient plus facilement avec un modèle de distribution centralisé. Toutefois, les serveurs

[105] Un système DRM est un système qui permet à un client d'obtenir un contenu sous forme protégée pour une utilisation limitée. Le client n'est pas autorisé à copier le contenu, ou à l'envoyer.
[106] Créé en 2005 par Kim Dotcom ce service d'hébergement de fichiers a été fermé en janvier 2012 par la justice Américaine.

centraux ne facilitent pas la distribution illégale de contenu. En 1999 est créé Napster[107], le premier service de partage de fichiers P2P avant que d'autres tels que Gnutella[108] ne suivent. Ces services n'ont pas tenu longtemps puisqu'ils ne bénéficiaient pas de la robustesse des réseaux Darknet qui est due à la décentralisation et à l'anonymat. C'est ainsi que des réseaux sombres comme Freenet ou I2P ont pris leur place comme l'avait fait valoir Biddle. Son analyse et son intuition l'ont amené à croire que les réseaux Darknet auront une influence majeure sur la société. Selon lui, il n'y a pas d'obstacle à la propagation des techniques de partage basées sur les réseaux darknets.

Il est impossible d'évoquer le Darknet sans revenir sur la notion de Mixnet exposée[109] par David Lee Chaum dans son article originel[110] 1981. Les *Mix network* sont des systèmes de courrier électronique qui se veulent garants de la confidentialité. Ce faisant, ils s'appuient sur des échanges chiffrés et sur un grand nombre d'intermédiaires afin de renforcer l'anonymat en cachant les utilisateurs parmi les utilisateurs. Les contenants que sont les darknets peuvent être des réseaux F2F (GNUnet, RetroShare), des réseaux Mixnets ou encore les deux en même temps permettant ainsi la construction d'un écosystème complet. Les premiers servent à l'échange de donnée et se font de manière anonyme, chiffrée et uniquement entre amis alors que les seconds permettent de communiquer. Outre ces possibilités, certains darknets permettent l'accès au Darkweb (2).

2. Le Darkweb

Le Darkweb n'est pas situé, ce n'est pas un endroit. Les termes Darkweb, *Deep Web* et Darknet ne sont pas interchangeables. Tout comme le net n'est pas le web, le Darknet n'est pas le darkweb. Le « *web sombre* » est un ensemble caché de sites web nécessitant des outils spéciaux pour y accéder. L'intérêt d'un tel réseau est évident : les utilisateurs peuvent y rester anonymes afin de pouvoir échanger des informations sensibles sans être censurés ou afin de conclure des affaires illicites sans craindre la police.

[107] http://www.napster.com.
[108] JAVANOVIC M., F. ANNEXTEIN F. et BERMAN K., *Scalability Issues in Large Peer-to-Peer Networks - A Case Study of Gnutella*, ECECS Department, University of Cincinnati, Cincinnati, OH 45221.
[109] Il présente « *the Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms* ».
[110] David Lee Chaum est un ingénieur et cryptographe américain ayant inventé plusieurs protocoles cryptographiques.

La navigation sur les services du Darkweb n'est pas toujours facile. A bien des égards, le contenu semble similaire à celui des sites du web de surface. Toutefois, les liens pour basculer d'un site à un autre sont très rare et les URL sont des séries de nombres et de lettres qui n'ont aucune signification : pour le darknet Tor, le «. *Onion* » remplace les très familiers « *.com* » ou « *.FR* ». De plus, les services cachés changent fréquemment d'adresse. Ainsi, il existe plusieurs index listant les adresses les plus importantes. En 2013, le plus connu de ces index était « *the Hidden Wiki* ».

En outre, certains darknets comme Tor permettent la construction d'un écosystème complet avec des blogs, des mails, un accès au web visible et au Darkweb… Avec ce genre de darknets l'accès au Darkweb est anonyme. Les adresses IP, sortes de signatures numériques à dix chiffres, ne sont pas partagées publiquement et empruntent un chemin aléatoire cryptant toute traçabilité ; sur le Darknet l'adresse IP ne permet pas la reconnaissance de l'ordinateur et le suivi des connexions internet. Ce faisant, l'utilisateur n'est pas identifiable et ne peut pas être tracé géographiquement (section 2).

SECTION 2
Les particularités des Darknets

Un darknet est donc un réseau alternatif, un réseau sur un autre réseau. Ainsi, chaque darknet a sa particularité, certains sont même inaccessibles et destinés à des usages gouvernementaux. Mais, il existe des points communs à tous les darknets, puisqu'en plus d'être décentralisés, ils aspirent tous à favoriser l'anonymat (§1). Par ailleurs, ce dernier peut être conforté par certains darknets utilisant la cryptologie (§2).

§1) Des réseaux anonymes décentralisés

Le *Deep Web* ne doit pas être confondu avec le Darknet : le premier est le web profond, isolé du web de surface, tandis que le second est l'internet sombre qui a vocation à être totalement anonyme. Le Darknet est un réseau pour lequel il n'y a pas de référencement par les algorithmes des moteurs de recherche classiques de sorte qu'il faille nécessairement connaître l'adresse spécifique du site concerné. A l'instar du Darknet, le *Deep Web* peut être décentralisé (A). La différence fondamentale réside donc dans le fait que le *Deep Web* ne garantit pas plus l'anonymat que le web visible (B).

A) Un système décentralisé

Internet est constitué de réseaux connectés entre eux dans lesquels des nœuds permettent les échanges. Pour beaucoup, internet serait un réseau décentralisé, voire déterritorialisé, alors que la réalité est bien différente. En effet, on remarque une centralisation de l'information vers des colosses comme *Facebook* ou *Google*. Les utilisateurs passent par les serveurs des compagnies à qui ils confient leurs données afin de pour pouvoir utiliser leurs services. Par système centralisé, il faut entendre système où chaque utilisateur dépend d'un même serveur[111]. Dès lors, toutes les informations sont au même endroit de sorte qu'il est facile de les trouver. Néanmoins, ce type de système présente des difficultés. Compte tenu du fait que les bases de données dépendent d'un seul point, il est plus facile de les affecter volontairement ou non. On parle de « *single point of failure* »[112]. C'est le cas des centres de données qui sont des sites

[111] GOFFI, *Centralisé, décentralisé, P2P, mais c'est quoi tout ça ?* 2015.
Disponible à cette adresse : https://www.goffi.org/post/2015/11/10/centralisé,-décentralisé,-P2P,-mais-c-est-quoi-tout-ça, [consulté le 16 avril 2016].
[112] Point unique de défaillance.

physiques regroupant les systèmes de stockage d'une même entreprise.

Un système est décentralisé ou distribué lorsqu'il n'a pas de centre. Par conséquent, sans qu'il y ait d'autorité principale, chaque utilisateur est une partie du réseau et peut échanger avec les autres. La forme « *acentrée* » interdit donc aux utilisateurs d'interrompre son fonctionnement. A titre d'exemple, les réseaux informatiques « *peer to peer*[113] » ou P2P, dans lesquels chaque client est un serveur, fonctionnent sous forme de *Deep Web* et selon une architecture décentralisée. Au contraire de l'architecture centralisée où tout est relié à un point unique à l'instar du modèle client-serveur, l'architecture décentralisée relie chaque ordinateur aux autres de sorte que chacun contribue à la diffusion des flux de données. Ces réseaux décentralisés permettent le partage de fichiers ou de flux multimédia continus[114] entre plusieurs ordinateurs qui communiquent par le biais d'un réseau sans aucun transit par un serveur central. Chaque ordinateur est un nœud qui peut donner son accord pour recevoir et obtenir des objets via une connexion directe. Le partage est donc fondé sur chaque ordinateur connecté qui constitue une ressource potentielle. Le début du XXIème siècle a été marqué par l'évolution massive des usages numériques et de cette technique du P2P. Cette nouvelle architecture se caractérisant par l'échange de données à grande échelle sans contrôle centralisé, a eu un rôle important dans l'éclosion du Darknet.

1. Les *peer-to-peer* : les cousins du Darknet

Le premier grand *peer-to-peer* est sorti en juin 1999 à l'initiative de trois entrepreneurs, Shawn Fanning, Sean Parker et John Fanning, qui ne pensaient certainement pas révolutionner l'industrie culturelle en créant une nouvelle économie numérique. Il s'agit de Napster, un réseau dédié aux échanges de fichiers musicaux qui a été créé afin de faciliter la communication et sur l'échange de musique sur Internet. Cette nouvelle communauté a réussi à contraindre l'industrie musicale à modifier son modèle commercial et à appliquer les règles relatives à la propriété intellectuelle. Toutefois, il s'agissait d'un P2P centralisé : tout le monde était connecté à un serveur central tout en ayant le rôle de serveur. Cette faiblesse a rapidement été exploitée si bien que Napster a été fermé par les autorités. A la suite d'une plainte déposée en 1999[115] et

[113] Dans le vocabulaire commercial « *peer to peer* » signifie de client à client.
[114] De *streaming*.
[115] La plainte est déposée par la *Recording Industry Association of America.*

après deux ans de poursuites, le P2P est fermé pour atteinte au droit d'auteur. Néanmoins, Napster n'est qu'un précurseur et c'est à partir de ce modèle que les réseaux P2P vont se multiplier et impacter l'industrie culturelle comme jamais auparavant. Le conflit entre les utilisateurs et l'industrie culturelle est lancé.

Il faut attendre *Gnutella*, dont la version initiale est sortie en 2000, pour voir le premier P2P décentralisé non structuré. Développé par deux programmeurs informatiques de l'entreprise Nullsoft, Justin Frankel et Tom Pepper, a repris le même procédé que Napster mais avec une architecture décentralisée rendant difficile sa neutralisation. Les nœuds ont le même rôle, ils sont à la fois client et serveur, et sont de même valeur. Puis d'autres vont rapidement suivre le mouvement. Il est possible de citer *eDonkey2000*, créé en 2000 et fermé en 2006, ainsi que le très célèbre *eMule*, créé en 2002 et *Kazaa* qui a été développé par Sharman Networks et Jaan Talinn. Ce dernier P2P et certains utilisateurs ont dû faire face aux poursuite engagés pour violation de la législation sur le droit d'auteur dans de nombreux pays à travers le monde.

En 2018, *BitTorrent* est le protocole P2P le plus utilisé. Mais ce dernier n'est pas totalement décentralisé et fonctionne via des serveurs spécifiques qui gèrent les listes de clients possédant une partie d'un fichier. Ce protocole d'échange *peer to peer* a été conçu dès 2001 à la fin de Napster par le programmeur américain, Brad Cohen. Certains pensaient que la victoire judiciaire de l'industrie face à *Napster* était synonyme de fin pour les P2P. Ils se sont évidemment trompés puisqu'il ne s'agissait que du commencement. En 2004, Brad Cohen, son associé Ashwin Navin et son frère Ross créent la société BitTorrent Inc. et rapidement le peer to peer devient le leader mondial en la matière. En 2006 à la suite du déclin des autres peer to peer BitTorrent est un protocole permettant le téléchargement rapide à partir de différentes sources et non à partir de la même source. Chaque fichier téléchargé est repartagé entre plusieurs utilisateurs. Concrètement au lieu de télécharger un fichier d'un giga octets[116] auprès d'un même utilisateur, l'individu nommé « *leecheur* » télécharge cent méga octets auprès de dix utilisateurs différents nommés « *seedeur* » ce qui facilite la distribution et augmente la vitesse de téléchargement. En effet, lorsque le nombre de téléchargements d'un même fichier augmente, celui de « *seedeur* » augmente également, ce qui accélère le téléchargement pour les

[116] Un octet est une unité de mesure informatique indiquant la capacité de mémorisation d'une mémoire telle qu'un disque dur ou une clé USB. Un méga octet représente 1 048 576 octets tandis qu'un méga octets 1 073 741 824 octets.

« *leecheur* » du fichier. Cependant, des poursuites judiciaires vont permettre de lutter contre ce phénomène P2P et d'aboutir à la fermeture de plusieurs sites utilisant ce protocole. La guerre du téléchargement est l'occasion de revenir sur la législation permettant de lutter contre la contrefaçon en France (2).

2. La guerre du téléchargement en France

Face à l'ampleur du phénomène international de la contrefaçon liée au développement d'Internet, les moyens de lutte se sont multipliés. Le monde virtuel, dans lequel règne un sentiment d'impunité lié à l'anonymat, est contraint de faire face à ce fléau qui s'est amplifié avec le déploiement de nouvelles technologies telles que le Darkweb, le commerce électronique, permettant l'envoi de contrefaçons de produits physiques, ou le « *streaming* », le *« direct download*[117] » et le *« peer to peer* », permettant d'avoir accès à des œuvres protégées par le droits d'auteur. Il existe deux types de la contrefaçon sur Internet. La première se matérialise par ses actes qui vont permettre d'identifier le ou les contrefacteurs et la seconde qui porte atteinte à la propriété intellectuelle est immatérielle. La lutte contre le téléchargement illégal n'est pas négligée par les pouvoirs publics français puisque les enjeux sont considérables. Françoise Nyssen estime qu'il s'agit d'un des plus « grands défis du siècle pour le cinéma. C'est une priorité. La France sera en première ligne pour le porter[118] ». Les acteurs sont nombreux. Les auteurs souhaitent préserver leurs droits de propriété intellectuelle. Ces derniers qui souhaiteraient engager une action en contrefaçon de leur droit de propriété intellectuelle disposent de deux options, la voie civile et la voie pénale. En effet, la contrefaçon constitue une infraction pouvant faire l'objet de poursuites devant les juridictions répressives.

À titre d'exemple, « *est punie de trois ans d'emprisonnement et de 300 000 euros d'amende toute fixation, reproduction, communication ou mise à disposition du public, à titre onéreux ou gratuit, ou toute télédiffusion d'une prestation, d'un phonogramme, d'un vidéogramme ou d'un programme, réalisée sans l'autorisation, lorsqu'elle est exigée, de l'artiste-interprète, du*

[117] Selon Françoise Nyssen, ministre de la culture dans le gouvernement d'Edouard Philippe en 2017, « *le piratage se fait dans 80 % des cas en streaming ou en téléchargement direct désormais* ». LAUSSON J., *En attendant sa réforme, la Hadopi aura droit à 9 millions d'euros en 2010*, 24 septembre 2018. Disponible à cette adresse : [consulté le 25 septembre 2018].
[118]LAUSSON J., *Hadopi : le gouvernement va recycler de vieilles idées pour lutter contre le piratage*, 19 avril 2018. Disponible à cette adresse : https://www.numerama.com/politique/346996-hadopi-gouvernement-va-recycler-de-vieilles-idees-lutter-contre-piratage.html, [consulté le 20 avril 2018].

producteur de phonogrammes ou de vidéogrammes ou de l'entreprise de communication audiovisuelle[119] ».

Néanmoins, la voie pénale pose des problèmes pratiques si bien que les titulaires de droit préfèrent majoritairement la voie civile. Les principales raisons sont la durée des procédures, l'absence de spécialisation des juges pénaux et la faiblesse de l'indemnisation au pénal. L'autre difficulté réside dans la localisation de l'auteur de l'infraction de contrefaçon sur Internet et dans la détermination de la législation applicable et de la juridiction territorialement compétente. Le 22 janvier 2015, dans l'affaire Hejduk c. EnergieAgentur[120], la Cour de justice de l'Union européenne s'est prononcée sur la question de la compétence d'une juridiction autrichienne à propos d'une action portant sur la violation d'un droit d'auteur à la suite de la mise en ligne d'une photo contrefaite en Allemagne. L'institution de l'Union européenne retient le critère de l'accessibilité du site Internet. Par conséquent, si un site est accessible depuis la France, les poursuites pour une éventuelle contrefaçon pourront être effectuées par le juge français.

Ensuite, l'article L.331-13, 2° du Code de la propriété intellectuelle dispose que la Haute Autorité assure « une mission de protection de ces œuvres et objets à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ». La « *Haute Autorité pour la Diffusion des Œuvres et Protection des Droits sur Internet* », dite HADOPI, est une autorité publique indépendante mise en place avec les lois n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet[121] et n°2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet[122]. L'autorité peut désormais mettre en œuvre une sanction administrative graduée allant du simple courrier d'interpellation à la coupure d'internet.

Ses membres « *peuvent, pour les nécessités de la procédure, obtenir tous documents, quel qu'en soit le support, y compris les données conservées et traitées par les opérateurs de*

[119] Code de la propriété intellectuelle art. L.334-4.
[120] CJUE 22 janvier 2015, C-441/13.
[121] Dite HADOPI 1.
[122] Dite HADOPI 2.

communications électroniques en application de l'article L. 34-1 du code des postes et des communications électroniques et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[123] » ; « *peuvent également obtenir copie des documents mentionnés à l'alinéa précédent*[124] » et « *obtenir des opérateurs de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à des services de communication au public en ligne a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise*[125] ».

C'est ainsi que le législateur a tranché en faveur des droits d'auteurs dans le conflit qui les opposaient au respect de la vie privée et à la liberté de communication en ligne. Or, ce type d'atteinte à la vie privée a été très mal perçu et les critiques se sont multipliées. Nombreux sont les internautes à l'avoir assimilée à une surveillance du web synonyme de totalitarisme et créant une justice à deux vitesses. La lutte contre la contrefaçon sur internet a placé l'anonymat des internautes sur le banc des remplaçants, voire en équipe réserve, puisqu'il constitue désormais une exception rare. L'inefficacité de la loi a montré que le « *tout répressif* » n'était pas la solution mais qu'il fallait envisager des formules alternatives permettant de financer les auteurs autrement, *Netflix* en est le parfait exemple. Les réseaux darknets reposent sur les mêmes principes que leurs cousins les réseaux P2P. Toutefois, ils ont une particularité supplémentaire puisque qu'ils sont anonymes (B).

B) Un réseau anonyme

Les darknets sont singuliers dans le sens où ils peuvent avoir des caractéristiques différentes. Certains sont populaires et réunissent des millions d'internautes tandis que d'autres forment de petites communautés. Certains sont faciles à utiliser tandis que d'autre nécessitent des compétences informatiques et beaucoup de motivation. Le point commun reste l'anonymat qui y est garanti en tout état de cause.

[123] Les hébergeurs et fournisseurs d'accès internet.
[124] Code de la propriété intellectuelle art. L.331-21 alinéas 3 et 4.
[125] Code de la propriété intellectuelle art. L.331-21 alinéa 5.

Cela a été précisé, les systèmes « *peer to peer* » sont des outils qui consentent à une décentralisation des services et à une haute disponibilité des données. Néanmoins, les connexions se font par TCP/IP[126] qui désigne « *l'ensemble des protocoles communs de communication permettant l'interconnexion généralisée entre réseaux hétérogènes, grâce au découpage par paquets des données numériques et au réassemblage des paquets à l'arrivée. Ces protocoles permettent une communication entre tous les ordinateurs reliés aux réseaux constituant Internet*[127] ». Il en résulte que l'adresse IP[128] supprime l'anonymat puisqu'elle permet à chaque ordinateur d'être identifié « *grâce à une suite de quatre nombres séparés par des points ou à leur équivalent sous forme de texte*[129] ».

Les plateformes « *friend-to-friend*[130] » quant à elles, fonctionnent sous forme de darknet. Ce terme inventé par Dan Bricklin[131] définit les réseaux de communication cachés privés. *Freenet*[132], *GNUnet, Safety Gate invisible ou Retroshare* autorisent le partage de fichiers et la communication en garantissant l'anonymat et la protection des données personnelles. Ces réseaux F2F sont des serveurs FTP[133] privés chiffrés qui permettent aux nœuds de transmettre un fichier (ou une requête de fichier) de manière anonyme. En effet, lors d'une transmission entre amis, les nœuds par lesquels passent les fichiers, ne dévoilent pas les adresses d'envoi et de réception.

§2) Des réseaux de confiance

La confiance peut être définie comme le sentiment, « *de quelqu'un qui se fie entièrement à quelqu'un d'autre, à quelque chose* » ou, « *d'assurance, de sécurité qu'inspire au public la*

[126] De l'anglais *Transmission Control Protocol over Internet Protocol* ;
[127] BALLE F., COHEN-TANUGI, L., *op. cit. p.28*, page 270.
[128] C'est l'emplacement exact de l'ordinateur.
[129] BALLE F., COHEN-TANUGI L., *op. cit., p.28,* page 270.
[130] Les réseaux « *d'ami à ami* » sont des « *peer to peer* » particuliers qui n'utilisent des connexions directes qu'entre personnes de confiance. D'autres connexions indirectes sont possibles, mais sans que que l'identité des utilisateurs soient dévoilées dans la mesure où un *friend-to-friend* permet un échange automatique et anonyme des fichiers.
[131] BRICKLIN D., *Friend-to-friend networks*. Disponible à cette adresse : http://www.bricklin.com/f2f.htm, 2000.
[132] Initialement, le *friend-to-friend* ne s'appliquait pas à Freenet qui divulguait les adresses IP lors des connexions entre nœuds.
[133] BALLE F., COHEN L., *op. cit. p.28*, un serveur FTP (*File Transfer Protocol*) est « *un protocole utilisé par certains logiciels spécifiques pour transférer des fichiers à partir d'un serveur vers un ordinateur personnel ou inversement* ».

stabilité des affaires, de la situation politique[134] ». Ces deux définitions peuvent être assimilées au Darknet. Les utilisateurs cherchent la sécurité admettent de nouveaux utilisateurs auxquels ils se fient entièrement. Dès lors, les anciens sont en haut de la hiérarchie tandis que les nouveaux en bas. En outre, il existe des procédés comme la cryptologie permettant de conforter l'anonymat. Il convient de présenter la notion (A) et son utilisation (B).

A) La notion de cryptologie

Il n'est pas possible d'étudier le Darknet sans étudier la cryptologie qui en est au cœur. Ce « *réseau invisible* » n'autorise la connexion des utilisateurs qu'aux personnes de confiance tout en leur permettant d'être connectés à un réseau mondial par le biais des amis des amis. Être admis sur un darknet n'est pas chose simple.

Pour ce faire, il faut prouver, par tout moyen, son appartenance à la communauté du réseau darknet en question : « *dans les premiers temps, le filtrage des participants était rare ; il était assez facile de postuler et d'être admis dans un darknet. Aujourd'hui, le filtrage est plus strict et le ticket d'entrée plus difficile à obtenir, car les arrestations augmentent et les infiltrations par les forces de l'ordre ou les entreprises de sécurité sont plus nombreuses*[135] ». En somme, les nouveaux arrivants doivent faire leur preuves en prouvant leur valeur afin que la confiance soit établie. Dès lors, ils pourront progresser dans la hiérarchie.

Lorsqu'un message est transmis sur le Darknet, l'identité de l'émetteur est inconnue, mais en cas d'interception par une tierce personne, le message reste visible de sorte qu'il puisse fournir des informations sur la personne émettrice. Ce faisant, la cryptologie est utilisée pour garantir la confidentialité des messages envoyés anonymement, il s'agit donc d'une garantie supplémentaire. Jean-Philippe Rennard [136] le définit comme « *l'étude des procédés de représentation des messages, de manière à ce qu'ils ne soient compréhensibles que par le ou les destinataires. Son usage est essentiel à la préservation du secret des communications sur Internet où elle est omniprésente* ». La cryptologie, du grec *cryptos* est la science du secret

[134] Définition disponible à cette adresse : http://www.larousse.fr/dictionnaires/francais/confiance/18082.
[135] *RAND : Markets for Cybercrime Tools and Stolen Data*, 2014. Disponible à cette adresse : http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf, [consulté le 9 avril 2018].
[136] RENNARD, J-P., *Darknet : mythes et réalités*, Ellipses, 2016, page 124.

englobant la cryptographie, l'écriture secrète et son analyse, la cryptanalyse ainsi que la stéganographie qui permet de faire passer inaperçu un message dans un autre. Le chiffrement est une technique de cryptographie qui permet de rendre impossible la lecture d'un document par une personne qui ne possède pas la clé de déchiffrement. Concrètement, c'est le procédé qui permet de transformer un message clair en message crypté. En somme, la cryptologie est la discipline tandis que le chiffrement le procédé.

Le chiffrement permet de protéger l'information contre sa destruction ou contre sa révélation à des individus qui ne devraient pas y avoir accès. En 2018, le chiffrement et la cryptologie sont présents partout : passeport biométrique, carte bleue, message envoyé sur *WhatsApp*[137]… Il s'est développé parallèlement aux communications par réseaux. Mais, cette idée de rendre le sens d'un message inintelligible n'est pas nouvelle puisque les premières traces de ce genre de procédés sont très anciennes : environ 1900 ans avant J.C, en moyenne Egypte, des hiéroglyphes inscrits sur la pierre tombale d'un fonctionnaire qui travaillait pour le Pharaon ont été sciemment transformés[138]. Depuis, les méthodes de chiffrage se sont multipliées, et sont extrêmement diverses, la plus connue est « le chiffre de César ». César utilisait une méthode de chiffrage dite de substitution qui consistait à remplacer une lettre donnée par une autre, en décalant l'alphabet.

Cette méthode a souvent été mentionnée par les historiens[139] : « *il avait d'ailleurs l'habitude, quand il communiquait un secret par écrit, de remplacer toujours la lettre qu'il aurait dû mettre la première par celle qui, dans l'ordre alphabétique, vient la quatrième après elle, afin que ce qu'il écrivait ne pût être compris par le premier venu*[140] » ; « *On possède enfin de César des lettres à Cicéron, et sa correspondance avec ses amis sur ses affaires domestiques. Il écrivait, pour les choses tout à fait secrètes, à travers des marques, c'est-à-dire un ordre arrangé de lettres de sorte qu'aucun mot ne pût être reconnu. Si on veut chercher et s'acharner jusqu'au bout, on change la quatrième lettre, c'est-à-dire un D à la place d'un A et pareillement pour toutes les autres*[141] » ; « *Nous avons un recueil des lettres de C. César à C. Oppius et Balbus*

[137] L'application mobile *WhatsApp* propose un service de messagerie instantanée et d'appels : « *les messages envoyés dans cette discussion et les appels sont protégés avec le chiffrement de bout en bout* ».
[138] *Khnoumhotep II (XIIe dynastie).*
[139] GUILLOT P., Histoire de la cryptologie, Université Paris 8, 2014.
[140] CASSIUS D., *Histoire romaine*, livre XL, 9.
[141] SUETON, *La vie des douze Césars, Classiques de poche, 2002.*

Cornélius, chargés du soin de ses affaires en son absence. Dans ces lettres, on trouve, en certains endroits, des fragments de syllabes sans liaison, caractères isolés, qu'on croirait jetés au hasard : il est impossible de n'en former aucun mot. C'était un stratagème dont ils étaient convenus entre eux : sur le papier une lettre prenait la place et le nom d'une autre ; mais le lecteur restituait à chacune son nom et sa signification ; ils s'étaient entendus, comme je viens de le dire, sur les substitutions à faire subir aux lettres, avant d'employer cette manière mystérieuse de correspondre[142] ».

Cette méthode utilisée pour traiter de ses affaires était encore utilisée durant la guerre de Sécession aux Etats-Unis de 1861 à 1865. En 1976, en pleine Guerre Froide, la cryptologie entre dans une nouvelle ère lorsque deux cryptologues américains[143] publient un article commençant par « *nous sommes aujourd'hui à l'aube d'une révolution en cryptographie* ».

Ils proposent un nouveau système reposant sur des données publiques : « *le secret est au cœur de la cryptographie. Pourtant, au début de la cryptographie, il y avait un flou à propos de ce qui devait être gardé secret. Les crypto-systèmes tels que le chiffre de César (où chaque lettre est remplacée par celle située trois places plus loin, A devenant ainsi D, B devenant E, etc.), dépendaient pour leur sécurité, du fait que tout le processus de chiffrement soit gardé secret. Après l'invention du télégraphe, la distinction entre un système général et une clé spécifique a permis que le système général puisse être compromis, par exemple par le vol d'un appareil cryptographique, sans que les futurs messages chiffrés avec de nouvelles clés ne le soient. Ce principe a été codifié par Kerckhoffs, qui a écrit en 1883 que compromettre un système cryptographique ne devrait entrainer aucun inconvénient pour les correspondants. Autour des années 1960, des crypto-systèmes furent mis en service, ils étaient estimés assez solides pour résister à une attaque cryptanalytique à clair connu, éliminant ainsi l'inconvénient de garder secrets les anciens messages. Chacun de ces développements a fait décroître la portion du système qui devait être préservée de la connaissance publique, en éliminant les expédients laborieux tels que la paraphrase des dépêches diplomatiques avant qu'elles ne soient présentées. Les systèmes à clé publique sont dans le prolongement naturel de ce courant vers la diminution de la sphère secrète*[144] ».

[142] Gelle A., *Nuits attiques*, livre XVII, § IX.
[143] DIFFIE W., HELLMAN M., *Department of Electrical Engineering*, Université Stanford, 1971.
[144] DIFFIE W., HELLMAN M., *New Directions in Cryptography*, Université Stanford, 1976.

La cryptologie a longtemps été réservée aux domaines miliaires et diplomatiques. Elle permettait d'échanger sur les adversaires, les relations internationales, les attaques et a fait de nombreux progrès durant la Seconde Guerre mondiale. Elle a donc emprunté un vocabulaire lié à la guerre et souvent été associée aux espions, aux agents en missions et aux soldats. Elle permettait de viser un destinataire privilégié à qui l'information était réservée. Désormais, la cryptologie est devenue un moyen de protection et de défense de la vie privée contre l'Etat notamment. C'est ainsi que Philip Zimmermann a conçu en 1991 le logiciel « *Pretty Good Privacy* » pour protéger les courriers électroniques. Ainsi, la cryptologie met en exergue des problématiques opposant d'un côté, les libertés individuelles et d'un autre, le contrôle social. Les individus sont-ils prêts à sacrifier leur vie privée pour la sécurité ? Il s'agit de trouver le juste équilibre entre une demande croissante des individus qui vise à sécuriser les échanges privés ou commerciaux et la mission étatique qui consiste à assurer la sécurité de la population. En effet, le chiffrement protège les citoyens mais limite par ailleurs l'efficacité de la police et des services secrets. Les enjeux sociaux et sociétaux sont nombreux. C'est pourquoi le chiffrement a longtemps été considéré comme une arme de guerre dans la plupart des pays développés.

En 1991, la réglementation française n'y était pas favorable : « *Si les nouvelles technologies de l'information et de la communication permettent des gains considérables en efficacité et en productivité pour les personnes et les entreprises honnêtes, elles profitent également aux organisations criminelles ou terroristes. Dans le cadre de la protection des personnes et des biens, de la sécurité intérieure et de la défense nationale, l'État doit mettre en place les mesures nécessaires pour éviter que ces technologies ne facilitent, en toute impunité et en toute discrétion, le développement d'actions ou de trafics illégaux (petite et grande délinquance, terrorisme, mafia, pédophilie, blanchiments d'argent, fraudes financières, espionnage industriel...)*[145] ».

Les premières traces de libéralisation en la matière sont apparues en 1998 mais le développement du commerce électronique a permis une évolution avec la loi du 21 juin 2004[146]. Son article 30 dispose que « *l'utilisation des moyens de cryptologie est libre* » (B).

[145] Réglementation française en matière de cryptologie, SCSSI, 1991.
[146] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

B) L'utilisation de la cryptologie

Le chiffrement permet de sécuriser l'envoi d'un message et de le rendre confidentiel, ce qui est différent de l'anonymat ; le chiffrement ne rend pas anonyme et l'anonymat n'assure pas la confidentialité. Si un individu souhaite cacher le contenu d'un message il le chiffre, s'il veut dissimuler son identité il utilise un outil d'anonymat ; une bonne hygiène numérique se conçoit en combinant le chiffrement avec un moyen d'anonymisation comme un darknet. Lorsqu'un message est transmis sur le Darknet, il est anonyme et l'identité de l'émetteur est inconnu ; mais le message reste lisible si bien qu'il est susceptible de fournir des informations sur la personne émettrice. Ainsi, des méthodes de chiffrement sont utilisées ; une lettre peut être remplacée par un signe pour que le message soit totalement réécrit ou alors l'accès au message peut être limité à certains destinataires. Pour la première méthode, la plus utilisée, il est nécessaire de connaître les symboles de remplacement pour déchiffrer le message. Celle-ci repose sur deux types de chiffrement.

Pour le premier, dit à « *clé symétrique* » ou « *secrète* », l'encodage et le décodage d'un message nécessitent l'utilisation d'une clé unique traitée par un algorithme. Cette clé est connue d'avance par l'expéditeur et le destinataire. Le problème réside dans le fait qu'il faut transmettre la clé unique à son interlocuteur ; le risque de compromission du système est grand puisqu'une personne étrangère à l'échange est susceptible de l'intercepter. Pour le second, dit à « *clé asymétrique* », deux clés sont créées. Un message chiffré avec la première clé peut être déchiffré par tout utilisateur ayant la clé associée. L'une est appelée « *clé privée* » puisqu'elle n'est pas transmise tandis que l'autre « *clé publique* » dans la mesure où elle est diffusée largement. Ce dispositif offre deux possibilités ; il permet d'une part, de garder la confidentialité d'un message, et d'autre part, d'authentifier l'interlocuteur grâce à la signature. Ce faisant, lorsqu'un émetteur envoie un message chiffré avec sa clé privée, le récepteur peut le déchiffrer avec la clé publique de l'émetteur ; cela permet la confirmation de l'envoie du message par le bon émetteur. L'inverse fonctionne également car l'émetteur peut aussi recevoir un message chiffré via sa clé publique et le déchiffrer grâce à sa clé privée. Si un individu souhaite envoyer un message chiffré, il le fait avec la clé publique du destinataire qui sera le seul à le déchiffrer grâce à sa clé privée. Cela garantit l'intégrité du message qui n'aura pas été modifié durant le transfert. La cryptologie dit à clé asymétrique est par exemple utilisée pour la

signature électronique de document, les passeports biométriques, les coffres forts électroniques.

Le 16 septembre 2016, le journaliste Darek Walter publie un article intitulé « *les 5 meilleures apps*[147] *de messagerie chiffrée*[148] », dans lequel il fait le point sur les cinq applications les plus populaires de messagerie chiffrée. Ces outils de communication sécurisés ne sont pas utilisés que par les malfaiteurs, mais également par des individus sensibles au respect de leur vie privée. La première application qui se nomme « *Dust Messagerie* » est dotée d'une fonctionnalité qui permet d'envoyer des messages chiffrés qui s'autodétruise automatiquement après 24h ou directement après la lecture si les paramètres ont été modifiés. En outre, l'application permet de détecter les captures d'écrans de la conversation et de masquer son nom d'utilisateur. *Wire*, la deuxième application chiffrée a été développée en Suisse et en Allemagne par le co-fondateur de *Skype*. Ses fonctionnalités sont variées puisqu'elle permet de partager sa localisation, d'envoyer des images et d'enregistrer des vidéos. Son intérêt réside dans le fait qu'elle permet d'échanger en étant à l'abri de tout enregistrement grâce au chiffrement de bout en bout. Ce dernier est un système de communication empêchant les écoutes électroniques des fournisseurs d'accès internet et de télécommunications qui ne sont pas en mesure d'accéder aux clé cryptographiques nécessaire aux décryptage des conversations. La troisième application, *Signal*, est l'application de message qu'utilisait Snowden[149]. Cette application de messagerie offre également un chiffrement de bout en bout. La quatrième application est très populaire en raison de son affiliation à *Facebook*[150], il s'agit de *WhatsApp* une application mobile multiplateforme utilisée par plus d'un milliard de personnes par jour en 2017.

Dans ses paramètres l'application précise que « *la confidentialité et sécurité font partie de notre ADN, c'est pour cela que nous avons intégré le chiffrement de bout en bout. Lorsqu'ils sont chiffrés de bout en bout, vos messages, photos, vidéos, messages vocaux, documents, mises à jour de statut et appels sont protégés pour ne pas tomber entre de mauvaises mains. Le chiffrement de bout en bout de WhatsApp garantit que seuls vous et la personne avec qui vous communiquez pouvez lire ce qui est envoyé ; il n'y a donc pas d'intermédiaires, pas même*

[147] Applications.
[148] WALTER D. (adapté par FILIPPONE D.), Les 5 meilleures apps de messagerie chiffrée), 16 septembre 2016. Disponible à cette adresse : https://www.lemondeinformatique.fr/actualites/lire-comment-salesforce-s-est-prepare-au-rgpd-71829.html [consulté le 28 avril 2017].
[149] Snowden est un lanceur d'alerte américain, ancien employé de la NSA et de la CIA. Il a obtenu un droit de résidence en Russie à la suite de nombreuses révélations sur la surveillance de masse américaine.
[150] L'application est rachetée par Facebook en février 2014.

WhatsApp. Vos messages sont protégés avec un cadenas, et seuls le destinataire et vous avez la clé spéciale qui permet de débloquer et lire votre message. Afin d'assure une protection supplémentaire, chaque message que vous envoyez a son propre cadenas unique et sa clé unique. Tout cela est automatique : vous n'avez pas besoin de quelconques paramètres ni de créer des discussions secrètes pour protéger vos messages[151] ».

Enfin, le journaliste Derek Walter évoque Telegram une application créée en Russie par les frères Pavel et Nikolaï Dourov. Les frères, opposés au régime Russe de Vladimir Poutine, veulent communiquer en échappant au service secret russe[152]. Une option de l'application offre la possibilité d'échanger des messages chiffrés de bout en bout afin qu'ils ne soient accessibles que sur les appareils de l'émetteur et du destinataire du message. En tant qu'application privilégiée des terroristes, l'application *Telegram* est fortement critiquée. Elle a été utilisée par plusieurs djihadistes[153] en France et en Allemagne afin de communiquer de manière protégée, notamment pour la préparation des attentats du 13 novembre 2015. Un député russe a proposé de la bloquer en Russie et le 13 avril 2018, un tribunal de Moscou a ordonné son blocage en Russie puisqu'elle a refusé de fournir aux renseignements russes des clés permettant d'avoir accès aux messages des utilisateurs[154]. En France, nombreux sont les dirigeants ou anciens dirigeants politiques à l'utiliser. Il est possible de citer Nicolas Sarkozy, Jean-Luc Mélanchon, François Fillon, Arnaud Montebourg et surtout Emmanuel Macron[155].

Mais la fonction principale des darknets reste la possibilité d'accéder à contenu invisible. Ce dernier se trouve sur le Darkweb, aussi appelé web sombre. (Chapitre 2).

[151] Disponible sur le site suivant : https://www.whatsapp.com/security/.
[152] KEMPF O., *Interdire Telegram ?* Conflits, octobre-décembre 2016, page 10.
[153] RONFAUT L., *L'application de messagerie Telegram fait le ménage dans les comptes de l'État islamique*, 19 novembre 2015. Disponible à cette adresse : http://www.lefigaro.fr/secteur/high-tech/2015/11/19/32001-20151119ARTFIG00069-l-application-de-messagerie-telegram-censure-78-comptes-de-l-etat-islamique.php, [consulté le 19 novembre 2015].
[154] Le Point, *La justice ordonne le blocage de la messagerie Telegram*, 30 avril 2018.
[155] PAQUETTE E., WESFREID M., *Telegram, l'appli favorite des politiques pour chiffrer leurs messages*, L'Express, 14 juillet 2016. Disponible à cette adresse : https://lexpansion.lexpress.fr/high-tech/telegram-l-appli-favorite-des-politiques-pour-crypter-leurs-messages_1811791.html, [consulté le 19 juillet 2016].

CHAPITRE 2
L'ACCES AU DARKWEB VIA UN DARKNET

Selon Olivier Tesquet, journaliste[156], techniquement, il n'y a pas un seul Darknet mais une infinité de réseaux privés anonymes construits entre pairs de confiance, « *d'ami à ami* ». Amaelle Guiton, journaliste indépendante[157], définit le Darknet comme un réseau privé virtuel, utilisé par des personnes qui souhaitent interagir entre elles. Considérer le Darknet comme une entité cohérente, relèverait selon elle « d*'un glissement sémantique, entretenu par la polysémie du qualificatif « dark » pouvant faire écho aussi bien à l'opacité de l'anonymat qu'au côté obscur* ».

Des dizaines de Darknet sont connus, certains sont confidentiels alors que d'autres regroupent de vastes communautés. Les principaux Darknet *Zeronet, RetroShare, I2P, GNUnet, SafetyGate Invisible, Freenet* et *Tor* permettent aux organisations et aux individus de partager l'information sur les réseaux publics sans compromettre leur vie privée. Il convient de s'attacher dans le second chapitre aux différents outils Darknet, à leur mode de fonctionnement et à leur mise en œuvre. Il s'agira de s'intéresser aux grands réseaux darknets tels Freenet mais aussi à des environnements plus restreints mais qui autorisent la communication secrète, par mail ou messagerie instantanée, et le partage de fichiers (section 1). Une seconde section permettra de s'attarder sur le plus populaire des darknets, Tor (section 2).

[156] Journaliste à Télérama où il suit plus particulièrement les questions numériques, il est en outre auteur de *Comprendre Wikileaks.*
[157] Amaelle Guiton a officié plusieurs saisons à la Matinale du « *Mouv'* ». Elle est l'auteure de *Hackers : au cœur de la résistance numérique*, aux éditions du Diable Vauvert et tient le blog www.techn0polis.net.

SECTION 1
Une infinité de darknets

Les travaux de *Biddle* et ses confrères ont montré que certains logiciels tels que *Napster* et *Gnutella* avaient été utilisés pour l'échange de fichiers de type P2P. Néanmoins, ces réseaux avaient des défauts : ils étaient trop centralisés et ne préservaient pas l'anonymat. Désormais, des réseaux darknet tels que *Freenet, I2P, GNUnet*, *Retroshare* ou encore *SafetyGate Invisible* permettent des échanges anonymes. La liste n'est pas exhaustive puisqu'il existe des centaines d'outils permettant de créer un darknet. Il s'agit de traiter les plus importants et de comprendre le fonctionnement du Darknet qui s'appuie sur des logiciels plus avancés et complexes que de simples outils VPN. Grâce au développement d'Internet, ces réseaux sont devenus accessibles pour un grand nombre d'utilisateurs.

Un darknet est un sous-réseau utilisant l'infrastructure internet grâce à un protocole qui lui est spécifique[158]. Il fonctionne selon une architecture décentralisée de type P2P et intègre des facultés d'anonymisation. Ainsi, un utilisateur de *Freenet* ne pourra pas accéder au réseau Tor et inversement. Le Darknet désigne alors l'ensemble des darknets et des outils facilitant cette quête de l'anonymat et de la confidentialité. Quelles sont les caractéristiques qui forgent la robustesse de ces réseaux ? Anonymat, confidentialité et vie privée. L'anonymat permet de dissimuler son identité sans pour autant cacher ses actions. La confidentialité permet de restreindre l'accès à l'information grâce au chiffrement. Dès lors les échanges ne sont pas nécessairement anonymes mais le contenu est chiffré. La protection de la vie privée consiste à préserver un espace d'intimité, que nous ayons quelque chose à cacher ou non. Chacun est libre de partager ce qu'il désire. L'environnement virtuel est imprévisible, il présente des traits singuliers reposant sur de nouveaux paradigmes. L'architecture et les fonctionnalités de ce réseau sombre dépassent tout ce qui a été imaginé jusqu'ici. Il convient d'étudier d'une part, les réseaux darknets les plus répandus (§1) d'autre part, les moins connus (§2).

§1) Les réseaux darknets les plus répandus

Dans la guerre contre le téléchargement, les réseaux *peer-to-peer* ont évolué en réseaux cryptés appelés darknets et ce, afin de faire face aux techniques légales utilisées par l'industrie du

[158] DAVADIE P., La théorie du Darknet, juin 2015.

disque. Les moyens de riposte sont l'anonymisation et les réseaux de confiance utilisés par les darknets. C'est dans ce contexte que sont devenus populaires les réseaux *Freenet* (A) et *I2P* (B).

A) Freenet

Développé à l'Université d'Edinburgh en mars 2000 par l'informaticien Ian Clarke[159], Freenet[160] est un réseau informatique visant à garantir une liberté d'expression et d'information totale grâce à l'anonymat. Cette plateforme *friend-to-friend*, téléchargée plus de deux millions de fois, permet d'utiliser les services de communication de manière anonyme et sécurisée. Elle a longtemps été perçu comme l'avenir du Darknet et accessoirement du téléchargement illégal.

Les créateurs de *Freenet* ont mis en place des logiciels utilisables sur le réseau. Leur programmation étant faite en Java, l'utilisateur doit nécessairement utiliser un navigateur Web pour s'y connecter. L'accès au réseaux Freenet se fait en téléchargeant un des logiciels sur *freenetproject.org*. *Freenet Reference Daemon* est un logiciel de communication, *Freesites Insertion Wizard* est un logiciel de création de site, *Frost* est un logiciel d'échange de fichiers peer-to-peer et de messagerie instantanée, *Freenet Message System* est un forum basé sur une « *toile de confiance* » alors que *Freemail* est un logiciel de courriel anonymes et chiffrés. C'est ainsi qu'il est possible de partager des fichiers, de parcourir des forums, de communiquer et d'accéder à des « *sitesFree*[161] », de façon anonyme et sans craindre la censure.

A l'instar des autres réseaux darknets, le système *Freenet* fonctionne selon une architecture décentralisée où chaque ordinateur participant stocke des informations récupérables par les autres participants, chaque nœud est un espace de stockage disponible pour les autres nœuds. Plus ces derniers sont nombreux dans le réseau, plus il y a d'espace de stockage permettant une plus grande rapidité. *Freenet* renforce la confidentialité de ses utilisateurs en protégeant les nœuds des attaques extérieures. Ainsi, ils ne sont pas reliés à un foyer central et peuvent restreindre leurs connexions aux pairs de confiance.

[159] CLARKE, HONG T., MILLER S., SANDBERG O., WILEY B., *Protecting free expression online with Freenet*, IEEE Internet Computing, 2002.
[160] https://freenetproject.org.
[161] Sites Internet accessibles uniquement par le biais de *Freenet*.

Il existe en effet deux modes de connexion : le mode darknet et le mode openet. Le premier favorise l'anonymat en se connectant manuellement aux pairs de confiance. Le second se connecte aléatoirement à un nœud qui n'est pas nécessairement de confiance. Ce modèle de connexions fiables permet d'accroître la sécurité du réseau en protégeant le contenu de l'information et l'identité des utilisateurs qui seront moins susceptibles d'être attaqués[162]. Le réseau est très opaque si bien qu'il est difficile pour un adversaire de cibler les nœuds responsables du stockage en vue de supprimer les données. Enfin, *Freenet* n'est ouvert qu'aux membres du réseau et ne permet pas de surfer sur le Web visible. Un autre darknet populaire mérite d'être présenter, il s'agit de *I2P* (B).

B) *I2P*

Créé en 2003[163], *I2P*[164], l'un des principaux réseaux darknets, abrite quatre couches de chiffrement permettant d'envoyer un message de manière anonyme et sécurisée en créant un réseau dans le réseau.

I2P est un réseau privé virtuel[165] créant un tunnel entre des ordinateurs distants. Ainsi, le système autorise l'accès réciproque entre des correspondants qui ne sont pas connectés au même réseau local. Toutefois, les ordinateurs ne s'exposent pas directement puisqu'ils utilisent des nœuds *I2P* comme intermédiaires dans le tunnel. Ce dernier présente deux caractéristiques. En premier lieu, il ne va que dans une seule direction et permet de masquer expéditeur et destinataire. Il en résulte qu'il existe deux sortes d'*I2P* tunnel, les sortants qui masquent les expéditeurs et les entrants qui masquent les destinataires.

En second lieu, un chiffrement garantit l'anonymat au sein de cette indirection en permettant la confidentialité du message et le fait que les intermédiaires ne connaissent que les nœuds précédents et suivants du message. Ce faisant, les informations contenues dans le message ne peuvent pas être utiliser afin d'identifier les correspondants. Les intermédiaires ne connaissent

[162] DOUCEUR J., The sybil attack. In Proceedings of the IPTPS02 Workshop, Cambridge MA, USA, 2002.
[163] Par Jrandom (il s'agit d'un pseudonyme).
[164] Il est possible d'obtenir ce darknet à cette adresse : https://geti2p.net/fr.
[165] Un RPV ou VPN (Virtual Private Network) est un système qui crée un lien direct entre des ordinateurs distants.

pas leur position dans le tunnel de sorte qu'ils ne puissent pas différencier correspondants et intermédiaires. Lorsque qu'un utilisateur souhaite envoyer un message à un autre utilisateur, il le transmet par le biais d'un des tunnels sortants en ciblant un tunnel entrant d'un autre utilisateur.

I2P n'est pas intrinsèquement un réseau proxy identifié par une adresse IP dans la mesure où le client qui reçoit le message est un identificateur cryptographique[166]. Lorsqu'un client souhaite contacter un autre client, il doit connaître certaines données clés regroupées et signées par le nœud dans une structure appelée « *routerinfo* ». Cette dernière contient l'identité du nœud et les adresses de contact de celui-ci.

L'accès à *I2P* se fait après avoir le téléchargement du logiciel sur *geti2p.net/fr/dowload*. Une configuration du modem ou du routeur est nécessaire pour l'installation. Une fois lancée, le navigateur *I2P* permet l'accès aux différents services. Il est possible de naviguer anonymement sur le Web visible ou sur le Darkweb, d'utiliser un service de messagerie instantanée[167] et d'échanger des fichiers[168]. D'autres darknets moins connus ont également vu le jour (§2)

§2) Au-delà des classiques : les darknets les moins connus

D'autres réseaux alternatifs moins connus ont vu le jour. Il en existe deux types : Les darknets F2P permettant l'échange de données (A) et les darknets permettant l'accès au Darkweb et à son contenu (B).

A) Les darknets *friend-to-friend*

Il convient de présenter les deux darknets *Friend-to-friend RetroShare* (1) et *GNUnet* (2).

1. RetroShare

[166] LAROUSSE, Dictionnaire de Poche, 2018 : « *Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données* ».
[167] *I2P Messenger.*
[168] Via I2PSnark.

Lancée en 2006, *Retroshare*[169] est une plateforme gratuite de pair à pair privée garantissant des communications sécurisées et un partage de fichiers entre amis. Ce réseau de partage social décentralisé est conçu pour l'utilisateur qui ne veut dépendre d'aucun serveur central. Il s'agit de lutter contre la censure, d'assurer la liberté d'expression et de cacher l'information des agences de renseignement et des compagnies d'espionnage.

Concrètement, Retroshare est un réseau d'ordinateurs appelés nœuds. L'adresse IP de ces derniers n'est connue que des voisins qui sont invités à le devenir en recevant une clé publique. Ainsi, il n'est possible d'échanger des informations et de ne partager des fichiers qu'avec les personnes autorisées. *GNUnet* fonctionne également selon le même procédé (2).

2. GNUnet

Fondé en 2001, *GNUnet*[170] est réseau darknet décentralisé qui garantit l'anonymat en ayant un fonctionnement similaire à celui des autres *peer-to-peer* anonymes. Dès lors, *GNUnet* propose une solution de partage de fichiers anonymes par le biais d'un réseau composé de nœuds appelés « *gnunetd* » qui sont responsables du transfert des messages chiffrés vers les autres pairs et qui agissent comme des routeurs.

GNUnet nécessite l'utilisation de différents protocoles de communication qui vont permettre aux utilisateurs d'informer de leur présence sur le réseau, de mettre en place une connexion et d'échanger des messages. Le protocole pair à pair définit sept messages distincts compris par tous les pairs. En arrivant sur le réseau, un hôte doit se manifester en envoyant un paquet « *HELLO* » à un autre hôte. Ce dernier, appelé hôte récepteur, envoie un « *PING* » afin de confirmer qu'il est joignable et le receveur de ce « *PING* » renvoie un « *PONG* » afin d'accuser la réception. Pour établir une connexion, un des nœuds doit envoyer à l'autre un « *SETKEY* » avec une clé de session permettant de chiffrer les messages de la communication, et un « PING ». L'autre nœud répond avec un autre « *SETKEY* », un « *PING* » et un « *PONG* » chiffrés de la même manière. Ensuite, le premier nœud répond au « *PING* » par un « *PONG* » contenant le même nombre aléatoire que le « *PING* ». Enfin, après l'établissement de la connexion, les nœuds peuvent échanger des messages chiffrés. En outre, il existe des darknets

[169] Disponible à cette adresse : http://retroshare.net.
[170] https://gnunet.org.

moins connus spécialement conçus pour l'accès au Darkweb (B).

B) Les darknets permettant l'accès au Darkweb

L'accès a un darknet est extrêmement simple et repose sur un principe clair : l'idée d'anonymat est basée sur le fait que les utilisateurs sont cachés parmi les autres utilisateurs. Un darknet n'est fiable qu'à partir du moment où il y a énormément d'utilisateurs. Dès lors, les concepteurs de darknet favorisent la facilité d'utilisation du logiciel et permettent l'accès au Darkweb. C'est le cas pour *Zeronet* (1) et pour *SafetyGate Invisible* (2).

1. Zeronet

« *Nous croyons aux réseaux et aux échanges ouverts, libres et incensurables* »[171]. Créé en 2015 à Budapest, *Zeronet* est une plateforme décentralisée, anonymisée et gratuite développée par un groupe d'informaticiens qui s'était regroupé sur un forum.

Très simple d'utilisation, *Zeronet* ne nécessite aucune configuration spécifique et peut être supporté par tous les navigateurs internet sur toutes les plateformes modernes telles que Mac, Windows et Linus. L'interface et les contenus sont dynamiques et ne ressemblent pas à la sombre description faite du Darkweb. L'utilisateur du Web de surface peut facilement y trouver ses repères. A l'instar des autres darknets, les contenus sont distribués directement entre les visiteurs sans passer par un serveur central et sans que les adresses IP ne soient dévoilées. Cette plateforme de partage permet donc de lutter contre la censure. Le réseau utilise protocole *BitTorrent* et les clés asymétriques. En se connectant l'utilisateur reçoit donc deux clés : une privée et une publique. Un darknet similaire a aussi été créé en France, il s'agit de *SafetyGate Invisible* (2).

2. SafetyGate Invisible

Développé par la société française *Aleph-networks, SafetyGate Invisible* est un réseau *friend-to-friend* privé d'entreprise garantissant une « *détection des fuites de données* », un *« accès anonyme au web et aux réseaux P2P* » et un « *échange fortement anonyme d'informations*[172] ».

[171] https://zeronet.io.
[172] http://www.aleph-networks.com/cybersecurity.php?solutionstabs=2.

Ce logiciel est créé tel un Darknet puisqu'il fonctionne selon l'architecture décentralisée « *Friend to Friend* » ou « *Pair to Pair privé* ». Il propose trois solutions conjuguant *Big Data* et *Cybersécurité*.

La première, la « *Data Leak Prevention* » détecte les « *fuites de données* » sur le Web profond et le Darknet : « *les objectifs de GM Data Leak Prevention sont divers : identifier les informations stratégiques ayant un risque de fuite en dehors de l'enceinte de l'entreprise ainsi que les contextes et les canaux de fuite de l'information, détecter les contrefaçons, maîtriser son identité numérique et tous les outils de la guerre économique* ».

Dès lors, le moteur de recherche « *Data Leak Prevention* » vérifie toutes les données rassemblées sur le Web profond et le Darknet afin de trouver les données piratées et d'identifier les sources de piratages envisageables.

La deuxième, le « *SG Darkproxy* » est une passerelle garantissant un accès occulte au web et aux réseaux « *peer to peer* ». Simple d'utilisation puisqu'elle ne nécessite aucune configuration, elle permet une navigation anonyme et une identification des sources d'informations sur l'ensemble des réseaux « *peer to peer* ».

La troisième, le « SG Invisible » garantit l'échange occulte d'informations au sein d'un réseau « friend to friend » privé d'entreprise. Ce faisant, les données sensibles sont protégées des hacktivistes[173] et concurrents qui ne peuvent plus les saisir. En somme, *SafetyGate Invisible* garantit un anonymat, une invisibilité et une protection de la source numérique en donnant accès à un réseau privé acentré.

Tous ces réseaux ne peuvent pas concurrencer Tor qui est devenu le plus populaire des darknets et qui a connu une forte médiatisation à partir de 2014. Il s'agit actuellement du darknet par excellence (Section 2).

[173] Intimement lié au cybermilitantisme et issu des termes « *hacker* » et « *activisme* », l'hacktivisme désigne le militantisme pratiqué par les hackers. Ainsi, les hacktivistes s'attaquent aux réseaux afin de défendre leurs convictions politiques ou religieuses. A titre d'exemple, Edward Snowden et le groupe Anonymous sont des hacktivistes.

SECTION 2
Tor, le plus populaire des darknets

Tor est bien connu du grand public, son image sulfureuse a été véhiculée par les médias qui l'ont présenté comme un outil permettant de dissimuler des opérations illicites. Son succès est incroyable, d'après le site web metrics.torprojet.org il y aurait chaque jour plus de deux millions d'utilisateurs ayant accès à plus de 30 000 sites cachés. Pourtant, Tor est un projet militaire. Originellement créé pour les besoins de *l'US NAVY*[174], Tor est actuellement développé par le *Tor Project*, une organisation indépendante et financé à 60% par le gouvernement américain. Il existe un paradoxe qui veut que la police américaine, l'armée américaine et la *NSA*[175] utilisent le réseau Tor à des fins de renseignement.

The Onion Router, désigné par l'acronyme Tor, est un réseau d'anonymisation permettant l'accès aux services cachés du darknet mais également au Web visible. Techniquement, il est constitué par des groupes de serveurs exploités par des bénévoles afin de garantir aux utilisateurs un accès plus sécurisé à des contenus cachés et une protection accrue de leur vie privée grâce à un anonymat quasi complet. L'intérêt d'un tel réseau est de concilier sécurité et facilité d'utilisation puisque l'accès au darknet se fait par le biais d'un simple logiciel intégré au navigateur. Dans un premier temps il s'agit d'effectuer la présentation de Tor (§1), puis dans un second temps son fonctionnement (§2).

§1) La présentation de Tor

Fondé en décembre 2006, Tor est une organisation à but non lucratif dont le siège se trouve dans le Massachusetts aux Etats-Unis. Soutenu par *l'Electronic Frontier Foundation*[176], le but de ce réseau alternatif est de préserver les libertés individuelles des utilisateurs utilisant les nouvelles technologies face aux Etats et aux grandes multinationales. L'idée est de faire en sorte qu'Internet soit une zone libérée de l'emprise des puissants. A l'origine Tor est issu d'un projet commun entre l'*US NAVY* et une ONG. L'idée a été développée dans les années 1990

[174] L*'US NAVY* est la marine de guerre des USA.
[175] *The National Security Agency* est responsable de la sécurité des systèmes d'information et de traitement des données du gouvernement américain.
[176] Organisation non lucrative internationale située à San Francisco aux Etats-Unis et fondée par John Perry Barlow, Mitch Kapor et John Gilmore des crypto-anarchistes fervents défenseurs des droits individuels sur Internet.

par les informaticiens David Goldschlag, Michael G. Reed et Paul Syverson afin que les services de renseignements américains et l'*US NAVY* puissent communiquer de manière cryptée et donc sécurisée notamment lorsque les agents étaient sur un sol étranger. En 2002, les informaticiens Roger Dingledine, Paul Syverson et Nick Mathewsone rejoignent le projet et travaillent sur le système de routage en oignon. En 2004, l'*US NAVY* arrête de soutenir le projet qui sera publié sous forme de licence libre avant d'être soutenu par l'*Electronic Frontier Foundation*.

Mais le gouvernement américain ne cesse de financer le projet. La situation semble irréelle. Tor est passé d'un soutien de l'*US NAVY* à celui de crypto-anarchistes combattant pour le droit à l'anonymat sur Internet, tout en étant financé par le gouvernement américain. Ce darknet critique ouvertement la politique des pouvoirs publics américains alors qu'il est financé à plus de 80% par le gouvernement américain qui semble vouloir garder une emprise dessus. En décembre 2015, c'est Shari Steele, l'ancienne directrice de l'*Electronic Frontier Fondation* qui prend la tête du projet et qui aspire à faire de Tor un outil utilisé par le grand public afin de protéger les individus des atteintes à leur vie privée. Cette défenderesse des droits numériques ne nie pas le fait que Tor est en grande partie financé par le gouvernement américain et admet les inconvénients de cette dépendance financière à laquelle elle est opposée[177] : « *ce n'est pas idéal. Ce sont des contrats gouvernementaux. Les contrats sont très spécifiques. Je viens de l'Electronic Frontier Fondation où nous n'avions aucune subvention du gouvernement* ». En raison de ces financements, Tor a été accusé de laissé des failles permettant les intrusions de la NSA. Pour certains, comme Eric Filiol un spécialiste de la cryptographie, Tor serait en fait contrôlé par les Etats-Unis : « *La grande capacité des Américains c'est d'imposer des standards qu'ils contrôlent* ». Il estime donc que les darknets et autres outils d'anonymats seraient des créations du gouvernement. Cela pourrait relever du domaine de la fiction, voire de la science fiction mais les révélations de Snowden vont prouver que cela n'est pas que de la paranoïa puisque les services de renseignements américains ont bel et bien tenté de forcer les techniques de chiffrement utilisés par des millions de personnes à travers le monde.

[177] STEELE S., *interviewée par Seth Rosenblath pour the Parallax*. Disponible à cette adresse: https://www.the-parallax.com/tag/shari-steele/. Texte original : « *It's not ideal. They're government contracts. The contracts are very specific. I come from the Electronic Frontier Foundation, where we didn't take any government money* », [consulté le 20 novembre 2017].

Pour les profanes, Tor devrait être interdit en raison de sa dangerosité. Cet outil de chiffrement et d'anonymisation des communications a précisément été conçu pour qu'on ne puisse pas savoir ce qu'il s'y passe. C'est le réseau lui même, la manière dont il fonctionne qui permettent cet anonymat. Totalement décentralisé, il est impossible de connaître le nombre de connexions effectuée sur le réseau Tor. De plus, cette forme de *mixnet*, qui ne permet pas le partage de fichiers *peer-to-peer*, cache chaque individu parmi les autres utilisateurs du réseau de sorte que plus la base d'utilisateurs de Tor est nombreuse et diversifiée, plus l'anonymat sera protégé. D'abord utilisé pour préserver les libertés individuelles de ses utilisateurs, il a ensuite été mis sous le feu des projecteurs en raison de sa capacité à faciliter la commission de certaines infractions. Les profils et intentions des individus se servant de Tor sont multiples. Le protocole technique pour accéder au darknet est très simple et les utilisateurs ne trouvent que ce qu'ils sont venus chercher en raison de l'absence de moteur de recherche sur Tor. Ils peuvent avoir des mobiles différents et vouloir échapper à la récupération de métadonnées par les GAFA[178], à la limitation de la liberté d'expression ou au pop-ups intempestifs, mais ce n'est pas tout. En effet, Tor est un outil efficace de contournement de la censure permettant à ses utilisateurs d'atteindre des destinations ou des contenus bloqués pour diverses raisons et garantissant des communications socialement sensibles. C'est le cas lorsque des sites web ou des services de messagerie instantanée sont bloqués par les fournisseurs d'accès Internet locaux à la demande des autorités, ou lorsque les utilisateurs souhaitent publier des sites web et d'autres services sans avoir à révéler l'emplacement de ceux-ci.

Par ailleurs, ils peuvent l'utiliser afin d'être protégés contre « *l'analyse de trafic* ». Cette dernière est une forme de surveillance sur Internet qui consiste à étudier les comportements et les intérêts des internautes afin de savoir qui communique avec qui. Les incidences sont nombreuses et peuvent être de tout genre puisqu'elle révèle beaucoup d'informations sur ce que font ou disent les internautes. A titre d'exemple, certains sites utilisent la discrimination par les prix en fonction du pays de connexion, alors que d'autres vendent des informations. Les journalistes utilisent Tor afin de communiquer en toute sécurité avec les donneurs d'informations. Les organisations non gouvernementales peuvent y avoir recours pour protéger leurs membres se trouvant dans un pays étranger. Enfin, les sociétés utilisent Tor afin de protéger leurs transactions sensibles des escrocs mais aussi afin de remplacer les VPN

[178] Il s'agit d'un acronyme désignant les grandes entreprises *Google, Apple, Facebook* et *Amazon*.

traditionnels[179] qui révèlent trop d'informations sur les communications. Cependant, même si Tor fait la promesse de garantir la sécurité et l'intimité de ses utilisateurs, cette idée d'anonymat est menacée par les tendances actuelles en matière de droit, de politique et de technologie puisque les communications entre les individus, les organisations, les entreprises et les gouvernements sont de plus en plus vulnérables à l'analyse. Les concepteurs de Tor veulent contrer ces tendances en facilitant l'accès à ce darknet au fonctionnement simple (§2).

§2) Le fonctionnement de Tor

Les concepteurs de Tor ont souhaité un accès simple à leur réseau : « *un système difficile à utiliser a peu d'utilisateurs et comme les systèmes d'anonymisation cachent les utilisateurs parmi les utilisateurs, un système avec peu d'utilisateurs garantit moins d'anonymat. La facilité d'usage n'est donc pas une simple question de convivialité, c'est un impératif de sécurité*[180] ». Ce faisant, il faut dans un premier temps télécharger et installer le navigateur Tor Browser et son moteur de recherche *DuckDuckGo*. Ces derniers s'installent très facilement sur tous les systèmes d'exploitation. Une fois lancée, le navigateur Tor peut être testé via le lien *Test Tor Network Settings.* Ce dernier permet à l'utilisateur de vérifier que l'IP identifié n'est pas la sienne. Si tel n'est pas le cas, la navigation est bel et bien anonyme. Tor offre deux possibilités de navigation. Il est possible d'une part, d'accéder au web visible de manière anonyme et d'autre part, d'accéder au darkweb via des liens en « *.onion* ».

Le réseau Tor est un « *réseau overlay distribué* » composé de serveurs garantissant le transit du trafic de manière anonyme. L'expression « *the Onion Router* » signifie routage en onion qui provient de l'encryptage de l'ensemble des données qui passent sur le réseau via chaque nœud qui tel un oignon, ajoute une couche d'encryptage au signal.

C'est ainsi que se fait la création d'une voie de réseaux privées via un circuit de connexions cryptées utilisant des relais appelés nœuds. Ledit circuit ne permet qu'un seul saut à la fois, et chaque relais le composant sait d'où proviennent les données et à quel relais les transmettre.

[179] Réseau virtuel privé qui permet de créer un lien entre des ordinateurs distants.
[180] DINGLEDINE, MATHEWSON R., N. et SYVERSON N., *Tor : The Second-Generation Onion Router. In 13th USENIX Symposium*, 2014, page 4. Texte original : « *A hard-to-use system users-and because anonymity systems hide users among users, a system with fewer users provides less anonymity. Usability is thus not only a convenience : it is a security requirement* ».

Les utilisateurs de Tor utilisent ces réseaux en se connectant à travers une série de tunnels virtuels au lieu d'établir une connexion directe. Aucun relai individuel ne connaît le chemin complet qu'un paquet de données a pris. Le dernier nœud reçoit les données chiffrées selon le même procédé puisqu'il ne connaît pas l'adresse IP du nœud précédent et du serveur cible qui est le site web. Ainsi, le circuit mis en place garantit un vaste échange de données sans qu'une analyse de trafic puisse déterminer la source et la destination de la connexion. De plus, il est difficile de faire le lien entre les actions antérieures et nouvelles des utilisateurs puisque les circuits sont modifiés toutes les dix minutes. Toutefois, le logiciel Tor ne se focalise que sur la protection du transport de données et ne résout donc pas toutes les difficultés liées à l'anonymat. Il est donc conseillé d'utiliser des logiciels tels que le navigateur « *Tor Browser* » qui permettront de protéger les informations sur la configuration de l'ordinateur de l'utilisateur et de ne pas fournir son nom ou tout ce qui serait susceptible de l'identifier. En effet, Tor ne protège pas l'utilisateur contre les attaques de surveillance consistant à analyser les statistiques des trafics entrant et sortant de l'ordinateur. Les attaquants déduisent de cette analyse que les trafics font partie d'un même circuit et que les données proviennent de l'ordinateur en question.

L'utilisateur qui connaît une adresse Tor en « *.onion* » peut l'utiliser via le navigateur *Tor Browser*. Ce genre d'adresse est composé de seize caractères pouvant être des chiffres de 1 à 7 et des lettres minuscules. Par exemple, l'adresse du « *Hidden wiki*[181] » est la suivante : *http://kpvz7ki2v5agwt35.onion*. Un relai est sélectionné aléatoirement par Tor afin de constituer un circuit de trois relais minimum via lesquels la requête de l'utilisateur passera. Ce type d'adresse est générée par une clé publique Dès lors, les données envoyées par l'émetteur comportent l'adresse du relais sélectionné aléatoirement par Tor, celle du relai final et un mot de passe appelé « *one time secret* » utilisable qu'une seule fois. Quant aux relais intermédiaires, ils ne connaissent que l'adresse du relais auquel il transfère le message. Pour des raisons de sécurité l'idée est d'éviter qu'un pirate informatique puisse connaître l'ensemble du circuit en attaquant un des relais d'autant plus que le circuit est modifié toutes les dix minutes.

L'accès a Tor s'est démocratisé grâce à de nouveaux logiciels tels que *Tor2web* aussi appelé *Web2Tor* qui permet aux utilisateurs du web de surface d'accéder aux services cachés en « *.onion* ». Ce logiciel a vraiment faciliter la tâche des personnes voulant accéder au Darkweb

[181] Il s'agit d'un Wikipédia référençant les services cachés du Darkweb.

sans être connectés à Tor. L'adresse « *.onion* » devient alors *.onion.to*.

Ce logiciel a été développé en 2008 par les informations américains Aaron Swartz et Virgil Griffith[182] afin de faciliter les tâches des lanceurs d'alertes et journalistes qui souhaitaient se connecter à Tor sans installation[183]. Il est sorti dans une version stable en 2008 et distribué via le site « *https://tor2web.org* ». La publication anonyme sont alors possibles. En outre, *Tor2web* semble être en mesure de bouleverser ce monde numérique puisque qu'une nouvelle étape a été franchie. En effet, certains moteurs de recherche du web de surface utilisent *Tor2web* afin de faire une recherche rapide pour trouver des sites en « *.onion* ». Il est donc possible de trouver le référencement de sites cachés sur le web de surfacique. Néanmoins, cet anonymat disparaît dès que l'utilisateur quitte le réseau Tor pour retourner sur le Web de surface puisqu'il est précisé que *Tor2web* ne protège que les éditeurs de contenus et non les lecteurs[184]. En somme, il n'est pas possible de commettre des infractions en toute discrétion. Le concept *Tor2web* a vocation à rendre accessible le Darknet en le rendant accessible.

L'enjeu d'une telle accessibilité se justifie d'un point de vue pratique et permet de distinguer certains utilisateurs. Cette possibilité de pouvoir consulter le contenu du Darknet sans être anonyme n'intéresse pas les criminels qui ne souhaitent pas être démasqués. Ainsi, les utilisateurs de *Tor2web* ne sont pas les trafiquants de drogue ou les pédophiles. Son intérêt est tout autre : un journaliste souhaitant rester anonyme et échapper à la censure d'un pays peut utiliser *Tor2web* pour publier du contenu en tant qu'éditeur protégé. Le fait que son site édité sur le Darkweb soit accessible sur le web visible lui permet d'avoir une plus grande visibilité. A titre d'exemple, *Wikileaks*, un site de lanceurs d'alerte, existe sur le réseau Tor. En somme, *Tor2web* respecte l'idéologie de Tor en luttant contre la censure et permet de différencier les cybercriminels des autres. La volonté des cofondateurs de Tor semble se réaliser : le réseau se démocratise et s'ouvre de plus en plus au grand public.

La gestion d'un relais Tor est-elle légale ? Oui, elle est parfaitement légale. En effet, l'article L.2-3-3 du code des Postes et Communications Electroniques[185] dispose que : « *toute personne*

[182] « *Tor2Web was originally developed by Aaron Swartz and Virgil Griffith », tor2web.org.*
[183] « *Tor2web is a project to let Internet users access Tor Onion Services without using Tor Browser* », *tor2web.org.*
[184] « *Tor2web only protects publishers, not readers* », *tor2web.org*
[185] La directive européenne 2000/CE du 8 juin 2000 a été transposée en droit français.

assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission ».

De plus, les relais de sortie sont gérés par des structures associatives telles que *nos-oignons.net* ou *torservers.net*, et ce en vue de bénéficier d'une protection juridique si nécessaire. En effet, la singularité du contenu du Darknet peut entraîner énormément de conséquences juridiques.

CONCLUSION DU TITRE I
LA PRÉSENTATION TECHNIQUE DU DARKNET

En l'espace d'une dizaine d'années, l'architecture des darknets a énormément évolué en passant d'un modèle utilisant le peer-to-peer, au développement d'un darknet comme Tor. Des protocoles d'adresses électroniques et d'échanges de fichiers friend-to-friend ont permis la mise en place de véritables réseaux autonomes anonymes et décentralisés. En outre, les darknets permettent d'utiliser le chiffrement qui crypte le contenu en le transmettant sous la forme d'une suite de caractères. Pour le décrypter, le destinataire devra alors utiliser une clé.

Contrairement à Internet qui est souvent présenté, à tort, comme un réseau décentralisé et anonyme, des réseaux parallèles comme Freenet ou Tor le sont réellement. Ces darknets sont des réseaux superposés à l'Internet classique, qui utilisent des protocoles spécifiques afin de communiquer et d'échanger de manière anonyme. Alors que les darknets désignaient dans les années 90 les réseaux parallèles à l'Arpanet, ils ont ensuite été assimilés dans les années 2000 au pair-à-pair permettant le téléchargement illégal, avant de désigner l'Internet sombre mis en avant aujourd'hui par les médias.

En effet, les darknets permettent l'accès au Darkweb qui représente les sites et applications informatiques accessibles via le Darknet ou plutôt un darknet. Concrètement, le Darkweb est une application informatique qui fonctionne sur un réseau darknet et permet d'accéder par le biais d'un navigateur au contenu mis en ligne sur le Darknet (Titre II).

TITRE II
LE CONTENU DU DARKNET

En dehors du Web visible, il existerait un vaste réseau caché de sites et de communautés, un monde où la liberté serait poussée au-delà de ses limites, où les individus peuvent agir comme ils le désirent. Ce monde aussi créatif et complexe qu'il serait dangereux est à votre portée. Il s'agit du Darknet[186], ce monde souterrain qui s'étend des sites populaires aux coins les plus sombres. Souvent évoqué dans les journaux, ce monde est mal compris et rarement exploré. Le Darknet serait une des innovations d'Internet les plus dangereuses : les pédophiles, les hackeurs, les vendeurs de drogues et armes, les extrémistes et les criminels en tout genre en auraient fait leur repère de prédilection. En effet, le Darknet n'est généralement connu que pour ses aspects les plus sombres. Cette mauvaise image a été véhiculée par les médias qui se sont adressés à un public adepte du sensationnel. Quoi de plus attrayant qu'un sombre réseau où les dealers fréquenteraient terroristes, tueurs à gages, pédophiles et vendeurs d'armes. Lieu de toutes les dérives, cette partie existe bel et bien, et attire beaucoup de monde.

Le Darknet repose sur un ensemble d'outils ayant permis des avancées technologiques et sociales qui étaient nécessaires avec l'évolution d'Internet. Néanmoins, ces outils peuvent aussi avoir un usage négatif et faire face aux perversions de la société. Ce faisant, le Darknet n'est pas une structure homogène, c'est un ensemble diversifié à la fois sombre et lumineux. Le Darknet représente une fraction non quantifiable de l'Internet dans son ensemble ; l'accès n'est pas direct mais il n'est pas compliqué. L'utilisation des réseaux darknets a évolué : d'abord utilisés pour le partage confidentiel de fichiers piratés, ils ont ensuite été utilisés pour la défense de la vie privée pour être in fine utilisés pour le partage de produits illégaux. Wikipédia définit un darknet comme « *un réseau superposé (ou réseau overlay) qui utilise des protocoles spécifiques intégrant des fonctions d'anonymisation. Certains se limitent à l'échange de fichiers comme RetroShare, d'autres permettent la construction d'un écosystème anonyme complet (web, blog, mail) comme Freenet. Les darknets sont distincts des autres réseaux P2P distribués car le partage y est anonyme (c'est-à-dire que les adresses IP ne sont pas partagées publiquement) et donc les utilisateurs peuvent communiquer avec peu de crainte d'interférence gouvernementale ou d'entreprise* ».

[186] Le terme Darknet sera utilisé pour désigner de manière générale les darknets ainsi que le darkweb.

Même si cette définition est pertinente, l'utilisation du terme « *Darknet* » suscite le débat. Les requêtes concernant ce terme ont fortement augmenté à partir de 2012 à cause de son image négative. En effet, en plus de faciliter les activités illégales de trafics d'armes et de drogues, d'achats de logiciels malfaisants, de pédopornographie, de contrefaçons (médicaments, faux papiers…), de ventes d'informations sensibles, ces réseaux permettraient le développement d'activités criminelles telles que le terrorisme via des forums spécialisés accessibles sur le Darknet.

La criminalité ordinaire a donc migré sur le Darknet comme le montre un rapport de la RAND publié en 2014[187]. Selon le vice-président marketing des produits de sécurité chez *Juniper Networks*[188] : « *L'étude de la RAND montre que si une économie remplit les critères suivants : élaborée, spécialisée, fiable, accessible et résiliente, alors elle a atteint la maturité* ». Cela a été le cas pour certains supermarchés du Darknet. Néanmoins, il ne faut pas généraliser. Certes, il est possible d'y réaliser des affaires criminelles, mais toute personne naviguant sur le Darknet n'est pas un malfaiteur. Certains explorent le Darknet pour leurs activités criminelles, mais d'autres ont des mobiles différents puisqu'ils le consultent par simple curiosité, pour des fins scientifiques ou alors pour préserver leur vie privée. En tout état de cause, il faut relativiser la vision négative du Darknet. En effet, n'importe qui peut créer un darknet afin de communiquer de manière sécurisée.

Il est impossible de quantifier les sites qui ne sont pas fiables et qui peuvent disparaître très rapidement. De plus, un site peut être dupliqué lorsqu'il y a beaucoup de visiteurs, et ce, afin de mieux gérer le débit ; mais cela permet également d'arnaquer les utilisateurs en créant une copie de site légitime jouissant d'une bonne réputation. En toute hypothèse ce problème de doublon complique le travail des organismes effectuant des études sur le contenu du Darknet.

En dépit de ces difficultés, diverses études existent. En 2016, une étude[189] sur 2700 sites du

[187] ABLON L., LIBICKI M., GOLAY A., *Markets for Cybercrime Tools and Stolen Data.*
[188] Michael Callahan.
[189] MOORE D., RID T., *Cryptopolitik and the Darknet*, Survival : Global Politics and strategy, International Institute for Strategic Studies, volume 58, 2016.

Darknet réalisée par Daniel Moore[190] et Thomas Rid[191] montre que 57% du Darknet serait occupé par des contenus illicites. Une autre étude réalisée sur 400 sites par *Terbium Labs*, une société de sécurité informatique, expose que 55% du Darknet ne serait pas illégal tandis que dans le contenu illégal, 45% concernerait la drogue et 1% la pédopornographie. Une autre étude montre que 80% du contenu du Darknet serait en lien avec la pédophilie.[192] Mais cette étude prenant en compte tous les visiteurs, en incluant les forces de l'ordre et les attaques *DOS* par exemple, est controversée. Ces études contradictoires sont révélatrices du flou qui règne autour du Darknet. En tout état de cause, à l'instar de la cybercriminalité ordinaire[193], la cybercriminalité dissimulée ne serait due qu'à un faible nombre d'individus.

L'objectif principal de ce titre est de présenter un monde controversé mais rarement exploré. Pour comprendre ce phénomène, il convient d'examiner dans un premier temps, les bons côtés du Darknet (Chapitre 1), et dans un second temps, les mauvais côtés du Darknet (Chapitre 2).

[190] MOORE D., est un ingénieur et chercheur spécialisé en *Cyber Threat Intelligence* une discipline basée sur les techniques de renseignement.
[191] RID T., est un enseignant chercheur à l'Université King's College London.
[192] Cette étude a été menée par OWEN G., un Docteur de l'Université de Portsmouth.
[193] Selon une étude menée en 2014 par BERTHIER T., et KEMPF O., deux membres de la chaire de cyberdéfense et de cybersécurité, 10% des cybercriminels seraient responsables de 90% des cybernuisances.

CHAPITRE 1
LES BONS COTÉS DU DARKNET

Le Darknet suscite encore énormément d'interrogations. Dans l'imaginaire collectif, il est perçu comme un ensemble de pages noires et glauques, accessible pour les adeptes des nouvelles technologies à la recherche de sensationnel. Souvent présenté comme un marché dépravé, où les enfants, les armes et les drogues pourraient être achetés par de simples bitcoins, le Darknet fascine et obsède. Mais, au delà de ce web sombre, il existerait une partie encore plus profonde appelée « *Marianas Web* ». Cette partie du web tire son nom de la fosse océanique la plus profonde et de l'endroit le plus profond sur terre : « *the Mariana Trench*[194] ». Sur le *Marianas Web* il serait possible de trouver les « *secrets les plus sombres de l'humanité dans son histoire* » : l'emplacement secret de l'Atlantide, les archives secrètes du Vatican ou même une entité artificielle toute puissante.

Sur le Web visible il est possible de trouver des informations sur le *Marianas web* : « *pour accéder au Marianas web vous avez besoin de quelque chose dont le nom est falcighol dérivation polymère, c'est tout simplement l'informatique quantique. Sans cela, vous ne pouvez pas accéder au Marianas web. Mais qui possèdent les connaissances nécessaires pour l'informatique quantique ? Le gouvernement. C'est la raison pour laquelle vous ne pouvez pas entrer dans cette partie du Web. Si jamais vous arrivez à y accéder, soyez prudent avec ce que vous faites*[195] ». Evidemment, le Marianas est un mythe qui a été créé à partir des fantasmes qui existent autour du Darknet[196], qui lui n'en est pas un.

À travers des articles moralisateurs et des tribunes grandiloquentes, le Darknet est devenu « *l'endroit du mal* ». Il y a une peur de l'inconnu malgré les avantages qu'il apporte. Il s'agit donc de le démystifier en essayant de comprendre ce qu'il représente réellement, en essayant de définir des mécanismes dynamiques de la plus simple des manières. Oubliez les récits sensationnalistes, les légendes urbaines, les théories qui permettent de faire le buzz autour du

[194] La fosse des Mariannes.
[195] ELBAKKALI A., Le Marianas web et les autres niveaux du Darknet/Web profond. Disponible à cette adresse : https://www.parlonsgeek.com/marianas-web-les-autres-niveaux-du-darknet-web-profond/, [consulté le 5 avril 2015].
[196] BLUE V., *The myth of Marianas web the darkest cornet of the Internet*, 18 décembre 2015. Disponible à cette adresse : https://www.engadget.com/2015/12/18/the-myth-of-marianas-web-the-darkest-corner-of-the-internet/, [consulté le 4 novembre 2014].

Darknet. Dans les faits, ce terme controversé n'est pas aussi impressionnant. Pour certains, le Darknet est la face sombre du Web, pour d'autres, c'est une zone du cyberespace dans laquelle la protection de la vie privée serait assurée. Mais en réalité, il s'agit d'un mélange des deux.

Les pirates et cyber-criminels sont attirés par certaines communautés du Web sombre qui leur permettent de partager des informations et de conclure des affaires sans crainte de représailles, d'autant plus qu'il est difficile de trouver quelles sont les lois à appliquer dans ce cas. Alors que les autorités tentent d'envisager une répression efficace, des recherches montrent que les marchés illégaux sur le Web sombre génèrent des millions de dollars chaque année.

Toutefois, il convient de préciser que les infractions commises ne sont pas inhérentes au Darkweb. Le trafic d'armes ou de stupéfiants, le blanchiment d'argent, l'escroquerie, la pédophilie, le terrorisme sont avant tout des problèmes sociaux se retrouvant sur cette partie du web qui leur octroie quelques particularités. Ainsi, le Darknet est à l'image de la société humaine. En réalité en dehors de ces infractions, le contenu du Darknet n'est pas si dangereux que cela. Il est possible d'y trouver des sites politiques, des blogs, des livres, des sites consacrés à la musique ou au cinéma, des radios, des documentaires qui montrent des individus se baladant dans les catacombes de Paris… Il y a même des forums de discussion dédiés aux conseils sexuels. Ce chapitre sera l'occasion de renverser les légendes qui existent à propos du Darknet en montrant qu'il garantit une protection de la vie privée (section 1) et qu'il n'est pas si sombre que cela (section 2).

SECTION 1
Le Darknet, garant de la vie privée

L'article 9 du Code civil dispose que « *chacun a droit au respect de sa vie privée* » et donne aux juges les moyens de faire cesser, le cas échéant en urgence, toute atteinte à la vie privée. Cette disposition générale s'accompagne aujourd'hui de diverses dispositions spéciales qui organisent la protection de la vie privée ou l'inimité de celle-ci.

Cette notion de la vie privée nécessite une étude liée à l'Internet utile aux internautes qui aspirent à défendre leurs droits dans un monde où la sécurité semble inexistante. En étant devant son ordinateur, un utilisateur pense être dans sa sphère privée. Pourtant, un manque de sécurité peut faire en sorte qu'il ouvre son espace privé au monde entier sans réellement comprendre ce que cela implique. En ouvrant une application sur son Smartphone, un utilisateur se demande-t-il où vont finir ses données de localisation ou de consultation ? *Facebook*, *Google* sont des systèmes de surveillance ; chaque fois qu'un internaute utilise un service gratuit, il n'est pas client mais produit. Certains n'en ont pas conscience, alors que d'autres admettent l'idée qu'ils sont surveillés et se disent qu'ils ne font rien d'illégal si bien qu'ils n'ont rien à cacher.

C'est donc dans un rapport de confiance que se trouvent le respect de la vie privée et la confidentialité des données et qu'apparaissent les limites à l'anonymat sur Internet. Dans sa décision sur la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers[197], le Conseil Constitutionnel estime qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent le respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789[198]. En somme, le Darknet est une arme permettant de lutter contre la collecte massive des données (§1) grâce à l'anonymat qu'il garantit (§2).

[197] Conseil constitutionnel, 19 janvier 2006, Décision n° 2005-532.
[198] Le Conseil constitutionnel estime que le droit au respect de la vie privée est protégé par l'article 2 de la Déclaration de 1789. Conseil constitutionnel, 29 novembre 2013, n° 2013-357 QPC.

§1) Une arme contre la collecte des données

Qu'est-ce qu'une surveillance de masse ? Concrètement, il s'agit d'une surveillance mondialisée mise en place sur des populations entières sans égard pour les frontières. L'existence de ce genre de pratique n'a été largement reconnue qu'après la mise en lumière des révélations de Snowden qui ont suscité un débat politique international quant au droit à la vie privée à l'époque du numérique. Par ailleurs, ces révélations ont créé des discordes entre les Etats-Unis et ses partenaires économiques et alliés.

Sur Internet les données sont infinies et ce n'est pas la liberté de communication en ligne qui va permettre une atténuation de ce phénomène. La transparence numérique totale est impossible et ceux qui s'en réjouissent mettent en avant le fait que cela permettrait à certains de rester impunis. Mais, à une époque où les données personnelles sont valorisées, le chiffrement des données est un moyen de protection légal permettant de prévenir les atteintes à la vie privée en empêchant l'identification des données de manière irréversible. Les utilisateurs sont en effet confrontés à des risques d'exposition de leurs données sans en avoir été informés et préfèrent se tourner vers de nouvelles méthodes telles que le chiffrement ou l'anonymat.

Néanmoins, aussi légale soit-elle, la technique de chiffrement est complexe si bien qu'elle n'est pas accessible à tous et reste limitée. Dans le Code pénal, deux parties distinctes organisent les atteintes aux personnes résultant des fichiers ou traitements informatiques et les atteintes à la vie privée. Dans le Chapitre VI du titre II relatif aux atteintes à la personnalité, ces dernières se trouvent à la section I, tandis que les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques dans la section V. Une vision claire des infractions du cyberespace, avec par exemple un chapitre du Code pénal dédié à ce genre d'infractions, semble nécessaire.

Pourtant, même si la notion d'anonymat n'y figure pas, le terme cryptologie est utilisé. L'article 434-15-2 fait référence à la cryptologie : « *est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités*

judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale ». Mais, cet article porte atteinte aux droits des individus tels que le droit de ne pas contribuer à sa propre incrimination ou le droit au silence. La recherche d'un équilibre entre les droits de chacun et la sécurité de tous doit être effectuée. L'encadrement est fixé par la loi qui est intervenue en la matière puisque les internautes sont restreints quant à l'utilisation de la cryptologie, mais le législateur a également tenté de limiter la libre circulation des données avec le Règlement général sur la protection des données personnelles.

L'activité des internautes n'est pas sans conséquence dans la mesure où des traces numériques sont laissées sur Internet. Ces traces, données à caractère informatif, peuvent permettre l'identification d'un utilisateur. Ainsi, les innovations sur Internet peuvent être dérivées afin de porter atteinte à la vie privée et à l'anonymat. Il existe de plus en plus de moyens d'identification dans le cyberespace. A titre d'exemple, l'adresse IP, sorte de numéro d'identification attribué au terminal de l'internaute, est considérée comme une donnée à caractère personnel par la jurisprudence [199] : « *la collecte pendant plusieurs années, d'adresses IP qui permettent l'identification des utilisateurs constitue un traitement automatisé de données à caractère personnel contenu dans un fichier lequel doit donner lieu à déclaration à la CNIL* ».

Voté le 27 avril 2016, le Règlement général sur la protection des données personnelles, dit RGPD, est entré en vigueur le 25 mai 2018 et a abrogé l'ancienne directive européenne 95/46/CE[200] et une grande partie de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. D'aucuns considèrent qu'il s'agit d'une énorme avancée. Les règles protégeant l'intégrité de l'identité des utilisateurs et les atteintes à leur vie privée sont renforcées. Pour plus d'efficacités, le RGPD s'inscrit dans la continuité de la directive européenne mais présente de nombreux changements. Il s'agit d'un règlement européen si bien que contrairement à une directive, il ne nécessite pas de transposition dans les Etats membres. Il encadre, au niveau européen[201], la collecte et l'utilisation des données relatives aux salariés, administrés et clients. Le renforcement des droits des personnes et de la confiance, éléments

[199] Cour de cassation, 1ère chambre civile, 3 novembre 2016, 15-22595.
[200] Relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[201] Plus précisément au sein de l'Union Européenne et de ses 28 Etats membres.

essentiels au développement économique et à l'innovation, est la pierre angulaire des 99 articles de la réforme. A cet égard, la Commission européenne a précisé que « *s'ils n'ont pas totalement confiance, les consommateurs hésiteront à faire des achats en ligne et à recourir à de nouveaux services. Cela risquerait de ralentir l'innovation dans l'utilisation des nouvelles technologies*[202] ».

Le règlement poursuit des objectifs bien établis. Il tend à renforcer les droits des utilisateurs qui auront le droit à la portabilité de leurs données personnelles leur permettant de les récupérer et de les réutiliser. Ensuite, le règlement aspire à une responsabilisation des acteurs traitant les données. Enfin, il vise à faire coopérer les autorités en matière de traitement des données. Elles seront amenées à prendre des décisions communes pour les cas transnationaux. La complexité de ce récent texte va compliquer son application tant pour les entreprises que pour les citoyens, c'est la raison pour laquelle certains utilisateurs préfèrent se fier à des méthodes de chiffrement pour échanger leurs informations et à l'utilisation du Darknet afin d'être anonyme (§2).

[202] Proposition de Règlement RGPD, COM(2012)11 final, Bruxelles, 25 janvier 2012.

§2) L'anonymat

L'article 4 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 dispose que « *la liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi* ». Des droits et des libertés existent sur Internet mais l'Etat est chargé de maintenir l'ordre public en intervenant sur Internet conformément aux textes qui lui permettent d'agir. L'anonymat se trouve alors au cœur d'un débat confrontant gouvernements, organisations internationales et citoyens. Il semble nécessaire à la préservation du respect de la vie privée et de la liberté d'opinion dans la cybersphère[203] mais le fait de ne pas révéler son identité peut compliquer la mission d'intérêt général assumée par l'Etat. En plus d'être limité par le droit et les points de vue opposés, le droit à l'anonymat est confronté aux développements des nouvelles technologies de l'information et de la communication dont fait partie le Darknet. Les questions relatives à l'anonymat sont un réel enjeu de modernisation de nos sociétés, notamment en raison de l'expansion des réseaux sociaux, des plateformes de *microblogging*[204], mais surtout des dispositifs de surveillance ayant créé un besoin affirmé des utilisateurs. Pour certains, être anonyme sur Internet est devenu une nécessité. L'anonymat, dont les contours semblent aléatoires, peut être défini comme « *l'état d'une personne, d'une chose dont on ignore le nom, l'identité*[205] ».

Autrement dit, l'anonymat sur Internet permettrait de rester inconnu, de ne pas être identifiable, ce qui garantirait le respect de sa vie privée et permettrait de faire face à la censure et aux restrictions. Tout ce qui est fait sur Internet peut avoir une répercussion car après chaque connexion, les robots de *Facebook* sont capables d'interpréter les vidéos et photos publiés et reconnaître un individu sur une photo sur laquelle on ne voit que son dos. Les logiciels espions, aussi appelés *spyware*, peuvent collecter toutes sortes d'informations sur l'environnement dans lequel l'internaute s'est installé. Son adresse IP, ses *cookies*[206], ses habitudes de connexion

[203] L'espace comprenant la totalité des sites web accessibles via Internet.
[204] Le *microblogging* est une sorte de blog simplifié permettant à l'utilisateur de poster des messages dont le nombre de caractère est limité. Twitter est la plateforme de microblogging la plus connue.
[205] Définition disponible à cette adresse : http://www.cnrtl.fr/definition/anonymat.
[206] Petit fichier conservant des informations sur l'internaute, à son insu et en vue d'une connexion ultérieure.

peuvent être utilisés à diverses fins, notamment publicitaires[207]. Les révélations d'un programme de surveillance[208] mené par la NSA ont montré que des géants comme *Google*, *Yahoo* ou encore *Facebook* étaient mêlés à ce programme. Ces données techniques sont ensuite interprétées grâce au *Big data* et au *Machine Learning*. Le premier constitue toutes les données devenues si volumineuses qu'elles dépassent l'intuition humaine et les capacités informatiques en matière d'analyse et de gestion de l'information et des bases de données. Cette explosion numérique de la donnée a créé un véritable écosystème économique impliquant les technologies de l'information. Le second utilise des algorithmes performants afin de doter les machines de reconnaissance d'objets, de perception de l'environnement… Par exemple, une donnée GPS pourra être associée à des recherches sur *Yahoo*, à des sites visités et même à des conversations instantanées afin de vous proposer une publicité susceptible de vous intéresser.

Dans ce contexte, anonymat serait synonyme de sécurité. Il existe plusieurs options pour devenir anonyme sur Internet. Toutes ne se valent pas. La première option est l'utilisation d'un serveur proxy qui est une sorte de serveur mandataire se connectant au site à la place de l'utilisateur qui ne le visite pas directement et qui n'est donc pas connu. Néanmoins, le proxy doit retransmettre les données à l'utilisateur et c'est là que réside une difficulté. En effet, la retransmission des données peut être longue et supposer une attente supplémentaire par rapport à sa propre connexion pour accéder au site. Par ailleurs, il faut savoir que les proxys ne garantissent pas un anonymat total. Le serveur mandataire peut révéler l'adresse IP de l'utilisateur ou espionner ses activités sans qu'il ne s'en doute.

La deuxième option est l'utilisation d'un réseau privé virtuel appelé VPN. Ce genre de réseau repose sur un protocole particulier cryptant les données échangées entre plusieurs ordinateurs. Il permet le chiffrement des protocoles HTTP, FTP[209] et IMAP[210]. Les informations ne sont pas lisibles durant le transfert puisqu'elles sont chiffrées par le VPN utilisé par le périphérique qui peut aussi bien être un ordinateur, un smartphone ou un routeur. Ce chiffrement est établi du

[207] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 37 : encore appelés « Spyware » en anglais, ils correspondent à un terme générique désignant les logiciels espions qui s'introduisent dans un système informatique afin de recueillir à des fins commerciales le profil d'un utilisateur au regard de sa navigation sur le réseau Internet… ».
[208] Appelé *PRISM*.
[209] Pour transférer des fichiers.
[210] Pour accéder à ses mails.

périphérique jusqu'au fournisseur d'accès internet qui ne peut pas vérifier le contenu des données. Le fournisseur d'accès internet renvoie ensuite les données au VPN par le biais d'internet. C'est à ce moment là que les données seront déchiffrées et renvoyées à leur destination. Par ailleurs, le VPN assure un anonymat en changeant la localisation et l'adresse IP de l'utilisateur. En effet, un VPN permet d'obtenir des adresses IP anonymes localisées dans des centaines de pays, d'accéder aux sites censurés et de crypter les données envoyées. Par conséquent, ce système permet de chiffrer les données et d'être anonyme. Toutefois, cette option repose sur le prestataire qui doit être de confiance pour garantir un réel anonymat et a un coût[211]. Le VPN enregistre les adresses IP utilisées pour visiter leur site et peuvent les transmettre en cas de réquisition judiciaire par exemple.

La troisième option est l'utilisation d'un darknet, qui permet à un utilisateur de transiter par plusieurs nœuds dans le monde. Chaque connexion entre les nœuds est fondue dans la masse si bien qu'il est difficile de retrouver l'utilisateur initial.

Les rapprochements entre anonymat et vie privée sont plaisants. Cette dernière peut également être perçue sous un aspect sécuritaire. Dans beaucoup de pays, il existe des règles sanctionnant l'ingérence du gouvernement dans la vie privée mais ces règles ne sont pas toujours appliquées. Certains pays demandent à leurs citoyens de révéler des informations considérées comme privées dans d'autres. Les défenseurs de la vie privée luttent contre la collecte de données sur les individus afin d'éviter l'apparition d'une « *société de contrôle* » et un droit à l'anonymat pourrait être la solution. Il convient alors de se demander si la société française ne tend pas vers un droit à l'anonymat (A) et de montrer dans quelles mesures l'anonymat est encadré (B).

A) Vers un droit à l'anonymat

En 2008, beaucoup défendent le besoin de la reconnaissance d'un droit à l'anonymat de l'expression sur le réseau Internet. L'article 5 de la Déclaration des Droits de l'Homme et du Citoyen prévoit que « *tout ce qui n'est pas défendu par la Loi ne peut être empêché, et nul ne peut être contraire à faire ce qu'elle n'ordonne pas* ». L'anonymat n'étant pas proscrit de manière générale, le droit à l'anonymat existe. A l'âge numérique, l'utilisation d'un pseudonyme permet d'exercer ce droit (1) mais la législation est en retard face au Big data (2).

[211] Une dizaine d'euros par mois pour un bon VPN.

1. L'utilisation d'un pseudonyme

A l'heure des mémoires numériques, la question d'un droit à l'hétéronymat se pose. Il s'agirait de reconnaître légalement une identité numérique alternative distincte de la personnalité civile garantissant notamment le droit à un nom, à un prénom et à une nationalité. Dans cet environnement 2.0 où liberté d'expression numérique et droit au respect de la vie privée sont confrontés, l'anonymat peut être consolidé par l'utilisation d'un pseudonyme. Sur le web, ce dernier, défini comme le « *nom choisi par une personne pour masquer son identité* », s'exprime principalement à travers le *login*[212] permettant de créer une infinité de noms. D'après le site du gouvernement[213], dans la vie réelle, « *les conditions d'utilisation d'un pseudonyme ne font l'objet d'aucune réglementation particulière. Il s'agit d'un nom d'emprunt, librement choisi par une personne pour dissimuler au public son identité réelle dans l'exercice d'une activité particulière. Le pseudonyme est notamment utilisé dans le domaine littéraire ou artistique* ». Pourtant, le recours au pseudonyme est une liberté très encadrée si bien qu'il est possible d'envisager des poursuites contre le titulaire du pseudonyme. Par exemple, « *il est interdit d'exercer la médecine sous un pseudonyme*[214] » , « *il n'est pas possible d'inscrire un pseudonyme sur un passeport*[215] » et le pseudonyme peut même être assimilé à un faux nom lorsqu'il a été utilisé dans le cadre d'une escroquerie[216].

De plus, l'utilisation d'un pseudonyme sur Internet peut être proscrite. *Facebook* lutte par exemple contre l'utilisation des pseudonymes avec des conditions d'utilisation non équivoques : « *les personnes qui utilisent Facebook donnent leur vrai nom et de vraies informations les concernant* ». Les procédures de vérification de l'identité de ses membres sont une priorité et le réseau social a même acheté *Confirm.io,* une enseigne dont la spécialité est la vérification de pièces d'identité. Cette chasse au « *pseudonymat*[217] », ayant pour prétexte le contrôle des commentaires sur Internet, est loin de faire l'unanimité dans la mesure où elle porte clairement atteinte au droit à l'anonymat. Le Comité des ministres du Conseil de l'Europe s'est

[212] Ce terme anglais désigne l'identifiant permettant de se connecter sur un système informatique ou un site web.
[213] Disponible à cette adresse : https://www.service-public.fr/particuliers/vosdroits/F355.
[214] Code de la santé publique art. R.4127-75.
[215] Disponible à cette adresse : https://www.service-public.fr/particuliers/vosdroits/F355.
[216] Code pénal art. 313-1.
[217] Dérivé des termes pseudonyme et anonymat, ce néologisme désigne l'état d'une personne dont on ne connaît que le nom d'emprunt, le pseudonyme.

penché sur la question en exprimant plusieurs recommandations relatives au droit à l'utilisation d'un pseudonyme[218] : « *le droit d'utiliser un pseudonyme devrait être garanti à la fois au regard de la liberté d'expression et du droit de communiquer et de recevoir des informations et des idées, et du droit au respect de la vie privée* ». Ces recommandations « *constituent un idéal à atteindre dont le Cour Européenne des Droits de l'Homme s'inspire pour faire évoluer sa jurisprudence*[219] », mais elles n'ont pas de valeur contraignante si bien qu'il serait opportun de légiférer sur cette question du pseudonyme directement liée à l'anonymat et à la liberté d'expression sur Internet (2).

2. Une législation en retard sur la technologie

Qu'est-ce que l'anonymat ? Existe-t-il un droit à l'anonymat spécifique à l'internet, un droit à l'anonymat de l'expression qui serait un prolongement de la liberté d'expression ? A titre d'exemple, en Allemagne la jurisprudence a estimé que ce droit à l'anonymat sur Internet relevait de la liberté d'expression protégée par la Loi Fondamentale[220]. La question se pose à une époque où les nouvelles technologies menacent l'anonymat.

Le *Big Data* qui a opéré de nombreux changements comportementaux est décrit par certains comme une nouvelle révolution industrielle comparable à la découverte de la vapeur, de l'électricité ou de l'informatique, mais il serait plus opportun de la qualifier de troisième étape de la dernière révolution industrielle. Ce phénomène est né à l'occasion de l'explosion quantitative des données numériques qui a contraint les chercheurs à trouver de nouvelles manières d'analyser le monde numérique. De nouveaux ordres de grandeur ont été découverts et ont permis un croisement massif des données à une échelle démesurée. Ainsi, la notion de *Big Data* désigne littéralement un ensemble de données massives quasi infinies correspondant à des informations publiées et échangées par les internautes. Ce système emporte des avantages mais aussi des inconvénients. Les enjeux sont énormes puisque grâce à des algorithmes il serait possible de prédire et anticiper des faits juridiques, sociaux et économiques tels que l'évolution

[218] Les recommandations sont adoptées en par le Comité des Ministres du Conseil de l'Europe et transmises aux gouvernements des Etats membres.
[219] PAILLER L., *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, 2012, page 61.
[220] Arrêt rendu par la cour d'appel de Hamm le 3 août 2011. Disponible à cette adresse : http://www.justiz.nrw.de/nrwe/olgs/hamm/j2011/I_3_U_196_10beschluss20110803.html, [consulté le 4 avril 2015].

du chômage, des grèves ou des décisions de justices. Cependant, le phénomène pose des problèmes de stockage qui ont nécessité la mise en place de modèles de stockage comme le *cloud* mettant encore plus en danger l'anonymat, mais aussi le secret des correspondances et le secret professionnel notamment.

La législation semble pourtant incompatible avec les analyses *Big Data*. En ce sens l'article 10 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose qu'aucune « *décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ». Cet article tend encore une fois à limiter l'insécurité juridique dans un univers où l'éparpillement des données personnelles empêche un réel contrôle de celles-ci. C'est dans ce contexte que l'anonymat est en danger (B).

B) L'encadrement de l'anonymat

Les adversaires de la liberté d'expression sont multiples. Les abus tels que la censure, le filtrage, le détournement de trafic ou les listes noires, doivent être combattus. Grâce à l'anonymat qu'il garantit, le Darknet est une arme efficace. Cependant, nombreuses sont les personnalités politiques, de gauche ou de droite, s'étant prononcées sur la question du règne de l'anonymat à une époque où la législation sur les nouvelles technologies de l'information et de la communication est au cœur des débats. Les textes sont éparpillés et les nombreuses opinions différentes, voire opposées.

En 2013, lors de la réception du Conseil représentatif des institutions juives à l'Elysée, François Hollande, ancien président de la République, entend lutter contre « *la tranquillité de l'anonymat qui permet de dire des choses innommables sans être retrouvé* »[221]. Très active sur les réseaux sociaux, Nadine Morano, ancienne ministre, a également fait part de sa volonté de lutter contre

[221] CLAVEL G., Anonymat sur Internet : pourquoi les politiques sont contre et pourquoi ils ne peuvent rien faire, 17 décembre 2013. Disponible à cette adresse : http://www.huffingtonpost.fr/2013/12/17/anonymat-internet-hollande-gages-reelles-solutions_n_4457659.html, [consulté le 17 décembre 2015].

l'anonymat : « *voilà longtemps que j'ai pris position contre l'anonymat sur internet devenu le déversoir de haine et de violence* »[222].

L'idée de créer une loi spécifique aux réseaux sociaux a été envisagée par le pouvoir politique mais cette prise de conscience est longtemps restée du domaine de la fiction. L'anonymat total doit être contrôlé. En effet, Harlem Désir, ancien premier Secrétaire du Parti socialiste, s'est exprimé en 2013 en reconnaissant l'impuissance du Parlement face à ce phénomène : « *c'est un travail qui doit être fait sur le plan international, parce qu'il y a des comptes qui sont hébergés ailleurs notamment aux Etats-Unis. Faire en sorte qu'internet, qui est un formidable outil d'échanges, de communication, de liberté, ne soit pas un lieu où ce qui est interdit, c'est-à-dire la haine, la haine raciale, l'incitation à la violence, puisse se diffuser* », expliquait-il. La même année, Manuel Valls, alors ministre de l'Intérieur, est intervenu lors du Forum international de la Cybersécurité pour dénoncer les dangers de l'anonymat sur internet : « *Sur la toile se déploie une criminalité qui peut mettre en péril des pans entiers de nos économies, de la souveraineté des États [...] la discrétion voire l'anonymat permis par internet, la difficulté à établir des preuves, la facilité d'utilisation et les profits rapides et élevés sont des facteurs aggravants* » estime le ministre qui met en avant une cybercriminalité « *industrialisée, organisée et mondialisée* ».[223] Le concept d'*Habeas Corpus Numérique* a été évoqué à plusieurs reprises afin de désigner les règles visant à concilier les nouvelles technologies de l'information et de la communication avec la sécurité et le respect des libertés individuelles. Cette formule a été envisagée par François Zimeray, avocat et homme politique français, qui définit l'*Habeas Corpus numérique* comme « *l'ensemble des règles et principes applicables au domaine des technologies de l'information et du stockage de données numériques, visant à rendre compatible le développement de la société de l'information avec le respect des droits individuels et des libertés fondamentales* ».

En tout état de cause, la peur de l'anonymat a conduit à un recul significatif du respect de la vie privée et à des atteintes à l'anonymat récurrentes et aux motifs très vagues. Il est vrai qu'en droit administratif français, l'ordre public, assuré par l'Etat, implique la tranquillité publique,

[222] Twitter, le 16 décembre 2013.
[223] LAMENDE M-J., *FIC : Manuel Valls souhaite évaluer la cybercriminalité au plus juste*, janvier 2013. Disponible à cette adresse : https://www.globalsecuritymag.fr/FIC-Manuel-Valls-souhaite-evaluer,20130130,35132.html, [consulté le 19 septembre 2015].

la salubrité publique, la moralité publique[224], la dignité de la personne humaine[225] et la sécurité publique. Néanmoins, cet objectif d'intérêt général ne doit pas être un prétexte pour porter atteinte à certains droits et libertés telles que la liberté d'expression (1), grâce à de nouvelles lois comme la loi pour la confiance dans l'économie numérique (2).

1. Une liberté d'expression limitée

La loi sanctionne certaines opinions lorsqu'elles sont assimilables à de l'antisémitisme ou à du racisme, et ce, malgré l'existence de la liberté d'expression[226] qui a pour corollaire la liberté de la presse, la liberté d'information ou encore la liberté d'opinion. Cette dernière liberté fondamentale a valeur constitutionnelle puisqu'elle est énoncée par l'article 10 de la Déclaration des droits de l'Homme et du citoyen de 1789 énonçant que « *nul ne doit être inquiété pour ses opinions, même religieuses* ». Cependant, à l'instar de toutes les libertés fondamentales, elle comporte nécessairement des limitations puisque le même article prévoit que la manifestation de cette opinion ne doit pas troubler « *l'ordre public établi par la loi* ». En outre, elle se heurte également au respect de la vie privée reconnu en France et à l'international. Dans une société démocratique telle que la France, la conciliation de ces droits fondamentaux est conflictuelle et force les juges du fond à procéder de manière casuistique à une mise en balance des intérêts d'espèce. Le droit au respect de la vie privée et le droit à la liberté d'expression ont la même valeur normative si bien qu'il appartient au juge de rechercher un équilibre entre ces deux droits afin de protéger l'intérêt le plus légitime.

En tout état de cause, la liberté d'expression telle qu'envisagée en France, n'autorise pas la censure préalable et ne sanctionne les abus de cette liberté qu'a posteriori. De plus, le juge ne peut interdire une publication sur internet qu'en dernier ressort. Ces règles sont les mêmes sur le Darknet même si la marge de manœuvre du juge est plus limitée dans le sens où l'identification de l'éditeur peut poser problème. Par principe, la loi répond aux propos racistes sanctionnés en fonction de leur gravité. A titre d'exemple, une circonstance aggravante est prévue lorsqu'ils sont tenus en public. Il en découle la nécessité de se demander dans quelles mesures internet peut-il être considéré comme public, notamment à la suite de l'expansion des

[224] Conseil d'Etat, *Société Les films Lutetia*, 18 décembre 1959.
[225] Conseil d'Etat, *Commune de Morsang-sur-Orge*, 27 octobre 1995.
[226] Convention de sauvegarde des droits de l'Homme et des libertés fondamentales art. 10 : « Toute personne a droit à la liberté d'expression ».

réseaux sociaux ?

Concrètement, les courriels, envoyés ou non via un darknet, sont des correspondances privées n'ayant pas un caractère public. Mais, la donne est différente sur un réseau social où un message peut être considéré comme public lorsqu'il est accessible à un grand nombre de personnes. Tout est une question de paramétrage. Dès lors, sur Twitter, si le compte est public, tous les tweets le sont également et sur Facebook, une publication est publique lorsqu'elle est ouverte aux paramètres « *tout le monde* » ou « *amis des amis* ». La Cour de cassation a eu à se prononcer sur un tel cas : « *que les propos litigieux avaient été diffusés sur les comptes ouverts par Mme Y... tant sur le site Facebook que sur le site MSN, lesquels n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressée, en nombre très restreint, la cour d'appel a retenu, par un motif adopté exempt de caractère hypothétique, que celles ci formaient une communauté d'intérêts ; qu'elle en a exactement déduit que ces propos ne constituaient pas des injures publiques ; que le moyen n'est pas touché en ses quatre premières branches*[227] ».

Récemment, la Cour de cassation[228] s'est à nouveau prononcée à ce propos en dégageant une solution allant plutôt dans le sens de la protection de la vie privé. Dans ce contexte, l'idée de la liberté de communication électronique se dessine. Elle tend à évoluer en liant d'une part les libertés d'expression et d'opinion et d'autre part, la liberté de communication en ligne. La législation française le montre clairement. Il est en effet possible de citer la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet. Composée de six chapitres, cette loi est surtout connue pour la création de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet[229] et pour sa volonté de mettre un terme aux partages de fichiers *p2p* lorsqu'ils enfreignent la législation relative aux droits d'auteur. Cette loi est due à la transposition d'une directive européenne 2001/29/CE tendant à la protection des droits d'auteur sur Internet.

De nombreux passages devant plusieurs instances Etatiques ont été nécessaires. À cette occasion, dans l'ordre, la Commission nationale de l'informatique et des libertés, le Sénat,

[227] Cour d'appel de Reims, 12 février 2014 n° 12/02936 ; Cour de cassation, 1ère chambre civile, 10 avril 2013 n° 11-19.530.
[228] Cour de cassation, chambre sociale, 20 décembre 2017 n°16-19609.
[229] Hadopi.

l'Assemblée Nationale, une commission mixte paritaire[230] et l'Assemblée Nationale une seconde fois, ont étudié cette disposition. Mais, c'est le juge constitutionnel qui a permis l'évolution de la liberté de communication en ligne. L'étude de la loi du 12 juin 2009 lui a permis d'énoncer qu'en « *l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services* ». Ce faisant, la vie démocratique et la liberté d'expression et d'opinion incluent un autre droit, celui d'accéder à des services de communication en ligne. Mais, comme pour toutes les libertés, il faut fixer des contours. Le Conseil constitutionnel a ainsi reconnu une limite concernant la pédopornographie à l'occasion de l'entrée en vigueur de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure. L'article 4 de cette dernière a modifié l'article 6 de la loi LCEN à propos de l'article 227-23 du Code pénal portant sur la pédopornographie : « *lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai* ». Mais, saisi par soixante députés et soixante sénateurs qui estimaient « *d'une part, que l'institution d'un dispositif de blocage des adresses électroniques donnant accès à certains sites internet constitue une mesure inappropriée voire contreproductive et d'un coût excessif au regard de l'objectif poursuivi de lutte contre la diffusion d'images pédopornographiques ; que, d'autre part, en l'absence d'autorisation judiciaire, l'atteinte portée à la liberté de communication par l'impossibilité d'accéder à ces sites serait disproportionnée* » ; le Conseil constitutionnel a dû se prononcer sur la constitutionnalité de cet article par une décision du 10 mars 2011[231]. En le déclarant conforme à la Constitution, le Conseil constitutionnel a bel et bien établi une limite relative au contenu pédopornographique. Ainsi, le législateur justifie la limitation de l'anonymat sur internet par la prévention des atteintes à l'ordre public. En ce sens, l'article 6-II alinéa 1er de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie

[230] Conformément à l'article 45 de la Constitution de 1958, cette commission, composée de sept sénateurs et de sept députés, est réunie en cas de désaccord entre le Sénat et l'Assemblé nationale sur une proposition de loi ou un projet.
[231] Conseil constitutionnel, 10 mars 2011, n°2011-625 DC, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*.

numérique, dispose que « *les personnes mentionnées aux 1 et 2 du I*[232] *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* » (2).

2. La loi pour la confiance dans l'économie numérique

En France, à la suite d'une transposition de la directive 2000/31/CE[233] du 8 juin 2000 sur le commerce électronique[234], celle du 21 juin 2004, abrégée sous le signe LCEN, a permis de dégager une certaine tendance en mettant en place plusieurs régimes applicables selon la qualité de l'acteur impliqué. Il peut en effet s'agir d'un hébergeur, d'un fournisseur d'accès à internet, d'un éditeur de contenus… Lorsqu'ils éditent à titre non professionnel, ces derniers sont visés par la l'article 6 de la loi LCEN. Concrètement, ce sont les internautes qui créent du contenu en ayant la faculté de rester anonyme, du moins, en apparence. Un bloggeur anonyme a, par exemple, cette possibilité s'il a préalablement transmis à son hébergeur internet[235] certaines informations nécessaires à son identification et mis à la disposition de ses internautes les coordonnées de cet hébergeur. En tant que garant des libertés individuelles, seul le juge pourra demander la levée de l'anonymat de l'internaute qui peut avoir des conséquences néfastes. Une politique de sécurité efficace doit nécessairement passer par un diagnostic précis et une réflexion quant à la formation de nouveaux enquêteurs qui doivent être en mesure de contrer l'anonymat. Dès lors, la coordination des actions de chacun des acteurs de la chaîne pénale ainsi que la simplification et la réunification des normes doivent être au centre des débats. Il s'agit de trouver le juste équilibre permettant de concilier, d'une part, le respect de grands principes tels que les garanties de la vie privé et la liberté d'expression et d'autre part, les exigences en matière de lutte contre la cybercriminalité. En effet, l'anonymat est porteur de promesses pour les libertés individuelles, mais il constitue également une menace de certains droits fondamentaux en ce qu'il peut être utilisé pour l'incitation à la haine ou l'écrasement de la diversité culturelle.

[232] Les hébergeurs.
[233] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.
[234] Et de certaines dispositions de la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques.
[235] Un hébergeur internet met à disposition des internautes des sites web gérés et conçus par des tiers. Les fournisseurs d'accès proposent souvent ce genre de service.

L'arsenal juridique français permet de lutter contre ce genre de pratique. Ainsi, l'article 225-1 du Code pénal dispose que « *toute distinction opérée entre les personnes physiques à raison de leur origine, de leur sexe, de leur situation de famille, de leur grossesse, de leur apparence physique, de leur patronyme, de leur état de santé, de leur handicap, de leurs caractéristiques génétiques, de leurs mœurs, de leur orientation ou identité sexuelle, de leur âge, de leurs opinions politiques, de leurs activités syndicales, de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée (...)* ». L'article 24 de la loi du 29 juillet 1881 punit « *ceux qui auront provoqué à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminées, de leur sexe, de leur orientation sexuelle ou de leur handicap* ». Toutefois, les poursuites ne sont possibles que si la victime ou une association spécialisée porte plainte avec constitution de partie civile. Le juge d'instruction ou le procureur[236], peut réquisitionner les enquêteurs pour contacter l'hébergeur du site afin qu'il transmette l'identité de l'éditeur.

C'est ainsi que les juges français ont été amenés à se prononcer sur une affaire de tweets antisémites le 12 juin 2013[237]. En l'espèce, à la suite d'un déferlement de messages antisémites et de l'utilisation des hashtags #UnBonJuif et #UnJuifMort, le réseau social Twitter est assigné en référé par plusieurs associations[238]. Ces dernières rappellent que Twitter qui dispose d'une filiale française, ne saurait se soustraire au respect « *des lois de police et de sûreté applicables à l'activité qu'elle déploie en France, à savoir l'exploitation de la version française du service de communication en ligne qu'elle édite et accessoirement le stockage de messages fournis par les destinataires de ces services* ». Elles s'appuient notamment sur l'article 6 de la loi LCEN qui impose aux intermédiaires techniques de conserver « *les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ». Twitter se défend en attestant que ses noms de domaines

[236] S'il n'y a pas de mise en examen.
[237] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 167.
[238] L'Union des étudiants juifs de France (UEJF), J'accuse ! (Action internationale pour la justice), SOS Racisme, le Mouvement contre le racisme et pour l'amitié entre les peuples (Mrap) et la Ligue internationale contre le racisme et l'antisémitisme (Licra).

et que son infrastructure technique et juridique sont gérés depuis les Etats-Unis et Twitter France « *a uniquement vocation à terme à jouer un simple rôle d'agence commerciale dans le cadre d'une mission marketing* », si bien que Twitter n'est pas tenu de conserver les données conformément au droit français. Cette stratégie est étonnante puisque Twitter se prive du statut protecteur offert par la loi LCEN et aimerait que la loi américaine, le « *Freedom of speech*[239] », lui soit applicable non seulement au Etats-Unis mais également en France. La société de droit américain s'est fondée sur les avis des CNIL européennes durant le G29[240] et estime que « *la seule présence sur le territoire français d'une antenne commerciale ne suffit pas à rendre les législations européennes sur la protection des données applicables* ». Dès lors, le traitement des données obéirait au droit américain. C'est l'analyse qui sera retenue par le tribunal de grande instance de Paris puisqu'un décret d'application de la loi LCEN prévoit que les données stockées soient conservées selon les exigences de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui n'a vocation à s'appliquer que si le responsable du traitement se situe en France : « *Les associations (...) ne démontrent pas que la société Twitter Inc. est établie en France ou utilise pour la conservation des données litigieuses les moyens, matériels ou humains de la société Twitter France ou de toute autre entité située sur le territoire français, autrement qu'à des fins de transit* ».[241] Le juge des référés s'est alors fondé sur l'article 145 du Code de procédure civile qui dispose que « *s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ». Cette dérogation au principe du contradictoire et à la nécessité d'un intérêt né et actuel comme condition de l'action en justice, est applicable en l'espèce puisqu'il s'agit de permettre l'identification des auteurs des tweets afin de les poursuivre pénalement même pour un litige international. Le tribunal de grande instance cite le Code pénal qui dispose qu'une infraction est « *réputée commise sur le territoire*

[239] La liberté d'expression aux États-Unis jouit d'un statut protecteur grâce au Premier amendement de la Constitution des Etats-Unis.
[240] L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales. Le G29 se réunit à Bruxelles en séance plénière tous les deux mois environ. Il a pour objectif de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays hors UE, de conseiller la Commission européenne sur tout projet ayant une incidence la protection des données et des libertés des personnes.
[241] Ordonnance du TGI de Paris, *UEJV contre Twitter*, 24 janvier 2013. Disponible à cette adresse : https://cdn2.nextinpact.com/medias/ordonnance-tgi-paris-24-janvier-2013-uejf-vs-twitter.pdf, [consulté le 19 octobre 2017].

de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire[242] » et ordonne « *à la société TWITTER INC de communiquer aux cinq associations en cause les données en sa possession de nature à permettre l'identification de quiconque a contribué à la création des tweets manifestement illicites dont les URL figurent au dispositif de l'assignation du 29 novembre 2012, qu'elle a rendus inaccessibles sur notification du 23 octobre 2012* ». Cette communication doit intervenir « *dans les quinze jours de la signification de la présente décision, et sous astreinte de 1000 euros par jour de retard passé ce délai* ».[243] Les contours des informations ne sont pas précisés par le jugement. La plateforme de *microblogging* semble avoir le choix entre transmettre les adresses IP ou des fichiers plus complets précisant les durées de connexion des utilisations. Une procédure devra ensuite être lancée par les associations pour que les fournisseurs d'accès internet donnent les coordonnées personnelles des auteurs des tweets litigieux.

Twitter interjette appel mais la Cour d'appel de Paris rend un arrêt confirmatif le 12 juin 2013.[244] Cette décision paraît justifiée au regard de plusieurs exigences. Tout d'abord, au regard des faits et des multiples impératifs sociaux, puisque l'indéniable réprobation qu'il faut accorder à ces écrits attentatoires à l'ordre public démocratique doit faire l'objet d'une réponse judiciaire efficace au lieu de sanctionner. Ensuite, au regard du droit, puisque l'utilisation de l'article 145 du Code de procédure civile est tout à fait opportune et permet de compenser les carences de la loi LCEN. La combinaison de ces éléments montre que les colosses comme *Twitter* ne doivent pas être au-dessus des lois et qu'il faut des moyens adaptés pour protéger les victimes. C'est l'occasion de faire un point sur la législation relative au web et plus particulièrement à l'anonymat en présentant la loi LCEN.

Les législateurs européens et français ont mis en place un régime aboutissant à un nouveau régime quant aux hébergeurs et aux éditeurs de contenus non professionnels qui utiliseraient *Twitter* ou *Snapchat*[245] par exemple. La loi LCEN tend à protéger les victimes de propos incitant à la haine tout en essayant d'instituer un régime protecteur de la liberté d'expression.

[242] Code pénal art. 113-2.
[243] Ordonnance du TGI de Paris, *UEJV contre Twitter*, 24 janvier 2013. Disponible à cette adresse : https://cdn2.nextinpact.com/medias/ordonnance-tgi-paris-24-janvier-2013-uejf-vs-twitter.pdf, [consulté le 19 octobre 2017].
[244] Cour d'appel de Paris, 12 juin 2013, n°13/06106.
[245] Lancée en 2011, cette application permet à l'expéditeur d'envoyer des images ou vidéos qui s'autodétruisent au bout d'une durée prédéfinie.

C'est le premier équilibre qu'il est possible de résumer. Les enjeux de cette loi sont d'encadrer l'anonymat afin d'autoriser une plus grande liberté d'expression dans un espace démesuré si bien qu'il serait possible de parler de droit à l'anonymat de l'expression. L'article 6 de cette loi [246] fixe un régime permettant une répartition des responsabilités entre les différents protagonistes de la communication en ligne.

D'abord, cet article définit les fournisseurs d'accès Internet comme des « *personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* ». Ensuite, il définit les hébergeurs[247] comme ceux « *qui assurent (...) le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature* ». Enfin, l'éditeur de contenu est présenté comme la personne « *dont l'activité est d'éditer un service de communication au public en ligne* ».

Toujours d'après l'article 6 de la loi LCEN, les premiers « *ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites* ». Il n'est donc pas possible de reprocher à l'hébergeur ou au fournisseur d'accès Internet d'avoir permis la diffusion de propos antisémites ou homophobes. En outre, contrairement aux éditeurs, la loi ne leur impose pas la mise en place d'un filtrage ou d'une censure car elle estime que leur activité revêt un caractère passif, technique et automatique ne permettant pas un contrôle systématique des informations échangées et stockées. A titre d'exemple, *Twitter* est bel et bien un hébergeur dans le sens où le réseau social offre les moyens techniques de répandre des informations et divers contenus tels que des photos, des vidéos etc. *Amazon*, une entreprise de commerce électronique basée à Seattle, contrôle chaque annonce mise en ligne et permet la recherche par le biais de mots clés pertinents tout en autorisant l'anonymat des vendeurs, ce qui implique sa qualité d'éditeur. Le premier a un rôle passif tandis que le second un rôle actif. Dès lors, l'éditeur a une obligation de contrôle impliquant une responsabilité quant au contenu diffusé sur son site (b) alors que l'hébergeur et le fournisseur d'accès internet bénéficient d'une responsabilité dite allégée (a).

[246] Dans le chapitre II intitulé « *les prestataires techniques* ».
[247] La loi ne définit pas textuellement les hébergeurs et fournisseurs d'accès internet mais le texte rejoint les définitions existantes.

a) La responsabilité des hébergeurs

La directive du 8 juin 2000[248] prévoyait une absence d'obligation générale en matière de surveillance : « *1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites* ». C'est ce qui a été prévu par l'article 6-I de la loi du 21 juin 2004 (∂). Toutefois, les droits communautaires et français prévoient une contrepartie, celle de permettre l'identification des internautes : « *2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement*[249] » (ß). L'objectif est de limiter la responsabilité des intervenants sans compromettre une éventuelle action qui permettrait le retrait ou l'inaccessibilité du contenu litigieux.

∂) Une responsabilité dite atténuée

Définis comme les personnes « *dont l'activité est d'offrir un accès à des services de communication au public en ligne* » ou 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 ou de messages de toute nature fournis par des destinataires de ces services* », les hébergeurs n'engagent pas directement leur responsabilité pour le contenu proposé par le biais de leurs services d'accès. En effet, les articles 6-I-6 et 6-I-7 de la loi LCEN dispose que « *les personnes mentionnées aux 1 et 2*[250] *ne sont pas des producteurs au sens de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication*

[248] http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32000L0031.
[249] Article 15-2 de la directive du 8 juin 2000.
[250] Ces alinéas visent les fournisseurs d'accès internet et les hébergeurs qui sont dont à l'abri de la qualification de producteur de contenu permettant d'emporter la qualité d'auteur principal pour les les infractions de presse visées au chapitre IV de la loi sur la liberté de la presse du 29 juillet 1881.

audiovisuelle » et « *ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites* ». En revanche, ils doivent retirer promptement le contenu illégal porté à leur connaissance.

En effet, les articles 6-I-2 et 6-I-3 de la loi LCEN disposent que « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible* » et qu'elles ne « *peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible* ». Ces articles 6-I-2° et 6-I-3° visent donc l'engagement des responsabilités civiles et pénales de l'hébergeur.

En appliquant un raisonnement *a contrario* il est possible d'en déduire que les hébergeurs « *engagent leurs responsabilités civile et pénale dès lors qu'ils ont eu connaissance du caractère illicite et qu'ils n'ont pas agi immédiatement pour retirer ces données* ». Ensuite, l'idée sous-jacente à l'énonciation « *si elles n'avaient pas effectivement connaissance de leur caractère illicite* » est que l'hébergeur peut ignorer le caractère illicite des contenus qu'il propose. Dès lors, sa réaction *a posteriori* n'est possible que si un tiers est intervenu pour indiquer à l'hébergeur que le contenu proposé est illégal. Cette intervention peut être le fait de l'autorité judiciaire ou d'un particulier. Il est alors demandé à l'hébergeur de « *retirer* » ou de « *rendre l'accès impossible* » aux donnés ou informations à caractère illicite.

Aussi, l'article 6-I-5 de la loi LCEN dispose que « *la connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants :*

-la date de la notification ;
-si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;
-les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;
-la description des faits litigieux et leur localisation précise ;
-les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;
-la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté ».

Cette présomption de connaissance permet aux tiers de contacter au préalable la personne à l'origine du contenu et de la prévenir que des démarches pourront être envisagées auprès de l'hébergeur. Ce dernier n'est pas en mesure de vérifier la véracité de toutes les informations qui lui sont transmises si bien qu'il pourrait être amené à supprimer du contenu licite. Ce faisant, le législateur a souhaité lutter contre les abus avec l'article 6-I-4 qui prévoit que « *le fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 EUR d'amende* ».

Il est alors possible de se demander si l'hébergeur a une obligation de surveiller le contenu proposé afin de vérifier qu'il ne soit pas illégal. L'article 6-I-7 de la loi LCEN y répond de manière non équivoque : « l*es personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites ».*

Toutefois, « compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de

leur orientation ou identité sexuelle ou de leur handicap ainsi que de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième, septième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 225-4-1, 225-5, 225-6, 227-23 et 227-24 et 421-2-5 du code pénal. A ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites ».

Ainsi, le législateur oblige les hébergeurs à mettre en place des dispositifs de signalements de contenus illicites comme sur *Facebook* par exemple. La charge de la preuve pèse sur la personne qui se prétend être la victime du contenu illicite.

Il est désormais possible d'imaginer une affaire relative aux tweets antisémites en 2018. *Twitter* serait l'hébergeur des tweets qui constituent le contenu illicite en ce qu'ils portent atteinte à la loi du 29 juillet 1881. La loi LCEN n'impose aucune surveillance a priori du contenu si bien que *Twitter* ne serait pas responsable de ces tweets. Cependant, *Twitter* pourrait engager ses responsabilités civile et pénale si la société n'enlevait « *promptement* » le tweet « *illicite* » alors qu'elle en aurait eu connaissance. La charge de la preuve pèserait sur la personne qui se prétend victime c'est-à-dire les associations. Cette dernière devrait alors prouver que *Twitter* avait connaissance du tweet illicite. En effet, en tant qu'hébergeur, Twitter est tenu de collaborer avec les autorités judiciaires, ce qui peut porter atteinte à l'anonymat (ß).

β) La collaboration avec les autorités judiciaires synonyme d'atteinte à l'anonymat

Ce statut protecteur a toutefois une contrepartie[251]. Celle qui contraint les hébergeurs à porter atteinte à l'anonymat en collaborant avec les autorités judiciaires.

[251] HUET J., DREYER E., *Droit de la communication numérique*, LGDJ, 2011, page 132.

L'article 6-II de la loi LCEN dispose en effet que « *les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires. Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III* ».

Le législateur organise donc une obligation qui consiste à conserver les données « *de nature à permettre l'identification de quiconque* ». Sont alors visées toutes les données de connexion. En effet, l'article 1er du décret n°2011-219 du 25 février 2011[252] précise les données qui doivent être préservées pour les fournisseurs d'accès internet ainsi que pour les hébergeurs. Les premiers doivent détenir et conserver, les données suivantes[253] : « *a) L'identifiant de la connexion ; b) L'identifiant attribué par ces personnes à l'abonné ; c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ; d) Les dates et heure de début et de fin de la connexion ; e) Les caractéristiques de la ligne de l'abonné* » ; concernant les hébergeurs, ces données sont : « *a) L'identifiant de la connexion à l'origine de la communication ; b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ; c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ; d) La nature de l'opération ; e) Les date et heure de l'opération ; f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a four*ni ». Enfin, ces données doivent être encadrées et couvertes par le secret professionnel garanti par la loi en ce qu'elles ont un caractère personnel. En effet, « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres*[254] ».

Grâce à l'article 6-III-2 alinéa 2 de la loi LCEN d'autres garanties existent concernant l'anonymat. Cet article dispose que « *les personnes mentionnées au 2 du I*[255] *sont assujetties*

[252] Ce décret est relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.
[253] https://www.legifrance.gouv.fr/eli/decret/2011/2/25/JUSD0805748D/jo/texte/fr.
[254] Article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[255] Les éditeurs de contenu.

au secret professionnel dans les conditions prévues aux articles 226-13[256] *et 226-14 du code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée* ». Il faut tempérer cette protection puisque le même article précise que « *le secret professionnel n'est pas opposable à l'autorité judiciaire* ».

Néanmoins, cette précision est opportune d'un point de vue juridique puisque l'article 66 de la Constitution de 1958 énonce que : « *l'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi* ». De plus, la création d'un droit à l'anonymat, aussi paresseuse soit-elle, nécessite obligatoirement l'existence de limites et de conditions. Pour les réfractaires, le Darknet est la solution. Outre l'engagement de la responsabilité des hébergeurs, celle des éditeurs de contenu est possible même si différencier les premiers des seconds n'est pas chose simple (b).

b) La responsabilité de l'éditeur de contenu

Il n'est pas toujours aisé de maîtriser ce qui différencie un éditeur d'un hébergeur de contenu. Matériellement, le premier produit un contenu tandis que le second permet l'accès à ce contenu. Pour la loi LCEN ces deux catégories font l'objet de régimes différents mais pour la jurisprudence une personne peut être à la fois éditrice et hébergeuse. En effet, Tribunal de grande instance a estimé le 9 mai 2009[257] que le Groupe *eBay*[258], était hébergeur pour une partie de son activité concernant les annonces de ses utilisateurs, et éditeur pour l'autre partie relative à la promotion et la régie publicitaire.

En l'espèce, des sociétés estiment que les plateformes *eBay* constituent un réseau de distribution facilitant la contrefaçon de produits cosmétiques et de parfums. Elles soutiennent que la société eBay n'a pas pris les mesures nécessaires afin d'endiguer les ventes sur ses plateformes de produits contrefaits en se réfugiant derrière sa qualité de simple hébergeur. Ainsi, le Groupe

[256] La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.
[257] Tribunal de grande instance de Paris 3ème chambre, 13 mai 2009. Disponible à cette adresse : https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-3eme-chambre-3eme-section-jugement-du-13-mai-2009-2/, [consulté le 24 juin 2015].
[258] Ebay est un site web américain de ventes aux enchères.

l'Oréal a décidé de la mettre en demeure par lettre datant du 22 mai 2007. Toutefois, les négociations ont échoué et c'est la raison pour laquelle le Groupe l'Oréal et huit autres sociétés[259] ont assigné le Groupe *eBay* en « *contrefaçon de marque, violation de leurs réseaux de distribution et responsabilité civile pour faute et négligence* ».

Le tribunal de grande instance de Paris estime qu'il « *convient en conséquence de rechercher le statut de l'activité faisant grief, un intermédiaire technique dans la prestation de services qu'il offre, pouvant avoir différentes activités dont les unes bénéficient du régime de responsabilité "aménagé" et dont les autres relèvent de la responsabilité de droit commun, étant précisé que le régime "aménagé" étant un régime d'exception au droit commun, son champ d'application doit être apprécié strictement* ».

Un exemple mérite d'être introduit. Un internaute, appelé X, loue un serveur à OVH une société offrant des services de cloud computing. Il décide d'y mettre en place un blog qui est une sorte de journal personnel sur Internet. Un autre internaute, nommé Y, poste un commentaire sur le blog. Quels sont les statuts des trois protagonistes du point de vue de la loi LCEN ? La difficulté réside dans le fait que les statuts sont interchangeables, et ce d'une part afin de limiter la responsabilité des intervenants, et d'autre part, afin de permettre une action via une requête auprès de l'hébergeur si un contenu litigieux a été publié. Pour conclure, OVH est bien hébergeur du blog qui est un site web, mais X est éditeur du site web et hébergeur des commentaires postés par Y. Concrètement, l'éditeur est responsable du contenu qu'il a édité. Ce régime se rapproche fortement de celui de la responsabilité de droit commun. En outre, le responsable de la publication s'expose aux poursuites pour des infractions comme l'incitation à la haine, la diffamation, la diffusion de contenu pédophiles etc.

La loi LCEN définit les éditeurs comme les personnes « *dont l'activité est d'éditer un service de communication au public en ligne* ». En effet, l'article 6-III-2 alinéa 1 de la loi dispose que « *les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I*[260]*, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1* ». C'est

[259] Ces huit sociétés sont toutes des filiales de l'Oréal.
[260] Les hébergeurs.

donc une réelle progression en matière de liberté d'expression mais aussi de protection de la vie privée. Pourtant, en raison de ces limites, certains se demandent s'il existe un réel droit à l'anonymat de l'expression et si les exceptions limitant ce droit ne seraient pas en fait le principe.

Il est possible de citer l'article 1 alinéa de la loi relative à la liberté de communication : « *l'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la protection de l'enfance et de l'adolescence, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle* ». Cette loi dite Léotard du 30 septembre 1986 limite clairement l'anonymat des éditeurs non professionnels de contenu.

L'idée de marchés anonymes et de systèmes de réputation remonte aux cypherpunks. Dans un monde comme le Darknet basé sur l'anonymat, il est plus difficile d'accorder sa confiance. Un utilisateur peut par exemple changer de pseudonyme après une opération afin d'obtenir une nouvelle identité virtuelle. Ainsi, les cypherpunks ont estimé que les utilisateurs se devaient d'avoir des pseudonymes longues durées. Dans son Manifeste crypto-anarchiste, Tim May, explique que « *la réputation est le point essentiel*[261]».

Le Darknet a donc contribué à cette quête d'anonymat, de confidentialité et surtout de liberté. Les révélations de Snowden ont montré que la NSA tentait de négocier avec les éditeurs de logiciels pour y mettre des portes dérobés afin d'y introduire des fonctions cachées portant atteintes aux libertés individuelles des utilisateurs. Dès lors, une catégorie de logiciel est devenue tendance : les logiciels *open source*[262]. Ces derniers mettent à disposition des utilisateurs leur code source si bien que chacun peut y accéder afin de le rendre plus

[261] « The reputation will be of central importance ».
[262] Il est possible de citer Firefox un navigateur Web, Libre Office un logiciel de traitement de texte, VLC un lecteur multimédia… Ces logiciels sont libres et gratuits.

opérationnel. Outre cette possibilité, ces logiciels garantissent l'absence de porte dérobée[263] et autres fonctions de surveillance. Néanmoins, ils ne sont pas sécurisés et ne permettent pas de naviguer de manière anonyme contrairement aux darknets qui sont garants d'un anonymat renforcé.

Mais, selon Andrew Lewman les réseaux Darknet ne sont pas infaillibles : « *je pense que si votre seul adversaire est la NSA[264] ou le GCHQ[265], alors vous avez certainement déjà perdu la bataille, parce que ce sont des agences disposant de plusieurs millions de dollars, de moyens fantastiques, face à un seul outil… De même que vous ne pouvez pas construire une maison avec seulement un marteau, il vous faute une boîte à outils complète et des savoir-faire pour battre de tels adversaires* ». C'est dans ce contexte que le Darknet est devenu un moyen de défense (Section 2).

[263] « *Dans un logiciel, une porte dérobée (de l'anglais backdoor, littéralement porte de derrière) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel* ». Définition disponible à cette adresse : https://fr.wikipedia.org/wiki/Porte_dérobée.
[264] *The National Security Agency* est le service de renseignements électroniques des Etats-Unis
[265] *The Government Communications Headquarters* est le service de renseignements électroniques du Royaume-Uni.

SECTION 2
Le Darknet, un moyen de défense

Le Darknet est un outil technologique qui peut être utilisé à bon comme à mauvais escient. Les activités sont certes cachées mais elles ne sont pas nécessairement illégales. La technologie a toujours eu un double visage selon l'usage qui en est fait.

Par exemple, Roey Tzezana, futuriste et auteur du « *Guide to the future* », explique comment il a fabriqué une arme à feu en utilisant une imprimante 3D : « *autrefois, la production se faisait dans des usines valant des millions d'euros mais aujourd'hui n'importe qui peut avoir ce genre de machine à la maison. Les gens possèdent donc le matériel nécessaire à la fabrication d'un revolver sans numéro de série et non soumis à la vérification des antécédents : une sorte d'arme fantôme. Un phénomène nouveau est en place, il s'agit d'une tendance de déqualification qui consiste en une diminution des compétences nécessaires pour atteindre un certain objectif* ».

Toutefois, Roey Tzezana montre une autre facette de l'évolution technologique. Il estime que d'ici dix ou vingt ans, un processus identique à celui des armes à feu va commencer à se produire et apporter des améliorations. Tout le monde sur terre prendra part à cet échange d'informations et à cet échange de nouvelles idées. Le Darknet peut être ce lieu où toutes les vieilles idées se mélangeront les unes aux autres. Néanmoins, cette révolution ne peut pas avoir lieu en utilisant les voies traditionnelles de l'information et c'est toute l'importance du Darknet qui permet de canaliser l'information et d'engendrer une Révolution que les pouvoirs en place souhaiteraient éviter.

Ce nouvel environnement virtuel présente des traits singuliers avec un fonctionnement qui semble insaisissable. Le Darknet est imprévisible et repose sur de nouveaux paradigmes. L'architecture et les fonctionnalités de ce réseau alternatif dépasse tout ce qui a été imaginé initialement. Les projets mis en place sur le Darknet sont destinés à protéger la vie privée des personnes qui ont accès à l'information et qui publient sur les plateformes permettant la communication gratuite. Dès lors, le développement de ces réseaux est fondé sur une volonté d'anonymisation assurant une protection des utilisateurs de nœuds sur le Darknet. Par ailleurs, les créateurs de darknets s'assurent que les gouvernements, occidentaux ou non, contrôlent le moins possible le partage d'information opéré par sa population. En effet, le Darknet a permis

la diffusion d'informations censurées dans des pays comme l'Iran ou la Chine. Faut-il pour autant avoir une vision manichéenne avec la censure d'un côté et la liberté d'expression de l'autre ? Cette question est pertinente puisque certaines idées peuvent être dommageables pour la société et nécessiter une restriction des communications par le biais de la loi.

A titre d'exemple, en France il existe une infraction permettant de lutter contre la propagation d'informations racistes, une sorte de censure légitime. Mais pour le créateur de Freenet, Ian Clarke, il n'y a pas de bonne censure : « *soit vous avez de la censure, soit vous n'en avez pas. Il n'y a pas de juste milieu* ». La liberté d'expression semble être une priorité pour les créateurs de réseaux darknets qui craignent les gouvernements et les colosses comme *Google* et *Yahoo*. Mais l'anonymat de ces réseaux est-il nécessaire ? Il permettrait de ne pas sanctionner après coup ceux qui exercent leur liberté d'expression et de garantir un droit à la vie privée. Il s'agit alors de créer un pseudonyme sécurisé correspondant à une « *cyber identité* » qui devra gagner la confiance des autres avec le temps. C'est l'idée qui a été mise en place par les *cyberpunks*. Le Darknet est ainsi devenu une arme contre le contrôle des gouvernements (§1) et un moyen pour s'exprimer librement (§2).

§1) Une arme contre le contrôle des gouvernements

En 1992, en rédigeant le « *Manifeste Crypto-Anarchiste*[266] » dans lequel il avance que « *les méthodes cryptologiques altèreront fondamentalement la nature de l'interférence du gouvernement et des grandes sociétés dans les transactions économiques* », Tim May devient une figure majeure du mouvement crypto-anarchiste. Il est précédé par Loyd Blankenship qui rédige « *La conscience d'un Hacker*[267] » le 8 janvier 1986 et suivi par John P. Barlow qui publie sa « *Déclaration d'indépendance du Cyberespace*[268] » en février 1996, par Christian As. Kirtchev qui publie « *Un Manifeste Cyberpunk* » le 14 février 1997 et par Meredith L. Patterson qui publie « *A biopunk Manifesto* » le 20 janvier 2010. Tous ces auteurs sont des crypto-anarchistes.

[266] MAY T., *The Crypto Anarchist Manifesto*, 1992.
Disponible à cette adresse : https://www.activism.net/cypherpunk/crypto-anarchy.html.
[267] BLANKENSHIP L., *La conscience d'un Hacker*, 8 janvier 1986. Disponible à cette adresse : http://cyberpunk.asia/pages_html.php?html=manifeste.
[268] P. BARLOW J, *Déclaration d'indépendance du Cyberespace,* Traduction édition-Hache 1996. Disponible à cette adresse : http://editions-hache.com/essais/barlow/barlow2.html.

Un crypto-anarchiste ou cypherpunk[269] est un individu intéressé par la cryptologie et ayant pour objectif la protection de la vie privée des internautes. Le terme cypherpunk est composé à partir des mots cypher[270] et punk et le terme crypto-anarchiste des mots crypto et anarchiste. L'anarchisme est défini par le dictionnaire Larousse comme la « *conception politique et sociale qui se fonde sur le rejet de toute tutelle gouvernementale, administrative, religieuse et qui privilégie la liberté et l'initiative individuelles*[271] » et le mouvement punk comme « *un mouvement culturel apparu en Grande-Bretagne vers 1975 et dont les adeptes affichent divers signes extérieurs de provocation afin de caricaturer la médiocrité de la société*[272] ». Pour faire simple, ces individus remettent en cause le rôle prééminent des gouvernements en utilisant le chiffrement comme moyen de défense.

Les cypherpunks maitrisent très bien le cyberespace qui va leur permettre de s'organiser puisque sur ce nouveau territoire numérique les lois n'ont pas toujours vocation à s'appliquer. Pour ce faire les crypto-anarchistes n'utilisent pas les réseaux centralisés mais sont adaptes des communications *« peer to peer* ». Le modèle économique ne leur plaisait pas puisque l'argent circulait de manière très centralisée en passant pas les banques mais l'apparition des cryptomonnaies a changé la donne. Imaginez si tous les biens de la planète étaient disponibles sur le marché noir, les Etats perdraient la majeure partie de leur capacité à réguler, à favoriser certaines entreprises jusqu'à perdre leur pouvoir. C'était le souhait des cryptos anarchistes, mais la réalité est bien différente.

Créé par Décret n°2011-537 du 17 mai 2011 - art. 2, l'article R211-22 du code rural et de la pêche maritime dispose qu'en « *cas de circonstances graves touchant à l'ordre public, la fédération colombophile française communique la liste nominative des colombophiles au ministre de l'intérieur et au ministre de la défense* ». Cet article peut paraître anecdotique mais il révèle que même la communication via pigeons voyageurs est contrôlée par l'Etat français qui souhaite contrôler tous les réseaux d'échange possibles.

[269] En réalité il y a une petite différence. Le cypherpunk crée le programme tandis que crypto-anarchiste se contente de l'utiliser.
[270] Chiffrement.
[271] Disponible à cette adresse : https://www.larousse.fr/dictionnaires/francais/anarchisme/3276.
[272] Disponible à cette adresse : https://www.larousse.fr/dictionnaires/francais/punk/65101?q=punk#64371.

Les gouvernements ont la mainmise sur les échanges entre tous les citoyens. Internet est l'exemple parfait de ce quadrillage mis en place par les institutions. La neutralité d'Internet semble fortement compromise (A), et ce territoire numérique est devenu un champ de bataille entre gouvernements et groupes d'internautes (B). Le Darknet semble être la solution permettant de faire face à ces deux problèmes.

A) L'absence de neutralité d'Internet

Il existe un conflit, que la plupart des internautes refusent de voir, qui se déroule actuellement pour obtenir le contrôle d'Internet et dont les acteurs sont les gouvernements, les lobbys, la *Silicon Valley*, les banques et les hackeurs activistes appelé *hacktivistes*. Cela démontre clairement l'absence de neutralité d'Internet.

Cette dernière est définie par Laurent Gayard[273] comme le « *principe suivant lequel aucun opérateur privé, fournisseur d'accès mais aussi de services, ne peut privilégier ses propres utilisateurs et ses propres produits par des politiques tarifaires ou des mesures techniques visant à privilégier dégrader ou bloquer selon les cas certains flux d'informations au détriment ou au profit d'autres. La neutralité réseau est donc un principe d'égalité de traitement de tous les flux de données, excluant toute discrimination à l'égard de la source, de la destination ou du contenu pour des motifs économiques ou politiques et à des fins de restriction, exploitation ou surveillance des données échangées* ».

Il précise en outre qu'Internet « qui se présentait comme univers horizontal ouvert à tous, est en train de se restructurer en silo, de façon verticale, autour de quelques grands opérateurs. Et tous sont américaines. Zéro européen ».

Cette mainmise des Etats-Unis amène à se demander si Internet est réellement neutre. La nature ambivalente de l'ICANN pose problème quant à cette indépendance puisqu'autrefois, malgré les nombreuses critiques, l'affection des noms de domaine et des adresses IP se faisait en application d'un contrat conclu avec le gouvernement américain. Les statuts de l'ICANN étaient régis par le droit californien si bien que l'autorité était placée sous le contrôle du

[273] GAYARD L., *Géopolitique du Darknet : Nouvelles Frontières et Nouveaux Usages du Numérique*, Iste édition, 2017, page 35.

procureur général californien et du département du Commerce des Etats-Unis. Tout changement de nom de domaine nécessitait l'accord de ce dernier avant d'être validé. L'influence de la justice et du gouvernement américains était manifeste avant un changement de situation quant aux statuts de l'ICANN. En effet, les révélations de Snowden et l'expiration du contrat entre l'ICANN et les Etats-Unis[274] ont contribué au fléchissement du contrôle des Etats-Unis sur l'affectation des noms de domaine. Bien avant ces événements, en 1999, le Comité consultatif gouvernemental[275] avait été instauré par les règlements de l'ICANN afin de lui fournir des conseils sur les perspectives de politique publique dans le cadre des noms de domaine (DNS).

Composé de 137 membres et de 30 observateurs issus de gouvernements nationaux ou d'organisations internationales, le GAC n'a pas de pouvoir décisionnel, il s'agit d'un comité consultatif : « *le GAC est un comité consultatif de l'IMS, créé en vertu des statuts de l'ICANN. Il conseille l'ICANN sur des dossiers de politique publique en rapport avec les responsabilités de l'ICANN à l'égard du système des noms de domaine (DNS). Le GAC n'est pas un organe décisionnel. Il émet des avis sur des questions relevant de la mission de l'ICANN*[276] ». Néanmoins, le GAC est contesté en raison de ses modalités qui prévoient désormais qu'il devra se prononcer à l'unanimité pour la validation de ses avis et communiqués. Certains États comme la France estiment qu'il y a de fortes chances que ces modalités favorisent les GAFA : « *On est dans la privatisation de l'ICANN, pas dans son internationalisation. Les Etats-Unis reprennent d'une main ce qu'ils donnent de l'autre*[277] ». Cette affirmation semble non pertinente puisqu'en théorie le GAC n'a qu'un rôle consultatif. Mais, en réalité le rôle de la GAC est en mesure d'empêcher les imprudences des Etats dans la mesure où chaque avis du GAC contraint les Etats à justifier un éventuel refus et à fournir une contre proposition avant de pouvoir l'ignorer.

Les relations internationales et la politique des Etats ont directement été influencées par cette réforme de l'ICANN mais aussi par le développement des darknets qui ne subissent pas le contrôle de tous ces protagonistes en matière de géopolitique numérique. Dans ce contexte, sont

[274] Le contrat entre les Etats-Unis et l'ICANN est arrivé à échéance le 1er octobre 2016.
[275] Gouvernmental Advisory Committee (GAC).
[276] https://gac.icann.org/about?language_id=3.
[277] CHAFFIN Z., *Paris dénonce une privatisation de la gouvernance d'Internet*, 24 mars 2016. Disponible à cette adresse : https://www.lemonde.fr/economie/article/2016/03/24/icann-paris-denonce-une-privatisation-de-la-gouvernance-d-internet_4889567_3234.html, [consulté le 25 mars 2016].

opposés les partisans de l'indépendance d'Internet et de la mondialisation de l'ICANN qui doit être gouvernementale, et les défenseurs de la politique américaine selon laquelle le secteur privé devrait avoir autant d'autorité que les gouvernements. Ce sont ces derniers qui semblent avoir gagné la bataille puisque malgré l'absence de lien juridique, l'ICANN semble toujours sous l'influence des Etats-Unis grâce aux GAFA qui influencent fortement l'attribution des noms de domaine. Or, les conséquences ne sont pas négligeables puisque depuis 1998, l'ICAAN dispose du protocole *WHOIS*[278] permettant d'accéder aux bases de données d'un site lors de l'enregistrement de son nom de domaine. De plus, l'ICANN a une fonction économique puisqu'une société de droit privé gère pour elle le paiement et l'organisation de 80% des noms de domaine existant.

Ainsi, la neutralité d'Internet passe nécessairement par l'émancipation des organes d'affection des noms de domaine mais cette indépendance semble utopique. En effet, nombreux sont les États à manifester leur désaccord concernant l'emprise des GAFA sur les nouveaux accords relatifs aux noms de domaine. C'est dans ce contexte, que le déploiement subversif du Darknet a fortement impacté les différentes autorités de régulation d'Internet puisque les darknets disposent de leurs propres noms de domaine et peuvent se priver de l'ICANN. Pour faire face à cette désorganisation de l'attribution des noms de domaine, l'organe de régulation a permis un élargissement des noms de domaines en autorisant l'adressage de nouvelles villes[279] et entreprises[280]. La révolution numérique est en marche mais son orientation est incertaine puisqu'il est difficile d'anticiper les conséquences des développements technologiques comme ont su le faire Peter Biddle, Paul England, Marcus Peinado, Bryan Willman[281]. C'est dans un tel contexte que les *cryptowars* se sont déclenchées (B).

B) Les *cryptowars*

En pleine *cryptowar,* après les attentats du 11 septembre, le président G.W Bush autorise les

[278] *Who is*.
[279] .paris par exemple.
[280] Nouvelles extensions Internet : un nouveau Big Bang pour les noms de domaine, dossier thématique n°11. Disponible à cette adresse : https://www.afnic.fr/fr/ressources/publications/dossiers-thematiques/nouvelles-extensions-internet-un-nouveau-big-bang-pour-les-noms-de-domaine.html, [consulté le 12 janvier 2017].
[281] BIDDLE P., ENGLAND P., PEINADO M., and WILLMAN B., The darknet and the future of content distribution. In Proceedings of the 2002 ACM Workshop on Digital Rights Management, Washington DC, USA, 2002.

États-Unis à espionner les communications téléphoniques sans l'autorisation d'un juge ; le Congrès américain adopte le *Patriot Act*[282] et la NSA met en place un programme de surveillance massive.

Snowden révèlera que la NSA ne s'est pas contentée de surveiller les terroristes en espionnant des millions d'américains innocents. Il a révélé l'utilisation de programmes qui n'ont jamais protégé les citoyens mais qui les privaient de libertés fondamentales auxquelles ils n'auraient jamais renoncé. Ils ont recueilli un tas de données sous couvert de la sécurité et sans égard pour les règles de procédure. Les documents du gouvernement américain et de la NSA montrent qu'ils enseignent à leurs agents comment repérer les failles, non pas des terroristes, mais de prédicateurs musulmans. Dès lors, le gouvernement a la possibilité de ruiner la réputation de toute personne dont il n'approuve pas le message.

Snowden, un ancien administrateur système sous-traitant de la CIA[283] et de la NSA, révèle des détails sur des programmes de surveillance de masse aux Etats-Unis et en Grande-Bretagne. Le 6 juin 2013, c'est le quotidien britannique *The Guardian* qui publie ces révélations. Entre 15 000 et 20 000 documents, transmis aux journalistes Glenn Greenwald et Laura Poitras, ont mis la lumière sur un réseau de programmes d'espionnage utilisé par la NSA pour intercepter les conversations numériques et téléphoniques de centaines de millions d'utilisateurs à travers le monde et notamment en Chine, en Europe et en Iran. Aux États-Unis, la NSA a collecté et analysé les données de plus de 300 millions de citoyens grâce aux outils de surveillance *XKeyscore*[284] et *PRISM*[285]. La synthèse de ces documents a montré que sous prétexte d'une lutte contre le terrorisme, les États-Unis ont évalué les politiques et stabilités économique d'autres États. D'après Snowden, en 2012 la NSA aurait collecté en une seule journée les adresses mails de 444 743 comptes Yahoo, 105 068 comptes Hotmail, 82 857 comptes Facebook et 22 881 comptes Gmail. Une fois récoltées les données lui permettaient d'établir des cartes détaillées de la vie sociale d'un utilisateur en prenant en compte ses relations

[282] Il s'agit d'une loi antiterroriste américaine votée par le Congrès et signée par George W. Bush le 26 octobre 2001 : « *Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme* ».
[283] *Central Intelligence Agency.*
[284] Grâce à ses 700 serveurs situés dans plusieurs pays à travers le monde, *XKeyscore* permet une collecte systématique des données de tout internaute.
[285] *PRISM*, aussi appelé US-984XN1, est un programme américain de surveillance électronique permettant la collecte de données sur Internet.

personnelles, religieuses, politiques et professionnelles. La liste des atteintes à la vie privée est longue. En effet, la NSA a également dérobé des clés de chiffrement afin d'écouter des conversations et lire des SMS en toute discrétion, elle a piraté des smartphones et utilisé des données de géolocalisation afin d'obtenir la position d'un individu.

Ces révélations ont eu de nombreuses conséquences puisque Snowden a été poursuivi pour vol, espionnage et utilisation illégale de biens gouvernementaux. Il s'est exilé à Hong Kong en juin 2013 puis a demandé l'asile politique en Russie où il a obtenu un droit de résidence jusqu'en 2020. Mais, ces révélations ont surtout eu un impact sur l'utilisation des darknets par les internautes du monde entier. A titre d'exemple, peu de temps après le scandale, le nombre d'utilisateurs quotidien du darknet Tor est passé de 500 000 à 1,5 millions. La NSA avait anticipé le problème puisqu'en 2007 lors d'une rencontre avec Roger Dingledine[286], les dirigeants de la NSA ont admis vouloir désanonymiser les échanges des utilisateurs de Tor[287]. En 2013, la NSA consacre plus de 34 millions de dollars afin de décrypter des services tels que des darknets. La révélation de l'identité d'un utilisateur du darknet est possible lorsque des moyens importants sont utilisés. Néanmoins, le décryptage massif des darknets n'est pas chose simple et les réseaux comme Tor ont vocation à devenir de plus en plus fiable et les cryptographes ne sont pas prêts de perdre cette nouvelle *cryptowar*.

C'est dans ce contexte qu'un groupe d'individus a agi en utilisant les darknets et la cryptologie. Les cryptos anarchistes constituent la branche d'un petit groupe de technophiles qui s'est constituée au tout début d'internet : les Cypherpunks. Le terme « cypher » signifie chiffrement ; les Cypherpunks sont des activistes de la cryptographie croyant au respect de la vie privée pour tous. Ce sont ces militants qui ont été à l'origine de l'un des premiers darknets qu'ils avaient appelé le « *blacknet* ». Ils ne sont pas prêts à accepter le fait qu'ils vivent dans un Etat informatique policier et veulent combattre cette dystopie de la surveillance.

Le Darknet est un outil et un moyen permettant de protéger leurs libertés contre les tendances autoritaires et les institutions politiques et sociales. Fondamentalement, l'une des raisons pour

[286] L'un des fondateurs de Tor et de Tor Project l'organisation qui développe Tor.
[287] BALL. J., SCHNEIER B., GREENWALD G., *NSA and GCHQ target Tor network that protects anonymity of web users*, The Guardian, 2013. Disponible à cette adresse : https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption, [consulté le 15 novembre 2015].

laquelle ils souhaitent le respect de leur vie privée est la volonté d'avoir une action humaine libre. Le fait d'être surveillé et de devoir contrôler ses propres actes, ralentit l'évolution de l'Homme. Cette forme de totalitarisme est beaucoup plus subtile ; en apparence tout le monde est libre, le consommateur peut regarder sa série préférée sur *Netflix*, mais, dès qu'un individu souhaite réellement changer les choses, il se fait attaquer. L'origine des *cryptowars* (1) et les *cypherpunks* illustrent parfaitement cette opposition entre les iconoclastes d'Internet et les gouvernements (2).

1. Les origines des cryptowars

Une guerre moderne a fait son apparition grâce aux améliorations techniques ayant fait du renseignement électronique un domaine prédominant : il s'agit de la « *crypto war*[288] », définie par Wikipédia[289] comme « *un terme informel pour désigner les efforts du gouvernement des États-Unis de limiter l'accès du public et des nations étrangères à des méthodes de cryptographie assez fortes pour résister à la cryptanalyse de ses différentes agences de renseignement, en particulier de la NSA* ».

Dès les années 1970, en pleine Guerre Froide, les États-Unis et leurs alliés ont entamé une lutte afin que les nombreuses technologies occidentales ne tombent pas entre les mains d'autres puissances, particulièrement de l'URSS. A partir des années 1990, à l'ère de l'ordinateur personnel et de la démocratisation d'Internet et des messageries électroniques, ces confrontations vont s'amplifier jusqu'à impliquer la société civile. La commercialisation d'Internet a permis aux États et aux instances de renseignement de profiter de ce territoire numérique pour effectuer une collecte d'informations.

En 1985, David Lee Chaum, l'inventeur de plusieurs protocoles cryptographiques, et précurseur en matière de monnaie électronique, prétend que l'outil informatique et numérique permet un fichage et une traçabilité performante des utilisateurs, et ce, afin de les surveiller et d'influencer leur mode de consommation[290]. Il propose d'utiliser un système de transactions anonyme fondé sur l'utilisation d'une signature aveugle permettant d'authentifier un message nonobstant son

[288] Guerre de la cryptographie.
[289] Définition disponible à cette adresse : https ://fr.wikipedia.org/wiki/Crypto_Wars.
[290] CHAUM D.L., *Security without identification : transaction systems to make big brother obsolete*, *Communications of the ACM*, volume 28, octobre 1985, page 1030–1044.

contenu[291] et fonde en 1990 la société Digicash Inc., la première cryptomonnaie[292].

La *cryptowar* s'intensifie et la mission des agences de renseignement en matière de surveillance électronique est tourmentée par l'apparition de la cryptologie civile de Phil Zimmerman[293]. Cette dernière utilise un algorithme de cryptage et des clés de cryptage symétrique afin d'encrypter et de décrypter toute sorte de fichiers et bases de données. Une clé publique est transmise tandis que la clé privée est conservée par l'utilisateur. Le message et la clé publique sont envoyés par l'envoyeur à l'interlocuteur qui télécharge le message et utilise sa clé privée pour le décrypter. Une empreinte digitale est en outre utilisée pour permettre l'authentification de l'expéditeur et éviter les usurpations d'adresse. Zimmerman a répandu le code source de son logiciel afin qu'il soit utilisé partout à travers le monde. Le Gouvernement américain, qui ne voit pas d'un bon œil l'expansion d'un tel logiciel, accuse Zimmerman[294] d'avoir violé l'*Arms control Act* de 1976 prohibant l'exportation sans autorisation du gouvernement américain des technologies qui peuvent être exploités à des fins militaires. À cette époque, la cryptologie est donc une nouvelle technologie pouvait être assimilée à une arme. L'acuité des discussions contemporaines en matière de chiffrement prouve que la *cryptowar* n'est toujours pas finie. L'impuissance du gouvernement face à la diffusion du programme de Zimmerman et de la cryptomonnaie de Chaum a permis à la cryptomonnaie et au Darknet d'émerger.

Le 25 mai 2005, la *Foundation for Information Policy Research*, spécialiste des nouvelles technologies de l'information, publie un article avec comme titre : « *les guerres de cryptographie sont finies, et nous avons gagné*[295] » . En réalité, à ce moment, seule la première *cryptowar* a été gagnée par les utilisateurs de la cryptologie et malgré les avancées juridiques et techniques, les enjeux du chiffrement étaient restés l'apanage des plus aguerris. En effet, les révélations d'Edward Snowden vont prouver que pendant des années les agences de renseignement ont été capables de contourner les protocoles de cryptologie utilisées par le grand

[291] CHAUM D.L., *Untraceable electronique mail, return adresses and digital pseudonyms*, *Communications of the ACM*, volume 32, 1981, page 1030.
[292] Une cryptomonnaie ou monnaie cryptographique est une monnaie numérique qui s'utiliser sur un réseau décentralisé *peer-to-peer*.
[293] Phil Zimmermann a créé *Pretty Good Privacy*, un logiciel de chiffrement de courrier électronique.
[294] Les poursuites ont ensuite été abandonnées et Zimmerman.
[295] Texte original : « *The crypto wars are finally over - and we've won !* ». Disponible à cette adresse : https://www.fipr.org/press/050525crypto.html, [consulté le 4 avril 2016].

public. À la suite de ces révélations, le déploiement de nombreuses techniques va être démocratisé et garantir une meilleure protection du droit à la vie privée et de la liberté de communication qui étaient menacés par les gouvernants qui opéraient une surveillance massive d'Internet. Grâce à Snowden, la deuxième *cryptowar* a été remportée par les cypherpunks. Deuxième et non pas seconde puisque la troisième *cryptowar* est actuellement en cours (2).

2. Les cypherpunks

Depuis 2003, Tim May est retraité de la société Intel où il était ingénieur. Il a contribué au mouvement crypto-anarchiste en publiant le Manifeste Crypto-Anarchiste en 1992 et le Cyphernomicon[296] en 1994. Il écrit beaucoup sur la confidentialité et la cryptographie et détaille un projet politique en essor dans les années 1990 à une période où les réseaux *peer to peer* sont en train de se développer.

Avec ses essais il souhaitait attirer l'attention des anarchistes sur les ressources technologiques informatiques : « *l'informatique est sur le point de fournir la capacité aux individus et aux groupes de communiquer et interagir entre eux d'une façon totalement anonyme. Deux personnes pourront échanger des messages, faire des affaires et négocier des contrats électroniques sans jamais connaître le Véritable Nom, ou l'identité légale, de l'autre. Les interactions à travers les réseaux seront intraçables, grâce au reroutage intensif de paquets encryptés et à l'utilisation de boîtiers hardwares inviolables implémentant des protocoles cryptographiques assurant une presque parfaite protection contre toute forme d'altération* » (…) *« Les technologies pour cette révolution, qui sera sûrement à la fois sociale et économique, ont existé en théorie pendant la dernière décennie. Les méthodes sont basées sur de l'encryption par clef publique, des systèmes de preuves à divulgation nulle de connaissance (ZKIP) et une variété de protocoles pour l'interaction, l'authentification et la vérification. Le centre d'attention est pour l'instant porté sur des conférences académiques en Europe et aux USA, conférences surveillées de près par la National Security Agency. Mais c'est uniquement récemment que les réseaux informatiques et les ordinateurs personnels ont atteint une vitesse suffisante pour rendre ces idées réalisables. Et la prochaine décennie va apporter suffisamment de vitesse supplémentaire pour rendre ces idées économiquement réalisables et surtout*

[296] C. MAY T., The Cyphernomicon, 1994.

instoppables » (…) « *L'Etat va bien entendu essayer de ralentir ou d'arrêter la propagation de ces technologies, en invoquant la sécurité nationale, leur utilisation par des dealers et des fraudeurs et la peur d'une désintégration sociale. La plupart de ces inquiétudes sont légitimes ; le crypto-anarchisme permettra la vente libre de secrets nationaux et de biens illicites ou volées. Un marché électronique anonyme pourrait même rendre possible de détestables foires aux assassinats et aux extorsions. Divers criminels et étrangers seront des utilisateurs actifs de CryptoNet. Mais cela n'interrompra pas la diffusion du crypto-anarchisme* » (…) « De la même manière que l'imprimerie a modifié et réduit le pouvoir des guildes moyenâgeuses et la structure du pouvoir social, les méthodes cryptographiques vont affecter fondamentalement la nature de l'influence des gouvernements et des corporations sur les transactions économiques[297] ».

Vingt-six ans plus tard, toutes les prédictions de Tim May se sont notamment réalisées grâce à l'apparition des darknets. Néanmoins, la réalité actuelle est opposée à l'utopie envisagée par Tim May qui voulait rassembler les utilisateurs dans un cadre libertaire. Au contraire, l'usage du chiffrement et des darknets a divisé Internet en créant différentes communautés n'adhérant pas toutes à l'idéologie de départ. En tout état de cause, le Darknet a des effets positifs en ce qui concerne la liberté d'expression (§2).

§2) Le Darknet, un moyen d'expression

En occident, l'image du Darknet est noire, diabolique et malveillante, alors qu'ailleurs dans le monde il est considéré comme un lieu où s'échange l'information anonymement et en toute sécurité. Il y a des endroits où le simple fait d'être connecté suffit pour que les individus soient arrêtés. Dès lors, les technologies deviennent une issue de secours pour ceux qui vivent sous un régime dictatorial. Mais pourquoi une telle innovation est-elle nécessaire au sein des régimes démocratiques.

Aujourd'hui, nous sommes à la croisée des chemins entre deux systèmes gouvernementaux en compétition. D'un côté, il y a un contrôle de la vie des citoyens, d'un autre, la domination des masses. Le gouvernement tente de sécuriser ses citoyens en arrêtant la menace que représente

[297] Disponible à cette adresse : https://www.activism.net/cypherpunk/crypto-anarchy.html, [consulté le 24 décembre 2015].

les loups solitaires, à savoir les criminels et notamment ceux qui voudraient renverser le gouvernement par la force ou non : les terroristes. Le peuple exige la justice sociale, il n'accepte pas les abus qui proviennent d'un camps ou de l'autre. Dans ce contexte, le Darknet donne une tribune aux lanceurs d'alerte (A) et à tous les internautes du monde souhaitant lutter contre la censure (B).

A) Les lanceurs d'alertes

Les individus ont très facilement peur de la nouveauté et de la différence, or les idées qui tournent autour du Darkweb sont nouvelles et les mots tels que anarchistes ou cryptographie peu communs. Les amalgames autour du Darknet sont tellement nombreux qu'il s'agit de se demander si le contenu qu'il héberge, qu'il soit licite ou non, est fiable. La peur de l'inconnu, de ce Darknet qui n'est pas facilement accessible, a créé une véritable méconnaissance des enjeux numériques.

Pourtant, le Darknet contient plusieurs points positifs. A titre d'exemple, les lanceurs d'alerte n'existeraient certainement pas sans le Darknet. En effet, parmi les sites cachés de Tor, il est possible de trouver les sites de lancement d'alerte d'un certain nombre de médias. Après l'affaire Snowden, il y a une prise de conscience de la capacité de surveillance très large des gouvernements occidentaux. C'est à ce moment que les darknets sont devenus des outils essentiels à la lutte contre les abus des Etats et des multinationales en empêchant notamment les intrusions dans la vie privée, à une époque où tout être humain a le droit de préserver ses secrets. Des individus comme Phil Zimmerman développent le chiffrement et l'anonymat parce qu'ils croient que leur travail favorisera la protection des libertés civiles contre les surveillances intrusives, particulièrement dans les pays aux régimes répressifs.

En France, les lanceurs d'alerte sont définis par le Conseil d'Etat[298] comme des personnes qui « *signalent, de bonne foi, librement et dans l'intérêt général, de l'intérieur d'une organisation ou de l'extérieur, des manquements graves à la loi ou des risques graves menaçant des intérêts publics ou prives, dont ils ne sont pas l'auteur* ».

[298] *Le droit d'alerte : signaler, traiter, protéger*, le 13 avril 2016. Disponible à cette adresse : http://www.conseil-etat.fr/Actualites/Communiques/Le-droit-d-alerte-signaler-traiter-proteger.

Dès lors, il faut bien les différencier des auteurs des faits qu'ils dénoncent ou signalent. Ils leurs sont extérieurs. Les lanceurs d'alerte ne sont pas auteurs ou complices de l'infraction car ils ne participent pas à l'élément matériel de l'infraction. L'article 6 de la loi dite Sapin 2 du 9 décembre 2016[299] a confirmé cette définition et la notion de désintéressement : « *un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance* » (1). Les exemples de Snowden et *Wikileaks* (2) illustrent bien le phénomène qui comportent énormément de risques.

1. Le régime juridique français des lanceurs d'alerte

La loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique[300] définit le lanceur de l'alerte. D'après cette définition, il faut la réunion de deux conditions. Premièrement, la personne physique doit agir « *de manière désintéressée et de bonne foi* ». Ainsi, une entreprise ne pourrait pas profiter de ce régime si elle divulguait les agissements illégaux d'un de ses concurrents. Secondement, le signalement doit porter sur « *un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance* ». Les faits envisagés sont très large mais la loi exclut logiquement « *les faits, informations ou documents couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son clien*t ».

Lorsque ces conditions sont remplies, l'alerte peut être lancée selon une procédure progressive

[299] Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.
[300] Https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B179D26055C267E372B58E8490BEC816.tplgfr29s_1?cidTexte=JORFTEXT000033558528&dateTexte=29990101.

prévue par l'article 8 de la loi dite Sapin 2[301]. Tout d'abord, le signalement de l'alerte doit être « *porté à la connaissance du supérieur hiérarchique, direct ou indirect, de l'employeur ou d'un référent désigné par celui-ci* ». En l'absence de réaction de l'individu destinataire de l'alerte, elle pourra être adressée « *à l'autorité judiciaire, à l'autorité administrative[302] ou aux ordres professionnels* ». Enfin, s'il n'y a pas de réaction dans un délai de trois mois, les révélations peuvent être rendues publiques. En somme, le lanceur d'alerte doit d'abord prévenir les autorités concernées. En cas d'inertie de ces autorités, il pourra exposer les faits sur la place publique.

Le respect de ces conditions permet au lanceur d'alerte de bénéficier d'une triple protection. D'une part, l'article 9 de la loi dite Sapin 2[303] prévoit une procédure garantissant « *une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées par celui-ci et des informations recueillies par l'ensemble des destinataires du signalement* ». S'il donne son accord, son identité ne sera connue que des autorités judiciaires.

D'autre part, le lanceur d'alerte bénéficie d'une protection contre une sanction disciplinaire en tant qu'agent public[304] ou salarié[305]. En cas d'exclusion, il peut être réintégré[306].

D'une dernière part, l'article 122-9 du Code pénal dispose que « *n'est pas pénalement responsable la personne qui porte atteinte à un secret protégé par la loi, dès lors que* cette

[301] Https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=32A872555F3257A400EA9E273E70A777.tpdila12v_2?idArticle=JORFARTI000033558657&cidTexte=JORFTEXT000033558528&dateTexte=29990101&categorieLien=id.
[302] Comme l'Agence française anticorruption ou l'autorité des marchés financiers.
[303]Disponible à cette adresse : https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=32A872555F3257A400EA9E273E70A777.tpdila12v_2?idArticle=JORFARTI000033558658&cidTexte=JORFTEXT000033558528&dateTexte=29990101&categorieLien=id.
[304]Disponible à cette adresse : https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=32A872555F3257A400EA9E273E70A777.tpdila12v_2?idArticle=LEGIARTI000033611288&cidTexte=LEGITEXT000006068812&dateTexte=20170505.
[305]Disponible à cette adresse : https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=32A872555F3257A400EA9E273E70A777.tpdila12v_2?idArticle=LEGIARTI000033611283&cidTexte=LEGITEXT000006072050&dateTexte=20170505.
[306]Disponible à cette adresse : https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=465E6A7D9FF73DB516B28D8FD45BAB12.tpdila12v_2?idArticle=LEGIARTI000033562402&cidTexte=LEGITEXT000006070933&dateTexte=20170505.

divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte prévus à *l'article 6 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique* ».

Par conséquent, le législateur est venu encadrer l'action des lanceurs d'alerte qui ont besoin d'une protection lorsque leur démarche est légitime. L'idée est de préserver les intérêts des entreprises et des lanceurs d'alerte grâce à une gradation. Entrée en vigueur le 1er janvier 2018, cette loi constitue une réelle avancée en matière de signalement d'alerte même si des interrogations demeurent quant aux modalités pratiques de la gradation du lancement de l'alerte (2).

2. Des exemples marquants

Les exemples de Snowden (a) et *Wikileaks* (b) ont montré que les lanceurs d'alerte s'exposaient à des risques réels.

a) L'affaire Snowden

L'affaire Snowden qui a clairement bouleversé les hauts sommets du gouvernement américain n'aurait pas été possible sans le Darknet. Né le 21 juin 1983, Edward Snowden est un informaticien et expert en sécurité. Il s'engage dans l'armée le 7 mai 2004 afin d'aider les peuples à lutter contre l'oppression mais quitte rapidement la formation à la suite d'un accident qui l'oblige à abandonner. C'est à ce moment[307] qu'il est embauché par la CIA afin de travailler dans la sécurité informatique. Son absence de diplôme a été compensée par ses compétences rares en informatique. De 2007 à 2009, il est affecté par la CIA à la mission américaine des Nations unies en Suisse. Cette période est formatrice mais surtout révélatrice quant aux méthodes de l'agence américaine. Il raconte comment un banquier suisse a été piégé par la CIA qui l'aurait délibérément rendu ivre et encouragé à rentrer en voiture afin de le protéger en échange d'information ; lors de son arrestation, la CIA lui a en effet apporté son aide pour qu'il

[307] En 2006.

devienne un informateur. C'est à partir de ce moment que Snowden a ouvert les yeux sur les agissements de l'agence américaine.

En 2009, il quitte la CIA pour rejoindre Dell, une entreprise américaine qui régit les systèmes d'information d'agences gouvernementales comme la NSA. Il est chargé de l'enseignement des méthodes de contre-renseignement électronique et dispose d'un accès considérable aux donnés de la NSA qu'il commence à rassembler dès 2012. L'année suivante, Il devient administrateur système pour Booz Allen Hamilton, un sous-traitant de la NSA. C'est ainsi qu'il continue son recueil d'informations ultraconfidentielles à l'aide d'une clé USB. Snowden est prêt à sacrifier sa vie confortable pour ses convictions[308] : « *je ne veux pas vivre dans une société qui fait ce genre de choses… Je ne veux pas vivre dans un monde où tout ce que je fais et dis est enregistré. Ce n'est pas une chose que je suis prêt à supporter* »[309]. En mai 2013, il quitte les Etats-Unis et se dirige vers Hong Hong pour y rencontrer les journalistes Glenn Greenwald et Laura Poitras, fondatateurs de « *Freedom of the Press Foundation* », une organisation dont l'objectif est de financer et soutenir les actions d'intérêt public ; il leur communique ses informations et leur confie des dizaines de milliers de documents de la NSA.

Par suite, il est poursuivi par la justice américaine pour vol, espionnage ainsi que utilisation illégale de biens gouvernementaux[310] et souhaite quitter Hong Kong pour se réfugier en Equateur : « *Moi, Edward Snowden, citoyen des États-Unis d'Amérique, je vous écris pour solliciter l'asile à la république de l'Equateur, face au risque de persécution de la part du gouvernement des Etats-Unis et de ses agents en relation avec ma décision de rendre publiques de graves violations de la part du gouvernement des Etats-Unis d'Amérique de leur Constitution – concrètement du quatrième et du cinquième amendement – ainsi que de plusieurs traités des Nations unies souscrits par mon pays*[311] ». Finalement, c'est la Russie qui lui accorde

[308] MACASKILL E., *Interview Edward Snowden*, NSA files source, 10 juin 2013. Disponible à cette adresse : https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why, [consulté le 25 août 2016].
[309] Texte original : « *I don't want to live in a society that does these sort of things … I do not want to live in a world where everything I do and say is recorded. That is not something I am willing to support or live under* ».
[310] La plainte est déposée en Virginie.
[311] Courrier international, *« Moi, Edward Snowden, je vous écris… »*, 25 juin 2013. Disponible à cette adresse : http://www.courrierinternational.com/revue-de-presse/2013/06/25/moi-edward-snowden-je-vous-ecris, [consulté le 22 août 2016].

un droit d'asile jusqu'en 2020 après une prolongation de trois ans[312].

Les révélations d'Edward Snowden ont modifié la donne en matière de droit des internautes et de préservation de l'anonymat. Le décor numérique est de plus en plus sombre puisque la cybersurveillance mise en place par la NSA porte directement atteinte à la vie privée des internautes.

L'incommode Déclaration d'Indépendance du cyberespace de John Perry Barlow a désormais un réel impact sur le monde numérique. Grâce aux réseaux alternatifs que sont les darknets, ce dernier incarne désormais un surprenant moyen d'échange libertaire permettant de lutter contre les outils de surveillance et la pression des Etats. Dès 2013, l'utilisation de logiciels comme *Pretty Good Privacy* ou Tor, n'est plus réservée aux spécialistes et se démocratise. Néanmoins, cette privatisation du réseau inquiète et certains redoutent l'apparition d'un Internet à deux vitesses et dénonce l'absence de neutralité du réseau par excellence. L'exemple de *Wikileaks* mérite également d'être présenté (b).

b. *Wikileaks*

Fondé en 2006 par l'informaticien Julian Assange, *Wikileaks* est une organisation non-gouvernementale qui donne une audience aux fuites d'informations et aux lanceurs d'alertes qui peuvent protéger leurs sources. Elle a fait l'objet de cyberattaques orchestrées par le gouvernement américain qui a tenté de faire fermer son site Internet.

En 2007 déjà, la base de données de WikiLeaks est complétée par plus d'un million de documents obtenus grâce à une grande communauté composée de dissidents situés un peu partout à travers le monde : en Chine, en Iran ou à Taïwan par exemple.

En 2010, une vidéo publiée sur *Wikileaks* avait déjà dénoncé les bavures de l'armée américaine en Irak : « *les principes généraux sur lesquels notre travail s'appuie sont la protection de la liberté d'expression et de sa diffusion par les médias, l'amélioration de notre histoire commune et le droit de chaque personne de créer l'histoire. Nous dérivons ces principes de la Déclaration*

[312] le 18 janvier 2017.

universelle des droits de l'homme. En particulier, l'article 19[313] *inspire le travail de nos journalistes et autres volontaires*[314] ».

Dès juillet 2010, les révélations faites par *WikiLeaks* sont diffusées par plusieurs journaux nationaux comme The Guardian[315], Le Monde[316], El Pais[317], le New York Time et Der Spiegel[318], généralement en Une.

En 2010, Wikileaks dénonce des crimes de guerre orchestrés par les Etats-Unis en diffusant les « *War Logs* », des dizaines de milliers de documents militaires secrets sur la guerre en Afghanistan. Mais, c'est avec les révélations du « *Cablegate* » qu'il est mis sous le feu des projecteurs : le 28 novembre de la même année, Wikileaks révèle plus de 250 000 documents qui seront relayés par des journaux partenaires comme le *New York Times* ou Le Monde ; il s'agit de télégrammes de la diplomatie américaine montrant les négociations opérées par les ambassades à travers le monde[319]. D'autres affaires vont suivre : en janvier 2011 un banquier suisse dénonce des personnalités de grandes entreprises et des personnages politiques qui utilisaient des paradis fiscaux dans les Caraïbes[320] ; la même année à la suite d'un séisme ayant entraîné la catastrophe nucléaire de Fukushima au japon Wikileaks publie des documents démontrant une faille puisque les réacteurs nucléaires ne pouvaient résister qu'à des séismes d'une magnitude de degré 7 sur l'échelle de Richter[321] ; le 25 avril 2011, le site dénonce les conditions de détention de Guantanamo ; en 2012 des informations sensibles sont publiées sur

313 « *Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontière, les informations et les idées par quelque moyen d'expression que ce soit* ».
314 « *The broader principles on which our work is based are the defence of freedom of speech and media publishing, the improvement of our common historical record and the support of the rights of all people to create new history. We derive these principles from the Universal Declaration of Human Rights. In particular, Article 19 inspires the work of our journalists and other volunteers* ».
315 *The Guardian* est un quotidien d'information britannique.
316 Le Monde est journal français.
317 *El Pais* est un quotidien généraliste espagnol.
318 *Der Spiegel* est un journal hebdomadaire allemand.
319 OURDAN R., *WikiLeaks : dans les coulisses de la diplomatie américaine*, 28 novembre 2010. Disponible à cette adresse : https://www.lemonde.fr/international/article/2010/11/28/wikileaks-dans-les-coulisses-de-la-diplomatie-americaine_1446078_3210.html, [consulté le 17 novembre 2014].
320 DELCROIX M., *Wikileaks s'attaque au secret bancaire*, 18 janvier 2011. Disponible à cette adresse ; http://www.rfi.fr/europe/20110117-wikileaks?utm_medium=twitter.
321 Libération, *Les centrales japonaises, « un problème sérieux » pour l'AEIA, révèle Wikileaks*, , 17 mars 2011. Disponible à cette adresse : https://www.liberation.fr/planete/2011/03/17/les-centrales-japonaises-un-probleme-serieux-pour-l-aeia-revele-wikileaks_722242, [consulté le 29 septembre 2015].

la Syrie[322] ; en 2013 Wikileaks publie les « *Kissinger cables* » un ensemble de documents liés à Henry Kissinger[323] et classés secret défense[324] ; le 23 juin 2015, le site révèle que trois présidents de la République, Hollande, Sarkozy et Chirac, ont été mis sur écoute par la NSA ; en juillet 2015, le site dévoile que des hauts responsables d'entreprises et du gouvernement japonais ont été espionnés par les Etats-Unis[325] ; en octobre 2016, des mails de l'ancien directeur de campagne d'Hillary Clinton sont publiés par Wikileaks, c'est la « *Pizzagate* » qui démontrerait l'existence d'un réseau pédophile autour de l'ancienne candidate à la présidence[326]. En raison de son caractère controversé, le site a rompu les liens avec de nombreux services de paiement et banques comme *PayPal*. Pour assurer sa survie future, Wikileaks a dû trouver de nouveaux moyens de financement et le Bitcoin a saisi cette opportunité. En effet, la cryptomonnaie est devenu un moyen de paiement pour envoyer des dons à Wikileaks et c'est à cette occasion qu'elle est devenue très populaire.

Julian Assange aspire à ce que Wikileaks devienne « *l'organe de renseignement le plus puissant au monde*[327] ». Néanmoins, ce site est considéré comme un « *service de renseignement hostile* » par les Etats-Unis[328]. Mike Pompeo, ancien directeur de la CIA et désormais secrétaire d'Etat des Etats-Unis, estime qu'il « *est temps de dire ce que WikiLeaks est réellement : un service de renseignement non étatique hostile, souvent soutenu par des acteurs étatiques comme la Russie* ».

En dépit de cette réputation, WikiLeaks a inspiré d'autres sites à travers le monde. A titre d'exemple, en janvier 2011, OpenLeaks a été créé par d'ancien membres de Wikileaks qui

[322] Disponible à cette adresse : https://wikileaks.org/syria-files.
[323] Prix Nobel de la paix en 1973, Henry Kissinger est secrétaire d'Etat des Etats-Unis de 1973 à 1977.
[324] *Wikileaks les kissenger cables*, 8 avril 2013. Disponible à cette adresse : http://www.rue89.com/2013/04/08/wikileaks-les-kissinger-cables-nouvel-assaut-contre-ladministration-us-241277, [consulté le 29 septembre 2015].
[325] LES ECHOS, *Les Etats-Unis ont espionné gouvernement et entreprises au Japon*, le 31 juillet 2015. Disponible à cette adresse : https://www.lesechos.fr/31/07/2015/lesechos.fr/021239469249_les-etats-unis-ont-espionne-gouvernement-et-entreprises-au-japon.htm, [consulté le 4 septembre 2015].
[326] 20 minutes, *Piratage des e-mails de la campagne Clinton : Les dégâts d'une simple faute de frappe*, 14 décembre 2016, https://www.20minutes.fr/high-tech/1980199-20161214-piratage-e-mails-campagne-clinton-degats-simple-faute-frappe, [consulté le 15 décembre 2016].
[327] HERBET M., *Wikileaks, une machine à scoops efficace mais opaque*, 26 juillet 2010. Disponible à cette adresse : http://www.lefigaro.fr/international/2010/07/26/01003-20100726ARTFIG00516-wikileaks-une-machine-a-scoops-efficace-mais-opaque.php, [consulté le 2 mai 2015].
[328] UNTERSINGER M., *Le chef de la CIA s'en prend violemment à Wikileaks*, 14 avril 2017. Disponible à cette adresse : https://www.lemonde.fr/pixels/article/2017/04/14/le-chef-de-la-cia-s-en-prend-violemment-a-wikileaks_5111561_4408996.html, [consulté le 15 avril 2017].

estimaient que Julian Assange n'était pas transparent et qui lui reprochaient sont « *autoritarisme*[329] ». En France, le 10 mars 2011, Mediapart, un site d'actualité, lance *FrenchLeaks*[330], au Qatar, *Al Jazeera* ouvre « *Al Jazeera Transparency* »[331], au Québec, *QuébecLeaks* est lancé le 9 mars 2011 afin d'obtenir « *une transparence complète de la part du gouvernement du Québec*[332] », et aux Etats-Unis le « *Wall Street Journal* » lance sa « *Safe House* » le 6 mai 2011[333].

Wikileaks fait office d'intermédiaire entre les informateurs et la presse mais le site affirme qu'il ne sollicite aucune information même si Julian Assange précise qu'il est susceptible de demander une aide pour obtenir des documents[334]. Le cas échéant, la divulgation des documents fonctionne anonymement. En effet, le site mise sur une protection de l'identité en raison du contenu qui touche à des points sociaux, politiques ou militaires permettant d'assurer une réelle transparence. Le site pense être étanche aux contrôles des autorités et impossible à censure. Ainsi, les technologies de chiffrement renforcent Wikileaks en garantissant un anonymat empêchant l'identification. Le site utilise des versions modifiées de PGP, Tor et Freenet (B).

B) Une arme contre la censure

Le mot « *Dark* » fait référence au caractère sombre de l'anonymat, qui permet de commettre des délits en tout impunité mais aussi et surtout de se protéger des abus des puissants. Certains le nomment « *Librenet* » car dans les pays où des pratiques acceptées en France ne le sont pas, le Darknet devient une échappatoire.

« *Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit* », cette liberté fondamentale prévue à l'article 19 de la Déclaration Universelle des

[329] Magret D., *Un ancien de WikiLeaks prépare un site concurrent*, 10 septembre 2011.Disponible à cette adresse : https://www.nouvelobs.com/les-internets/20101211.OBS4515/un-ancien-de-wikileaks-prepare-un-site-concurrent.html, [consulté le 14 octobre 2015].
[330] Page disponible à cette adresse : https://www.frenchleaks.fr.
[331] Al Jazeera Transparency Unit. Disponible à cette adresse www.ajtransparency.com.
[332] www.branchez-vous.com : QuébecLeaks, la version québécoise de Wikileaks.
[333] Page disponible à cette adresse : https://www.wsjsafehouse.com.
[334] NYSTEDT D., *Wikileaks leader talks of courage and wrestling pigs*, PC World Australia, Sydney, 28 octobre 2009.

Droits de l'Homme[335] a pour corollaire la liberté de la presse, la liberté de réunion, la liberté d'association ainsi que le respect d'autrui. En France, les individus sont libres d'avoir n'importe quelle opinion et d'accéder à toutes les informations sans que quelqu'un puisse les censurer. La profusion de la connectivité Internet a occasionné un accroissement de la disponibilité de l'information, tout en renforçant le discours et la liberté d'expression. Toutefois, il est imprudent de croire aveuglement à la théorie selon laquelle l'Internet est incontrôlable puisque la pratique a démontré qu'il était possible d'en censurer une grande partie. En effet, les utilisateurs des services en ligne sont les plus exposés par ce manque d'anonymat[336], même en utilisant un darknet.

En Chine par exemple, si un utilisateur se connecte sur Tor, il sera aussi visible que s'il portait une pancarte avec pour inscription « *Hey, je n'aime pas le régime* ». En utilisant un darknet du jour au lendemain alors qu'il utilisait un réseau commun, un internaute peut attirer l'attention et être mis sous surveillance. Une fois repéré, son identification sera rapide. Selon Eric Filiol, spécialiste de la cryptologie et ancien Lieutenant-Colonel dans l'armée de Terre « *avec un outil comme Tor, vous allez peut-être blinder la porte, mais si votre maison est en carton, ou si vous avez laissé vos clefs sous le paillasson, cela ne sert pas à grand-chose…* ».

Les premiers grands promoteurs du Darknet sont les associations de journalistes. Selon Olivier Tesquet, journaliste[337], si *Google* et *Facebook* étaient à mi-chemin entre l'architecture Haussmannienne et le panoptique Foucaldien, les darknets seraient un peu la psychogéographie de la dérive[338]. Il y a une volonté de civiliser les darknets comme l'internet a été civilisé. Penser que le Darknet est entièrement verrouillé est une erreur. Les autorités cherchent à délivrer un message politique en l'instrumentalisant. En effet, les chiffres donnés sont les chiffres du FBI probablement surestimés dans la mesure où il n'y a aucun moyen de les vérifier. Ils sont donnés à partir d'une conversion de bitcoins qui a beaucoup fluctué. Un réseau d'anonymisation comme Tor a précisément été conçu pour qu'on ne puisse pas savoir ce qu'il s'y passe. C'est le réseau lui même, la manière dont il fonctionne qui permet cet anonymat.

[335] Déclaration Universelle des droits de l'homme, adoptée par l'Assemblée générale de l'ONU à Paris, le 10 décembre 1948.
[336] TAN Z., W. FOSTER W., GOODMAN S., *China's state-coordinated internet infrastructure Communications of the ACM*, 1999.
[337] Journaliste à Télérama où il suit plus particulièrement les questions numériques, il est en outre auteur de *Comprendre Wikileaks.*
[338] Ce sont des outils modernes de surveillance et le Darknet lutte en plaçant l'individu au centre.

Olivier Tesquet échange avec ses sources et avec d'autres journalistes par le biais du Darknet. Il utilise « *Signal Messaging* », un outil aussi simple, en terme d'ergonomie et d'utilisation, que les autres applications du quotidien, et parle de résistance passive et de banalisation du Darknet. Un réseau darknet peut être utilisé pour la protection des sources mais aussi pour le journaliste lui même dans des pays où l'activité journalistique est condamnée. Les réseaux darknets sont donc créés afin préserver l'anonymat si bien qu'il n'est pas conseillé d'alterner la navigation entre le darkweb et le web visible afin de ne pas compromettre cet anonymat. Le Darkweb offre des fonctions similaires à celles du web public pour que l'internaute n'utilise qu'un seul navigateur.

Toutefois, le Darknet a été détourné de son utilité initiale et a désormais un sombre côté ayant fait l'objet d'une forte médiatisation. Il convient de traiter les mauvais côtés du Darknet (Chapitre 2)

CHAPITRE 2
LES MAUVAIS COTÉS DU DARKNET

Lorsqu'il découvre le Darknet en 2016, le député de Paris Bernard Debré n'en revient pas : « *La France est une plaque tournante de la drogue, un supermarché de la drogue !* », l'ancien Ministre décrit comment « *se procurer sur Internet des drogues et de se les faire envoyer par voie postale !* ». Lors d'un reportage en immersion[339], il mène en collaboration avec le président d'une association anti-drogue[340], Serge Lebigot, et le journal Valeurs Actuelles, une opération afin de montrer à quel point il est facile de se procurer des stupéfiants de toute sorte sur le Darknet.

Le 21 juin 2016, il réclame une mission parlementaire et déplore dans l'hémicycle : « *Cocaïne, champignons hallucinogènes, marijuana et cannabis de synthèse, voici les drogues qu'on peut se procurer aussi facilement que l'on commande une paire de chaussure. Comment est-ce possible ? C'est simple, directement sur internet par des sites bien souvent hébergés aux Pays-Bas, paiement par carte bleue et la marchandise arrive sous pli, discret, à l'adresse de votre choix. Une autre option, plus sûre mais un peu plus compliquée existe, passer par le Darknet : nous voilà sur le plus grand marché de l'horreur du monde, les trafiquants en tout genre y côtoient terroristes, pédophiles, pour payer il suffit de disposer de Bitcoins, monnaie virtuelle qui s'achète auprès des banques en ligne et la livraison là encore, par voie postale venant cette fois-ci de France. Après analyse demandée par un hebdomadaire[341] et réalisée par la Police, le constat est édifiant, la cocaïne étant d'une qualité jamais vue, pure à 90%[342]. Je demande que soit mis en place un véritable programme de lutte contre le trafic au sein de l'Union Européenne en assurant un meilleur contrôle aux frontières et en traquant les acheteurs français. Je demande, par ailleurs, que soit mise en place, une mission d'information sur la lutte contre ce trafic et les nouveaux modes de distribution des nouvelles drogues en France qui prennent progressivement la place des dealers physiques. Je demande qu'on interdise les Bitcoins qui servent surtout au trafic et au blanchiment d'argent* ».

[339] *Darknet : enquête sur l'hypermarché virtuel de la drogue*. Disponible à cette adresse : https://www.youtube.com/watch?v=RaUGdrik74Q, [consulté le 15 avril 2017].
[340] Parents contre la drogue.
[341] Valeurs Actuelles.
[342] Le gramme y serait vendu à un peu plus de 80 euros.

Ce coup de communication ayant permis au grand public la découverte du Darknet ne s'arrête pas là car selon Bernard Debré, il est possible de s'y procurer *« des kalachnikovs, du TNT, des faux billets, des organes à greffer, de la cocaïne* ». Il ajoute même que « *le Darknet dérégule même les dealers de drogue en France ! C'est l'ubérisation*[343] *de la drogue*[344] ».

Effectivement, les raisons pour lesquelles des individus utilisent le Darknet sont nombreuses et ne correspondent pas toujours aux points de vue des concepteurs[345]. Les profils des individus surfant sur le web sombre sont divers et ont très souvent un point commun puisque beaucoup accèdent au web sombre dans le dessein d'y commettre des infractions. Par exemple, les personnes qui sympathisent avec l'Etat Islamique peuvent communiquer ou même rechercher des financements via le Web sombre. En outre, il existe un infâme marché noir appelé *Silk Road* où s'effectue achats et ventes d'arme, de drogue ou de contrefaçon.

De manière générale, les infractions commises sur le Web sombre peuvent être divisées en plusieurs catégories. Premièrement, il existe des cybermarchés noirs sur lesquels il est possible de trouver des contrefaçons, des drogues, des numéros de cartes bancaires, des armes, etc. Deuxièmement, des échanges de contenus choquants et illégaux sont effectués sur le Web sombre. Dès lors il est possible d'avoir accès à des images pédopornographiques, de torture, de cannibalisme, de sexe violent, etc. Enfin, des services illégaux permettent de faire appel à un tueur à gage, de transporter des organes, d'acheter des logiciels malveillants, etc.

Par conséquent, toutes ces infractions sont liées aux formes de criminalité « *traditionnelles* », qui ont été facilitées par les nouvelles technologies de l'information et de la communication au point de constituer un nouveau vecteur de criminalité. Les cybercriminels étendent leur emprise en même temps que le développement d'Internet. Leur force réside dans le fait qu'ils ne sont pas visibles de sorte qu'il est difficile de les connaître. Chaque utilisateur d'Internet s'expose à une menace et peut devenir malgré lui, la cible d'un délit. Les conséquences peuvent être importantes pour les individus, les organisations mais aussi pour l'Etat. En outre, il existe d'autres infractions qui n'existaient pas avant l'apparition d'Internet, ce sont les atteintes aux

[343] Ce néologisme désigne le phénomène économique qui consiste à utiliser les nouvelles technologies afin de mettre en relation professionnels et clients dans le cadre d'un service.
[344] *Bernard Debré (LR) : comment j'ai acheté de la drogue sur internet*, 28 juin 2016.
[345] BOUHADANA I., GILLE W., HARIVEL J., Darknet le côté obscur du Net, Panthéon Sorbonne Magazine n°6, Janvier-Février 2014.

STAD.

Ainsi, journalistes et politiques en proie à de nombreuses contradictions, tentent tant bien que mal de les résoudre mais avec des raccourcis à la limite de la désinformation. Ce chapitre sera l'occasion de vérifier ce qui a été avancé à propos du contenu accessible via Tor (Section 1) mais aussi de traiter du Bitcoin, cette cryptomonnaie présentée comme « *la monnaie du crime* » (Section 2).

SECTION 1
Le contenu accessible via Tor

En 1972, bien avant la création d'Amazon, des étudiants de l'Université de Stanford et du MIT ont effectué la première transaction en ligne. En utilisant leur compte ARPAnet, ils ont vendu une petite quantité de marijuana à leurs homologues du Massachusetts. C'est probablement la première transaction illégale en ligne. Depuis, Internet a clairement transformé les marchés et le commerce. Désormais tous les acheteurs et vendeurs du monde sont connectés.

De nouveaux marchés ont été ouverts et facilités si bien que les achats en ligne sont devenus une habitude pour la moitié des consommateurs mondiaux. Parallèlement à ce commerce électronique qui génère des milliards de dollars, il existe un autre marché qui progresse aussi très rapidement. Ce monde souterrain propose l'achat de toute sorte de choses, qu'elles soient légales ou non. En 2014 un sondage mené auprès de 80 000 consommateurs de drogues à travers quarante-trois pays a montré que les clients se fournissaient de plus en plus sur Internet. Au début des années 2000, le premier grand marché en ligne de stupéfiants est créé sur le Web visible : « *The Farmer's Market* ». En 2010, ce marché a migré vers le Darknet. En 2015, il existe environ 40 000 sites sur le réseau darknet Tor. Grâce à son système sophistiqué de chiffrement, Tor est l'endroit idéal pour les marchés non réglementés. Bien que de nombreux services cachés soient légaux, environ 15% concernent des marchés illégaux. Les services cachés de Tor sont des sites ayant une extension URL en .onion. Ces sites peuvent être créés par tout utilisateur souhaitant proposer divers services. Chaque URL, contenant 16 caractères alphanumériques, peut être créé de façon automatique ou à partir de vrais mots afin de permettre une meilleure identification du contenu. Un URL en .onion peut héberger différents services tels qu'un site web, un service d'email ou de messagerie instantanée.

Avec l'arrivée de ces « *marchés noirs* », il y a légitimement eu un enchainement de critiques et de consternation. En 2011, le « *Sydney Morning Herald*[346] » estime que «Les autorités sont impuissantes face au florissant marché de la drogue en ligne [347] », alors qu'en 2012, the « *Daily*

[346] Le *Sydney Morning Herald* est un journal Australien publié quotidiennement.
[347] Texte original : « the flourishing online drug market authorities are powerless to stop ».

Mail[348] » appelle *Silkroad* « l'endroit le plus sombre d'Internet[349]». En outre, Charles Schumer, sénateur de l'Etat de New-York depuis 1999, demande une enquête sur *Silkroad* en 2011 et décrit le site comme « *La tentative la plus audacieuse pour vendre de la drogue en ligne* [350] ». S'il n'est pas surprenant que les marchés de stupéfiants en ligne existent, le fait qu'ils fonctionnent l'est. En effet, les marchés sombres sont des environnements exceptionnellement dangereux pour mener des affaires. Les acheteurs et les vendeurs sont anonymes et ne se rencontrent jamais. Il n'y a aucun régulateur à qui s'adresser si le vendeur ou les administrateurs du site décident de prendre votre argent. En dépit de tous ces paramètres, les marchés du Darknet prospèrent car ils ont su s'adapter. La seule vraie différence qui existe entre ces marchés et les sites de commerce classiques est le fait que les produits proposés à la vente sont différents. Le reste est assez similaire car on y retrouve toutes les fonctionnalités de base : un menu vertical, des photos en haute définition, un panier d'achat, des commentaires, des produits en promotion, la livraison gratuite, une messagerie interne, un forum et même un système de notation des vendeurs.

Sur le Darknet, l'utilisateur ne trouve que ce qu'il est venu chercher, il est nécessaire d'utiliser des annuaires d'adresses de sites particuliers tels que les *hidden wiki*[351] ainsi que des moteurs de recherche tels que *Onion city* ou *Grams*. Le contenu accessible est volatile et la durée de vie des sites faible : d'une heure à quelques mois. Les sites illégaux doivent leur fiabilité à leur discrétion et à leur furtivité. Le premier critère est garanti grâce aux caractéristiques du réseau. Le second nécessite, comme dans le monde réel, un changement de lieu de trafic. Tor offre la possibilité d'effectuer des transactions illégales grâce au e-commerce façon Darknet (§1), mais l'offre de contenu va au delà de la vente de drogue ou d'armes. Le Darknet serait devenu un repaire de criminel (§2).

§1) L'e-commerce façon Darknet

Les aspects criminologiques de ce travail de recherche m'ont amené à naviguer sur le Darknet. Il s'agissait de comprendre les fonctionnalités et le potentiel criminel du web sombre. Une préparation méthodique m'assurant une hygiène numérique a été indispensable pour une telle

[348] Le Daily Mail est un journal Britannique.
[349] Texte original : « *the darkest corner of the Internet* ».
[350] Texte original : « *the most brazen attempt to peddle drugs online that we have ever seen* ».
[351] Ce sont des wikis cachés.

navigation. Ce faisant, l'exploration du Darknet a nécessité l'achat d'un ordinateur neuf rattaché à aucune adresse IP. En outre, l'accès au Darknet se faisait systématiquement par le biais d'une connexion permise grâce à un Hotspot public avec une adresse mel spécialement créée afin de naviguer sur le Darknet. Les deux réseaux utilisés ont été Freenet et Tor. Ainsi, tout ce qui est exposé dans ce chapitre a été vérifié[352].

Le e-commerce de surface repose sur le marketing et la communication. L'interface d'un site web doit être attrayante et le côté pratique ne peut pas être négligé. Oubliez ces fondamentaux, sur le Darknet les sites sont rudimentaires, le développement ergonomique n'est pas la priorité. Tous les sites se ressemblent et disposent juste d'une barre permettant aux utilisateurs de naviguer entre les différentes catégories de produits. La création d'un identifiant et d'un mot de passe est nécessaire pour l'inscription. Ensuite, l'utilisateur doit se doter d'un portefeuille de cryptomonnaie, le plus souvent de bitcoin puisque la plupart des paiements se font avec cette cryptomonnaie[353].

La sécurisation de ces derniers se fait via un système de cagnotte appelé « *mixeurs* » : plusieurs clients utilisent un portefeuille commun et lors d'un achat, l'argent provient du compte « *mixeur* » et non du portefeuille de l'acheteur qui ne pourra pas être directement rattaché à la transaction. Outre ce service qui permet de garantir un anonymat certain non assuré par le bitcoin, il existe les « *escrow* ». Critère de fiabilité d'un site marchand, les *escrow* permettent de bloquer l'argent le temps de la livraison. Un *escrow* est donc composé d'un vendeur, d'un acheteur et d'un tiers, généralement administrateur du site, qui recevra un pourcentage pour le travail effectué. Deux des protagonistes, ou parfois trois, doivent intervenir pour finaliser la transaction. Cette garantie supplémentaire rassure le client qui a plus de chance de recevoir sa commande même s'il doit quand même faire confiance à la tierce personne qui peut disparaître avec la somme.

D'une manière générale, le Darknet est associé à Tor qui est lui même associé à *Silkroad* le supermarché de la drogue en ligne par excellence (A). Pourtant, il existe de nouveaux marchés (B) qui méritent d'être présentés.

[352] Les explications de ce paragraphe sont issues de ma propre navigation sur le Darknet et de l'ouvrage suivant : BARTLETT J., *The Darknet*, Cornerstone Digital, 2014.
[353] 40% des paiements cybercriminels selon un rapport d'Europol.

A) *Silkroad*, le supermarché de la drogue

Créé en 2011, à son apogée *Silkroad* était composé de 4000 vendeurs et de 150 000 clients anonymes à travers le monde. Sa particularité ? Les produits mis en vente sont souvent illégaux. Utilisable via Tor, ce marché propose toutes sortes de produits. Il est possible d'y trouver de la drogue, des médicaments, des ouvrages, des sex-toys, des contrefaçons de cigarettes ou de vêtements… En deux ans, plus d'un million de transactions ont rapporté entre 700 000 et 1,4 millions bitcoins[354]. Mais en plus du caractère commercial, le site est créé comme un mouvement politique associé aux revendications des Cypherpunks. Son succès est fondé sur la réputation qui est fondamentale sur le Darknet. Les statistiques des différents marchés et les avis des internautes sont importants dans ce marché où la concurrence est rude. Donc, pour faire des bénéfices un vendeur se doit d'être irréprochable.

Le succès de ce marché a bien évidemment attiré l'attention du FBI qui a mené l'enquête. Leurs recherches les amènent au pseudonyme « *altoid* » qui évoquait *Silk Road* avant même qu'il soit connu. Aussi étonnant que cela puisse paraître, il s'agissait bien du créateur de *Silk Road* qui utilisait une adresse *Gmail* créée avec de vraies informations personnelles. Dès lors, les enquêtes ont découvert que le mail avait été créé par un certain Ross Ulbricht dont les idées correspondaient fortement à celles de DPR le gérant du site. Ross, un jeune homme diplômé d'un master scientifique, est accusé d'être le fondateur et l'administrateur du site. La lecture de ses conversations montre que Ross a commandité plusieurs assassinats. Il est poursuivi et condamné à la prison à perpétuité. Il s'agit de traiter dans un premier temps la mise en place du marché (1), avant d'étudier dans un second temps, la réputation numérique (2) qui a été le fondement de sa réussite.

1. La mise en place du marché

Le 27 novembre 2010, un utilisateur nommé « *Altoid* » poste un message sur « *the Shroomery* », un forum du web visible proposant des champignons hallucinogènes : « *J'ai visité un site web appelé Silk Road. C'est un service caché de TOR qui permet d'acheter et vendre toute sorte de choses anonymement. Je pense à acheter quelque chose, mais je voulais savoir si quelqu'un en*

[354] Entre 13 et 15 millions euros.

avait déjà entendu parler pour le recommander[355] ». Deux jours après ce même *Altoid* intègre une discussion au sujet de cryptomonnaie sur *bitcointalk.org* : « *est-ce que quelqu'un a déjà visité Silk Road ? C'est une sorte d'Amazon anonyme. Je ne pense pas qu'il y ait de l'héroïne, mais ils vendent d'autres trucs* [356] ». *Altoid* propose un URL apportant plus de précisions et invite les utilisateurs à s'inscrire comme vendeur ou acheteur. Le lien montre que « *Marijuana, Shrooms*[357] *and MDMA*[358] » y sont déjà en vente. Grâce au bouche à oreille, quelques vendeurs et acheteurs s'y inscrivent.

En mai 2011, plus de 300 produits étaient proposés, presque tous des stupéfiants. Le véritable tournant de ce marché aura été la publication d'un article sur *Silkroad* par le blog « *Gawker* » en juin 2011. Dès lors, des milliers d'internautes se précipitent dessus pour y trouver une alternative sérieuse aux autres sites de vente. En effet, l'ergonomie et les fonctionnalités du site sont très intéressantes. Outre le fait que les différents produits sont répertoriés par catégorie sur le côté gauche site, les vendeurs y sont représentés avec une brève description et une photo. De plus, un lien vers un service client est donné pour la gestion des éventuelles plaintes liées aux achats. Derrière cette façade le site est très sophistiqué, accessible via le navigateur Tor et les achats de produit ne se font qu'avec des bitcoins. Les visiteurs qui sont invités à s'inscrire avec des pseudonymes numériques communiquent sur un forum sécurisé qui leur est dédié, et ce, de manière cryptée et sécurisée car une fois lus, les messages sont automatiquement supprimés. En outre, la gestion du site est très intéressante et bien adaptée à la clientèle.

En octobre 2011, *Altoid* retourne sur *bitcointalk.com* afin de trouver des administrateurs pour le maintien du site. Dès lors, il forme une équipe de cinq administrateurs. Ces derniers, payés entre 1000 et 2000 dollars par semaine, traitent les plaintes des acheteurs et des vendeurs, règlent les différends entre utilisateurs et surveillent les éventuelles infiltrations des autorités. Des rapports hebdomadaires sont transmis par le biais de Tor Chat à l'administrateur principal du site : « *Dread Pirate Robert* ». Malgré les attaques répétées et les arrestations de vendeurs, *Silkroad* se développe jusqu'à devenir le plus grand marché de drogue en ligne de tous les

[355] Texte original trouvé sur le Darknet : « *I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it* ».
[356] « *Has anyone seen Silk Road yet ? It's kind of like an anonyous Amazon.com. I don't think they have heroin on there, but they are selling other stuff* ».
[357] Il s'agit de champignons hallucinogènes
[358] La MDMA est une drogue de synthèse souvent contenu dans des pilules appelées ecstasy.

temps. Selon le FBI, *Silkroad* a effectué plusieurs milliards[359] de dollars de ventes grâce à 4000 vendeurs anonymes ayant contracté avec 150 000 clients à travers le monde. Les commissions de DPR ont été estimées à 20 000[360] dollars par jour. Cependant, son projet n'avait pas qu'une motivation financière. Les nouveaux utilisateurs sont accueillis avec ce message : « *J'aimerais prendre un moment pour partager avec vous ce qu'est Silkroad et comment vous pouvez passer votre temps ici. Commençons par le nom. L'originale « Route de la soie » est un ancien réseau commercial connectant l'Asie, l'Afrique et l'Europe. Elle a joué un rôle fondamental en mettant en relation leurs économies. J'espère que cette « Route de la soie » moderne pourra apporter la même chose, en créant un cadre permettant à des partenaires commerciaux de se rencontrer pour obtenir des bénéfices mutuels de manière sûre et sécurisée*[361] ».

Le nom de DPR est tiré d'un livre de 1973 intitulé « *The Princess Bride* » dans lequel le pirate est un hors-la-loi qui protège les personnes vulnérables. La spécificité de DPR réside dans le fait qu'il n'est pas personnifié par un seul homme mais par une série d'individualités qui se transmettent les responsabilités et la réputation. Le choix d'un tel nom est significatif : *Silkroad* est un mouvement politique. Ce dernier s'étend sur des forums du web de surface en prônant cette idée de liberté. Dealers, consommateurs, défenseurs des libertés individuelles : tous se sont investis pour la prospérité de ce marché en ligne non réglementé.

Tout bascule en automne 2013. En dépit des efforts déployés par les administrateurs de Silkroad, les agents du FBI réussissent à l'infiltrer en novembre 2011. Le 1er octobre 2013, ils arrêtent Ross Ulbrich un homme de 29 ans[362] soupçonné de trafic de drogue, de provocation à un assassinat, de piratage informatique et de blanchiment d'argent. DPR a été trouvé à cause d'une erreur de débutant. Lorsque *Altoid* intervenait sur les forums, il le faisait avec un compte rattaché à une adresse mail enregistrée au nom de Ross Ulbrich : rossulbrich@gmail.com. Connu sous le nom de « *Joshua Terrey* », Ross est diplômé d'un Master et vit en colocation

[359] 5 millions de bitcoins.
[360] *DPR* prenait jusqu'à 15% des transactions.
[361] « *I'd like to take a moment to share with you what the Silk Road is and how you can make the most of your time here. Let's start with the name. The original Silk Road was an old-world trade network that connected Asia, Africa and Europe. It played a huge role in connecting the economies trade agreements. It is my home that this modern Silk Road can do the same thing, by providing a framework for trading partners to come together for mutual gain in a safe and secure way* ».
[362] Ross Ulbricht est né le 27 mars 1985 à Austin dans le Texas, une ville très progressiste, étudiante et iconoclaste, très prisée pour les nouvelles technologiques.

avec des individus qui le prenaient pour un trader récemment rentré d'Australie[363]. À la suite de cette arrestation, les choses évoluent vite et le site est fermé. Les visiteurs de Silkroad sont maintenant accueillis par un nouveau message : « *le site a été saisi par le FBI* [364] ». La nouvelle se répand très rapidement sur les forums anonymes tels que « *4chan* » : « *CELA VIENT DE SE PASSER, OH MON DIEU*[365] » a écrit un utilisateur en partageant une capture d'écran de l'avis de retrait du FBI. Un autre utilisateur du forum répond : « *est-ce que vous réalisez ce que cela signifie ? Cela ne concerne pas que les pédophiles avec leur pizza (nom de code qui désigne un film pédopornographique) ou nos drogues. Nous perdons toutes les zones sures que nous avions*[366] ».

Est-ce la fin ? Certainement pas. En effet, sept jours après l'arrestation d'Ulbricht, « *Libertas* », un des administrateurs de Silkroad, poste un message sur le forum afin de présenter un Silkroad 2.0. *Libertas* et d'autres administrateurs du site travaillent avec acharnement afin de reconstruire le site allant même jusqu'à reprendre certains codes sources du site original. Les vendeurs sont impatients de reprendre leurs activités si bien que les administrateurs sont inondés de mails leur demandant d'accélérer la mise en ligne du site. Face à cet engouement, un des administrateurs a dû leur répondre sur le forum « *nous allons aussi vite que possible*[367] ». Un mois plus tard, le site est de nouveau opérationnel et DPR refait surface sur *Twitter* le 6 novembre 2013 : « *vous ne pourrez jamais détruire le principe de #Silkroad*[368] ». Il poste ensuite sur le forum : « *Silkroad vient de renaître de ses cendres et est maintenant prêt pour votre retour. Bienvenue à la liberté* [369] ». Toutefois, les efforts des administrateurs ne sont pas suffisants puisque *Silkroad* perd sa position de leader sur le marché.

D'autres marchés se sont imposés dès 2013. C'est le cas du « *Black Market Reloaded* » et du

[363] MAC R., *Living With Ross Ulbricht : Housemates Say They Saw No Clues Of Silk Road Or The Dread Pirate Roberts*, 9 octobre 2013.
Disponible à cette adresse : https://www.forbes.com/sites/ryanmac/2013/10/09/living-with-ross-ulbricht-housemates-say-they-saw-no-clues-of-silk-road-or-the-dread-pirate-roberts/, [consulté le 9 janvier 2015].
[364] Texte original : « *The hidden site has been seized by the Federal Bureau of Investigation* ».
[365] Texte original : « *IT JUST HAPPENED OMGF, OMGF, OMGF, OMGF* », la phrase est écrite en majuscule afin de mettre en exergue le discours.
[366] Texte original : « *Do you guys realise what this means ? It's not just about pedos with their pizza or us whoth our drugs. We are losing every safe haven we've got ».*
[367] Texte original : « *we are going as fast as we can* ».
[368] Texte original : « *You can never kill the idea of #Silkroad* ».
[369] Texte original : « *Silkroad has risen from the ashes and is now ready and waiting for you to all to return home. Welcome back to freedom* ».

« *Russian Anonymous Market Place* ». Mais à la suite de l'anéantissement de Silkroad, les principaux marchés du Darknet sont devenus instables. Les vrais sites subissent les attaques répétées de divers hackers ainsi que des forces de l'ordre tandis que de faux sites trompent les acheteurs pour leur dérober leurs bitcoins. A titre d'exemple, le site « *Utopia* », mis en place en février 2014, a été neutralisé par la police néerlandaise dans un délai de quinze jours. Les acheteurs et les vendeurs ont perdu la stabilité que leur garantissait *Silkroad*. Une atmosphère de suspicion et de paranoïa pèse sur les marchés. Les autorités ont gagné une bataille, mais pas la guerre. En effet, début 2014, les marchés redeviennent dignes de confiance et fiables et les ventes battent des records : 100 000 entre janvier et avril 2014 pour Silkroad 2.0. Ce dernier doit son succès à sa réputation et à des mécanismes de confiance fondés sur la réputation (2).

2. La réputation numérique

Les marchés du Darknet ne sont accessibles que via un navigateur spécial comme *Tor Browser*. Dès lors, les acheteurs y accèdent souvent grâce au « *Hidden Wiki*[370] », ou à une autre page d'index qui aide à naviguer sur ce web sombre. Ces pages exposent les nombreux marchés existants et le choix est difficile : au moins trente cinq marchés en 2014. Les répertoires qui sont en .onion listent les services qui se trouvent sur le réseau Tor en les catégorisant. Selon Nathalie Nahai, l'auteur de « *Webs of influence*[371] », un ouvrage sur la persuasion en ligne, les internautes jugent inconsciemment les sites web en se fondant sur des « *indices de confiance* ». En règle générale, explique Nahai, ils se réfèrent à la conception du site et accordent leur confiance aux sites simplement construits et facile à utiliser. Nathalie Nahai affirme qu'il s'agit d'une mesure fiable pour évaluer le niveau de confiance du site. La conception et le développement des sites en ligne est une priorité pour les grandes entreprises de commerce électronique qui dépensent énormément. C'est pourquoi les sites du Darknet adoptent la même stratégie. Chaque site a son propre logo. Lorsqu'il refait surface en novembre 2013, *Silkroad* 2.0 conserve le logo du premier *Silkroad* : un commerçant sur un chameau. Le logo du site « *Agora Market* » est un bandit masqué qui brandit une paire de pistolets, tandis que celui du site « *the Outlaw Market* » représente un cowboy.

La concurrence est rude et les méthodes pour attirer les clients sont nombreuses. En avril 2013,

[370] Ce site est accessible sur le Web de surface.
[371] NAHAI N., *Webs of Influence : The psychology of Online Persuasion,* The web psychologist, 2012.

« *Atlantis* », un site concurrent de *Silkroad*, mène une campagne agressive afin d'attirer les acheteurs qui s'approvisionnent chez le concurrent : « *Vous devez donner une bonne raison aux clients de quitter leur marché. Nous le faisons de différentes manières : convivialité, sécurité, meilleurs tarifs (pour le compte vendeur et la commission), un site plus rapide, un support clientèle et des commentaires sur les vendeurs* [372] » a avancé l'administrateur du site. En outre, chaque site ajoute ses propres fonctionnalités. Toutefois, les e-mails de bienvenue et les logos ne suffisent pas à rassurer sur le Darknet. L'esthétique du site « *The Sheep Market* » n'avait plus d'importance lorsque le site s'est envolé avec les 40 millions de Bitcoins des acheteurs et vendeurs. De même pour *Silkroad* 2.0 qui a été piraté en février 2014, avec près de 2,7 millions de Bitcoins perdus. Dès lors, les utilisateurs se fient aux différents forums du Darknet qui dénoncent les sites d'arnaques. Il existe également sur le Web de surface des blogs et des forums dédiés à la recherche de marché et à la discussion sur les fonctionnalités de sécurité. Compte tenu des différents avis postés à travers ces différents forums, en 2014, *Silkroad* 2.0 est encore l'une des meilleures options. Par exemple, « *Defcon* », le nouvel administrateur du site, promet de rembourser tous les vendeurs lésés, et de ne pas toucher de commission avant la résolution de tous les différends. Ce ne sont pas des paroles en l'air puisqu'en avril 2014, *Defcon* a déjà remboursé la moitié des Bitcoins perdus sur Silkroad.

Silkroad 2.0 offre la plus grande variété de produits et le plus grand nombre de fournisseurs : 13 000 listes. S'inscrire sur Silk Road 2.0 est extrêmement simple. Tout d'abord, il suffit de créer un nom d'utilisateur et un mot de passe. Ensuite, après avoir complété le *CAPTCHA*[373], les utilisateurs peuvent lire sur la page principale du site : « *Welcome back*[374] ». Dès lors, le choix est incroyable, il y a près de 870 vendeurs qui proposent toutes les drogues possibles et

[372] Texte original : « *You need to give customers a good reason to move from their existing market. We do this in several different ways : usability, security, cheaper rates (for vendor acount and commission), website speed, customer support and feedback implementation* ».
[373] Texte original : « *Completely Automated Public Turing test to tell Computers and Humans Apart* » soit « *Test public de Turing complètement automatique ayant pour but de différencier les humaines des ordinateurs* ».
[374] Bon retour.

inimaginables : MDMA[375], MDAI[376], 4-emc[377], 4-mec[378], 5-APB[379], 5-IT[380], 6-APB[381], butylone[382], méthylone[383], MPA[384], cannabis, cocaïne, héroïne, opium…

En outre, il y a des sections pour l'art, pour les livres, pour l'alcool, pour de la contrefaçon et pour toute sorte de choses. A titre d'exemple, il est possible d'y trouver des armes à feu, des produits électroniques « *tombés du camion*[385] », des kits de changement d'identité, de suicide ou de piratage, de louer les services d'un pirate informatique, de suivre les appels de son partenaire, d'acheter de la fausse monnaie… En 2014, un utilisateur de *Silkroad 2.0* réalise une enquête en utilisant un programme informatique lui permettant de récolter les détails relatifs à 120 000 ventes entre janvier et avril. C'est ainsi que nous apprenons que la *weed*[386] est l'article le plus vendu (20% de l'ensemble des produits vendus). Elle est suivie de près par la cocaïne (19%), et par le haschich[387] (12%). Mais un vendeur proposant un produit original, à un prix intéressant peut vite être en tête des ventes. Le marché est international puisque les fournisseurs, principalement basés aux Etats-Unis (33%), au Royaume-Uni (10%) ou en Australie (10%), expédient leurs produits dans tous les pays du monde. Toutefois, il faut noter que les grosses opérations sont réalisées par un nombre limité de vendeurs : 21 vendeurs ont vendu plus de 1000 articles entre janvier et avril 2014, 418 vendeurs en ont vendu plus de 100, ce qui donne une moyenne de 178 articles par vendeur. Grâce à la valeur de chaque produit, il est possible de faire une estimation type du chiffre d'affaires des principaux vendeurs durant cette période : le chiffre d'affaires mensuel moyen d'un bon vendeur est compris entre 10 000 dollars et 20 000 dollars, soit un salaire mensuel compris entre 5 000 dollars et 10 000 dollars[388]. Un salaire

[375] La MDMA est une drogue de synthèse souvent contenu dans des pilules appelées ecstasy.
[376] Cette drogue a les mêmes effets que la MDMA mais elle reste moins efficace.
[377] Le 4-Ethylmethcathinone est une drogue de synthèse psychostimulante et entactogène.
[378] Le 4-Methylethylcathinone est une drogue de synthèse psychostimulante et entactogène.
[379] Le 5- (2-aminopropyl) benzofurane est un un entactogène synthétique de la classe chimique des benzofuranes et des amphétamines. Cette drogue produit des effets hallucinogènes euphoriques.
[380] Le 5- (2-aminopropyl) indole est considéré en France comme stupéfiant depuis 2013. Cette drogue a des effets stimulants.
[381] Le 6-(2-aminipropyl) benzofurane est une drogue de synthèse qui crée des sensations de stimulation, de bien-être, de bonheur et d'euphorie.
[382] La butylone est un produit de synthèse qui crée une sensations d'euphorie et de bien-être.
[383] La méthylone est un produit stupéfiant considéré comme un nouveau produit de synthèse.
[384] La méthiopropamine est également un nouveau produit de synthèse.
[385] Vendus sans facture à la suite d'un vol.
[386] Il s'agit de de fleurs séchées de cannabis aussi appelées *marijuana.*
[387] Le haschich est le nom courant de la résine de cannabis.
[388] Généralement les produits sont achetés en gros à un prix deux fois moins élevé que celui de la vente au détail.

très décent, mais incomparable à celui d'un baron de la drogue. En comparaison avec le trafic de drogue traditionnel, ces chiffres correspondent au salaire d'un semi-grossiste ou d'un vendeur au détail et non au salaire d'un négociant international à grande échelle. Les études montrent qu'un dealer de rue français gagne environ 8 000[389] euros par mois alors qu'un grossiste gagne beaucoup plus. Certains vendeurs, ayant déjà leurs contacts et intermédiaires, maximisent les profits grâce à ce nouveau marché qui leur est offert. Selon une autre étude[390] effectuée en janvier 2016 par la *RAND Corporation*[391] sur huit des principaux cryptomarchés dont *Silkroad*, 57% des offres de produits seraient constituées de drogues, 37% de cette proportion de cannabis, 29% de stimulants comme la cocaïne et les amphétamines et 19% représenteraient les variantes de l'ecstasy. Ce qui aurait généré entre 12 et 21 millions de dollars par mois. Selon cette même étude, il existerait en 2016 plus de cinquante cryptomarchés proposant six fois plus de produits qu'en 2013. En ce qui concerne les vendeurs, la plupart serait basée aux Etats-Unis et aurait généré 36% du chiffre d'affaire total de l'échantillon examiné soit 5 millions de dollars par mois. Les soixante-huit vendeurs français ne représentent que 1,8% de ce chiffre d'affaire soit 240 000 dollars. Par ailleurs, l'étude montre que les commandes de plus de 1000 dollars représenteraient plus d'un quart du chiffre d'affaire dans le cadre de trafics hors lignes. Il est même possible d'effectuer des commandes de plus d'un kilogramme si bien que les cryptomarchés constitueraient un important relais d'acheminement de drogue vers les marchés locaux.

L'achat de drogue hors-ligne est conditionné par des critères géographiques et relationnels. Mais, sur le Darknet les paramètres sont différents avec des milliers de fournisseurs qui opèrent à travers le monde. Dès lors, il s'agit de se fier à leur réputation avant d'effectuer un achat éclairé. Comment ? Grâce aux « *user review* [392] ». Des notes sur cinq ainsi que des commentaires permettent d'évaluer la fiabilité d'un vendeur. Par exemple, en février 2014, un vendeur fiable reçoit l'appréciation suivante : « *5/5 : Ce vendeur est très fiable, il est très amical, je vais revenir rapidement*[393] », tandis qu'un autre visiblement moins fiable se voit attribuer le commentaire suivant : « *1/5 : Ce vendeur est un putain d'arnaqueur. Le produit*

[389] Soit environ 9400 dollars.
[390] Disponible à cette adresse : https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html. Taking Stock of the Online Drugs Trade, 2018.
[391] La RAND Corporation est une institution américaine qui vise à améliorer la politique et le processus décisionnel par l'analyse et la recherche.
[392] Ce sont les avis publiés par les internautes qui ont déjà testé le produit.
[393] Texte original : « *This seller is very reliable, he is friendly, I will back soon* ».

n'est jamais arrivé [394] ».

Les acheteurs aussi ont une réputation à protéger. Ils sont jugés en fonction de l'argent qu'ils ont déjà dépensé et en fonction du nombre de remboursement demandé. Le succès de DPR sur *Silkroad* est dû à la confiance qu'il avait accumulée en deux ans grâce à des transactions couronnées de succès. Sa réputation était virtuelle, et personne ne savait qui se cachait derrière ce pseudonyme. À l'instar des sites de vente existant sur le Web visible, une réputation sur le Darknet se fait sur le long terme. Lorsque *Silkroad* a été saisi, les vendeurs ont perdu leurs identités numériques et la réputation qui y était liée. Le Darknet a clairement révolutionné le trafic de drogue. En effet, l'achat de drogue dans la rue ne permet pas d'avoir de recours si les choses ne se passent pas comme prévu ou si le produit n'est pas satisfaisant. Par conséquent, la pureté de la drogue achetée dans la rue est très variable. Elle est généralement coupée avec d'autres substances, et ce, afin que les intermédiaires maximisent leurs profits sans égard pour la santé des acheteurs. À l'opposé, avec les systèmes de commentaires, le darkweb offre un moyen très fiable de déterminer la qualité et la pureté des produits. Quid des tarifs pratiqués sur le Darknet ? Sur *Silkroad*, la cocaïne est proposée à des prix plus intéressants que dans la rue tandis que la marijuana est proposée à des prix moins avantageux. Néanmoins, « *Wedja* », un utilisateur, avance qu'il préfère payer un peu plus cher son produit s'il a l'assurance qu'il sera de bonne qualité.

En raison de l'argent qu'il y a en jeu, certains essaient de contourner le système mis en place. A titre d'exemple, il est possible de créer un faux profil afin de rédiger de mauvais commentaires sur les concurrents ou de payer des utilisateurs afin qu'ils rédigent des critiques favorables. Heureusement, face à ces méthodes, la communauté se réunit souvent pour dénoncer les escrocs. Mais une opération peut-elle être sûre à 100% ? *Silkroad* a tout fait pour permettre cela. De la même façon que sur les sites commerciaux du web visible, les achats sur les marchés du Darknet se font grâce à un paiement préalable qui contraint les acheteurs à être très vigilants.

Cependant, les arnaques sont devenues monnaie courant et ont contraint DPR à intervenir en

[394] Texte original : « *This seller is a fucking scammer. Product never arrived* ».

conseillant d'utiliser les « *escrow* [395] » : *« Utilisez les escrow. Cela ne peut pas être suffisamment souligné. 99% des arnaques proviennent des personnes qui créent de faux compte vendeur et demandent aux acheteurs de les payer directement ou de débloquer le paiement avant la livraison*[396] ».

Ce système existe déjà sur Ebay mais cela reste une innovation sur le Darknet. Il s'agit de portefeuilles spécifiques à chaque site de vente. Sur *Silkroad* un acheteur doit créer un portefeuille dans lequel il transfère des bitcoins. Lors d'une commande, l'acheteur transfère la quantité nécessaire de bitcoins de son portefeuille à celui du portefeuille *Silkroad*. Il s'agit en quelque sorte d'une caution qui sera contrôlée par un administrateur du site. Le vendeur, informé que l'argent a bien été transféré, pourra envoyer la commande. Une fois le produit reçu, l'acheteur prévient le site qui débloque la somme afin de la transférer sur le portefeuille du vendeur. Ce système est protecteur mais le risque est toujours présent car il faut faire confiance au site qui détient les bitcoins. Or, s'il est rare que les administrateurs volent les utilisateurs, les sites peuvent être les victimes d'hackeurs ou neutralisés par les autorités. En tout état de cause, les possibilités de recours sont restreintes. C'est pourquoi, *Defcon* a proposé un nouveau moyen de paiement, plus sûre encore, appelé « *multi-signature escrow* ». Lorsqu'un achat est accepté par un vendeur, un nouveau portefeuille de stockage bitcoin est créé et le vendeur approuve l'ordre. Quant à l'acheteur, il approuve la transaction après qu'il a reçu le produit. In fine, c'est au site d'approuver ou de décliner. Pour l'instant rien de nouveau. La particularité réside dans le fait que l'argent n'est libéré que lorsque deux des trois protagonistes s'enregistrent avec leurs clés de chiffrement si bien qu'aucune personne ne peut s'envoler seule avec les bitcoins. Dès lors, les utilisateurs avertis n'utilisent que les sites proposant ce nouveau moyen de paiement.

L'anonymat des bitcoins n'est pas total. Cette cryptomonnaie nécessite un enregistrement de toutes les opérations effectuées entre les utilisateurs sur un registre appelé *blockhain*. Donc, lorsqu'un utilisateur envoie ses bitcoins de son compte à son portefeuille *Silkroad*, il y a un enregistrement sur la *blockhain*. Certes, personne ne sait à qui ce portefeuille bitcoin appartient si bien que la vie privée n'est pas affectée. Néanmoins, les utilisateurs utilisent leur compte

[395] Ce terme dérive de l'ancien français. Une escroue était un parchemin portant reconnaissance d'une obligation.
[396] Texte original : « *Always use the escrow system ! This can't be stressed enough. 99 per cent of scams are people who set up fake vendor accounts and ask buyers to pay them directly or release payment before their order arrives* ».

bancaire de sorte qu'ils puissent être identifiables si des recherches approfondies venaient à être effectuées. Les développeurs ont dont créé une nouvelle astuce utilisant des comptes écrans : le *« trumbling service*[397] ». Les bitcoins sont envoyés sur un compte central où plusieurs utilisateurs vont mettre leurs bitcoins. Il s'agit d'un lavage à petite échelle. En effet, lors d'un achat, l'argent émane du compte central et non du portefeuille de l'acheteur. Ce système est payant mais les frais sont très bas[398].

La réception du produit est l'une des étapes les plus délicates pour les acheteurs. Ces derniers transmettent une adresse cryptée que seul le vendeur sera en mesure de lire. Toutefois, lors de la réception du colis, ils ne sont plus anonymes et deviennent vulnérables. La majorité des acheteurs utilisent leur vraie adresse et se reposent sur les méthodes furtives du vendeur. Mais, certains utilisent une adresse de dépôt : une maison abandonnée disposant d'une boîte aux lettres fonctionnelle par exemple. Le produit sera envoyé dans une enveloppe ordinaire et rembourrée avec du papier à bulles, un envoi qui ressemble à n'importe quel autre envoi et qui n'attire donc pas l'attention. La poste ne représente pas un danger pour les acheteurs puisqu'elle a un mandat qui la contraint à transporter toute lettre et colis qui lui sont confiés et n'est pas autorisée à ouvrir ce qu'elle transporte. La responsabilité du contenu de l'envoi revient à l'expéditeur. Afin de minimiser les risques, les acheteurs français effectuent leurs achats sur les cryptomarchés français en vue d'éviter les douanes qui peuvent intercepter les colis.

En somme, le processus d'achat habituel commence par la création d'un compte sur la plateforme de vente souhaitée en utilisant une adresse mail anonyme. Ensuite, l'étape suivante est l'anonymisation des bitcoins via un *Bitcoin mix*er. Lorsque cette étape est accomplie, le client peut passer la commande et en échanger directement avec le vendeur par le biais d'une messagerie chiffrée anonyme. A la suite de cette étape, le client approvisionne son compte bitcoins auprès d'un service *escrow* et effectue l'achat auprès du vendeur. Ce dernier se charge d'envoyer le colis via les services postaux classiques en prenant soin de le confiner afin que l'envoie paraisse anodin. Une fois le colis reçu, le client débloque les fonds auprès de l'e*scrow* et évalue le vendeur sur le site.

L'achat de drogue sur *Silkroad* a introduit une nouvelle dynamique : le client est roi. En effet,

[397] Les mixeurs.
[398] 1 à 5% des transactions et jusqu'à 7% en France.

pour faire face à la concurrence, les dealers sont très attentifs, proposent des offres promotionnelles, envoient des petits extras, les produits sont de qualité et les prix très attractifs. Les acheteurs mécontents peuvent s'exprimer grâce aux commentaires et sélectionner les meilleurs dealers. De plus, le système est très sécurisé et offre énormément de garanties : les mixeurs et les *escrow* ont déjà été évoqués. Ce nouveau marché signe la fin du monopole local des cartels. En 2016, l'Observatoire européen des drogues et des toxicomanies a publié un rapport mettant en avant l'essor des ventes de drogue sur le Darknet[399]. Même constat, en 2017 avec le *Global Drug Survey*[400] qui a rendu son rapport annuel sur la consommation de stupéfiants en interrogeant 120 000 consommateurs répartis dans 50 pays. Ce rapport pointe du doigt l'augmentation des achats de drogue en ligne : 25% des consommateurs anglais, 13% des consommateurs français, 11% des consommateurs belges ou encore 7% des consommateurs canadiens auraient acquis de la drogue via le Darknet durant les douze derniers mois. Ces statistiques concernent *Silkroad* ainsi que les nouveaux marchés (B).

B) Les nouveaux marchés

Le 6 novembre 2014, Eurojust, Europol et le FBI annoncent l'arrestation du créateur de *Silkroad* 2.0. Il s'agit de Blake Benthall, connu sous le pseudonyme *Defcon*. Cette opération a été possible grâce à une infiltration dans le groupe des administrateurs. L'enquête menée par les autorités de cinq pays, dont la France, a donc permis la fermeture de *Silkroad* 2.0 et la condamnation de *Defcon* et ses complices. Le 13 juillet 2017, la version 3.1 de *Silkroad* et la plupart des autres sites similaires ont été fermés lors d'une grosse opération. Le ministère de la Justice Américain, le FBI et les organismes internationaux Eurojust et Europol ont par ailleurs annoncé avoir fermé « *le plus grand marché noir en ligne de l'histoire* [401] » : *AlphaBay*. Selon Andrew McGabe « *AlphaBay était environ 10 fois plus gros que Silkroad* [402] ». « *C'est le plus grand démantèlement de marché noir en ligne de l'histoire* [403] » a déclaré Jeff Sessions, le procureur général des Etats-Unis[404], lors d'une conférence de presse à Washington le 13 juillet 2017. Ce nouveau supermarché de la drogue, accessible via Tor, proposait les mêmes produits

[399] European Monitoring Centre for Drugs end Drug Addiction, *The internet and drug markets*, 11 février 2016.
[400] Disponible à cette adresse : https://www.globaldrugsurvey.com.
[401] Texte original : « *The largest darknet marketplace in history* ».
[402] Texte original : « *AlphaBay was roughly 10 times the size of the Silkroad* ».
[403] Texte original : « *This is the largest darknet marketplace takedown in history* ».
[404] Le procureur général est membre du cabinet du président des Etats-Unis.

que *Silkroad* : drogues, données de cartes de crédit, armes, et autres produits illégaux étaient en vente. Ainsi, de nouveaux marchés ont succédé à *Silkroad* (1), à travers des dizaines de pays dont la France (2).

1. Les successeurs de Silkroad

Lancée en décembre 2014, soit peu de temps après la fermeture de *Silkroad* 2.0, *AlphaBay* devient rapidement le premier marché en ligne du Darknet. Le succès est dû au fait que *AlphaBay* adopte les mêmes méthodes que *Silkroad*. Au cours des 90 premiers jours de fonctionnement il comptabilise déjà 14 000 utilisateurs, en octobre 2015, il en comptabilise plus de 200 000 utilisateurs[405] et lors de sa fermeture en juillet 2017 il en compte plus de 400 000[406]. Avant sa fermeture, le site propose 250 000 listes de stupéfiants ainsi que 100 000 autres produits illégaux. Le 28 mars 2015, le site est controversé à la suite de la mise en vente de comptes « *Uber*[407] » volés : « *Nous avons enquêté et nous n'avons trouvé aucune preuve de violation. Tenté un accès frauduleux ou vendre des comptes est illégal et nous avons informé les autorités de ce rapport. C'est une bonne occasion de rappeler aux gens d'utiliser des noms d'utilisateur et des mots de passe inédits afin d'éviter d'utiliser les mêmes informations d'identification sur plusieurs sites et services*[408] ».
Même chose en octobre 2015 lorsque la société londonienne de télécommunications *TalkTalk*[409] a été hacké et que les donnés volées ont été mises en vente sur *AlphaBay*.

Les entreprises doivent constamment s'adapter face à ces nouveaux marchés comme le souligne DIdo Harding le PDG de *TalkTalk* : « *TalkTalk met constamment à jour ses systèmes afin de s'assurer de leur fiabilité contre la menace cybercriminelle qui évolue rapidement en affectant un nombre croissant d'individus et d'organisations. Nous prenons toute menace relative à la*

[405] CIMPANU C., *Alphabay Dark Web Market Taken Down after Law Enforcement Raids*, 14 juillet 2017. Disponible à cette adresse : https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/, [consulté le 15 juillet 2017].
[406] Soit dix fois plus que la première version de *Silkroad*.
[407] Uber est une entreprise américaine qui met en contact des conducteurs et des utilisateurs pour la réalisation de services de transport.
[408] Texte original : « *We investigated and found no evidence of a breach. Attempting to fraudulently access or sell accounts is illegal and we notified the authorities about this report. This is a good opportunity to remind people to use strong and unique usernames and passwords and to avoid reusing the same credentials across multiple sites and services* ».
[409] BRIAN M., *TalkTalk hacked in significant and sustained cyberattack*, 23 octobre 2015. Disponible à cette adresse : http://www.engadget.com/2015/10/23/talktalk-hacked/.

sécurité des données de nos clients comme extrêmement sérieuse et prenons toutes les mesures nécessaires pour comprendre ce qui s'est passé »[410].Selon le journal britannique « *the Daily Mail*[411] », ce nouveau marché pourrait même être lié à la mafia russe.

En juillet 2017, lorsque le site *AlphaBay* n'est plus opérationnel, les utilisateurs se posent énormément de questions. Sur les forums de discussions, les utilisateurs sont inquiets et s'interrogent sur la raison pour laquelle le site a été fermé. Certains craignent une « *exit scam* » c'est-à-dire une fuite des administrateurs avec l'argent des utilisateurs. D'autres, soupçonnent les autorités en s'étonnant du manque de déclaration de leur part contrairement à la saisie de *Silkroad*. Peut-être, préfèrent-elles garder le silence en vue de poursuivre les investigations. En tout état de cause, cette instance ne devrait pas affecter les affaires sur le Darknet. En effet, ce genre de disparation met la lumière sur le Darkweb si bien que cela amène de nouveaux utilisateurs. Cela entraîne donc une migration des utilisateurs vers les plateformes similaires comme « *Hansa* » par exemple.

Finalement, le site a été fermé par les autorités. C'est une série d'erreurs de sécurité élémentaire qui va entraîner la chute de *AlphaBay*. En effet, Cazes, le créateur présumé du site, a commis la même erreur que DPR en utilisant une vraie adresse mail lors de la création du site. Alexandre Cazes était un informaticien qui séjournait en Thaïlande depuis huit ans. Il a une femme et travaille en tant que programmeur informatique.

Son adresse mail « *pimp_alex_91@hotmail.com* » lui permet de déclarer que son objectif est que son site devienne le plus grand marché sous-terrain d'*eBay* de l'univers mais elle est également utilisée pour son profil *LinkedIn* et son entreprise de réparation d'ordinateur au Canada. Dès lors, les forces de l'ordre n'ont pas rencontré de difficulté pour le repérer. Mai 2017, elles commencent à être de plus en plus actives sur le site. En juin, un mandat international est émis par un tribunal américain pour l'arrestation de Cazes qui se trouve en

[410] Texte original : « *TalkTalk constantly updates its systems to make sure they are as secure as possible against the rapidly evolving threat of cyber crime, impacting an increasing number of individuals and organisations. We take any threat to the security of our customers' data extremely seriously and we are taking all the necessary steps to understand what has happened here* ».
[411] TONKIN S., *TalkTalk customers' bank details stolen in massive online hack are already up for sale at £1.62 a time*, 1er novembre 2015. Disponible à cette adresse : http://www.dailymail.co.uk/news/article-3298943/TalkTalk-customers-bank-details-stolen-massive-online-hack-sale-1-62-time.html, [consulté le 23 décembre 2017].

Thaïlande. Il est soupçonné de trafic de stupéfiants, de faux et usage de faux, de blanchiment d'argent, de trafic d'armes… Le 5 juillet 2017, les forces spéciales de la police canadienne perquisitionnent EBX Technologie, la société canadienne de Cazes ainsi que deux de ses propriétés[412]. Le même jour, il est arrêté par la police thaïlandaise dans sa résidence située à Bangkok grâce au concours du FBI et de la DEA[413]. L'enquête prouve que Cazes n'était vraiment pas prudent, son ordinateur contenait en effet un document non chiffré détaillant l'ensemble de ses actifs mondiaux, et la localisation des serveurs du site. Dès lors, la police thaïlandaise confisque quatre voitures de luxe et trois maisons pour une valeur totale de 400 millions de bahts soit 10 millions d'euros[414]. En outre, les autorités révèlent que le site était hébergé par plusieurs serveurs qui se trouvaient dans différents pays à travers le monde et qu'il disposait de plusieurs centaines de millions de dollars en cryptomonnaie. Ce faisant, cette arrestation a nécessité une collaboration internationale avec les autorités d'une demi-douzaine de pays. Le 12 juillet 2017, alors qu'il est emprisonné en Thaïlande, Cazes est retrouvé mort dans sa cellule, une heure avant son rendez-vous avec le procureur américain pour son extradition vers les Etats-Unis. Le jeune homme de 26 ans se serait suicidé à l'aide d'une serviette. Le 16 juillet 2017, la femme de Cazes est accusée de blanchiment d'argent. À la suite de cette arrestation, les utilisateurs sont inquiets et se demandent si leurs informations sont en danger. Sur le forum de discussion *Reddit*, un utilisateur nommé invest674 poste le message suivant : « *je suppose que beaucoup de personnes risquent d'être identifiées s'ils disposent de l'historique de ces 30 derniers jours* [415]».

Un autre marché important a connu une croissance rapide après son lancement le 14 janvier 2014, il s'agit du site « *Evolution* ». Ce marché est semblable aux autres marchés du Darknet. Ainsi, il interdit la pédopornographie, les services liés aux meurtres, le terrorisme, la prostitution mais autorise le commerce de données de cartes de crédit. Le site devient très populaire, notamment en raison de son professionnalisme mais aussi grâce à son taux de disponibilité. Cependant, tout s'écroule lorsque le site est déconnecté le 18 mars 2015. Les

[412] MONTREAL GAZETTE, *RCMP's Dark web investigation leads to searches in Montreal*, 5 juillet 2017. Disponible à cette adresse : http://montrealgazette.com/news/local-news/rcmps-dark-web-investigation-leads-to-searches-in-montreal-trois-rivieres, [consulté le 24 avril 2018].
[413] Drug Enforcement Administration. Aux Etats-Unis il s'agit d'un service de police fédéral qui lutte contre le trafic de stupéfiants.
[414] Disponible à cette adresse : http://www.bangkokpost.com/news/crime/1285758/.
[415] Texte original : « *I suppose a lot of people would have their info leaked if they have the last 30 days history* ».

administrateurs disparaissent avec les 12 millions de dollars des utilisateurs, il s'agit de la plus grosse « *exit scam* » de l'histoire du Darknet.

Par conséquent, le Darknet offre énormément de possibilités tout en restant un monde instable exposé à de nombreuses attaques. Lorsqu'un marché est démantelé, il est très rapidement remplacé par un nouveau marché encore plus performant. Il existe en effet des centaines de marchés illégaux sur le Darknet. Le site *deepdotweb.com* référence tous les marchés existants. « *The Market list* » propose 155 marchés divisés en plusieurs catégories. Ainsi, les « *TOP MARKETS !* » sont « *Dream market* » et « *The Trade Route* » qui ont respectivement 97,54 et 99,61% de commentaires positifs. En outre, une catégorie est nommée « *Invite / referral only markets* ». Il s'agit des sites fonctionnant par cooptation grâce à un code d'invitation ou un lien de recommandation pour l'inscription. Des marchés comme « *cannabis road* » ou « *black bank bitcoin market* » sont proposés dans cette catégorie. Le premier a été piraté, tandis que le second a fait l'objet d'une « *exit scam* », ce qui conforte l'idée que le Darknet est fondamentalement instable. Une autre catégorie est appelée « *Multisig or Trusted* ». Ce sont les sites les plus fiables ayant déjà fait leurs preuves sur le long terme. Tel est le cas de « *Traderoute* », de « *CGMC – cannabis growers & merchants cooperative* » ou encore de « *wall street market* ». Une troisième catégorie s'intitule « *Escrow markets* » et ne propose que les marchés utilisant les *escrow* : « *Dream Market* » ou « *the Majestic garden* » en font partie. Il est également possible d'avoir à faire directement aux vendeurs sans passer par un marché. En effet, certains vendeurs tels que « *Your drug* » ou « *Qualityking* » opèrent avec leurs propres sites. Les mauvais sites sont également référencés dans la catégorie « *Dead / scam markets links* » dans laquelle se trouvent les marchés *AlphaBay* et *Evolution*. Enfin, une catégorie classe les marchés par pays : « *Markets for specific languages / countries* ». Il y a un marché italien, « *italian Deep Web* », un marché russe « *Hydra* » et également un marché français (2).

2. Le marché français

L'activité commerciale est l'axe majeur du Darknet, elle est très organisée et ne se préoccupe pas des frontières. Les clients sont situés aux Etats-Unis, en Asie, en Europe ou en Australie. Les vendeurs aussi se trouvent un peu partout si bien qu'il est opportun de se demander s'il existe un marché français. La réponse est oui, il existe des sites français mais il y en a peu et ils sont très fermés.

Selon TrendMicro[416], 40 000 utilisateurs composeraient le marché français du Darknet. Ces marchés sont accessibles via Tor avec des liens en onion et référencés sur le site deep.dot.web. À titre d'exemple, le marché « *The French Connection* » qui propose des stupéfiants a fait l'objet de 76 « reviews[417] » et a une note de 3,58/5. Les commentaires des clients sont de toutes sortes. En juillet 2017, l'utilisateur « *Skunky* » a posté le commentaire suivant en attribuant la note de 5 : « *Pour ma part , consommateur depuis des dizaines d'années , les produits opiacés de la FC sont désormais les seuls qui me font de l'effet , toutes les autres cames[418] du net ne me font aucun effet ! Il est clair que la tar[419] de FC est puissante, très puissante avec un effet qui ne dure pas trop longtemps cela me va très bien car même si ce n'est pas de l'héro afghane brune, ben c'est la seule qui me cartonne. En plus, FC fait des reship quand il y a des soucis il suffit d'être honnête avec eux et ils seront honnêtes avec les clients … Continuez comme cela la FC* ».

Toutefois, les avis sur le « *French Connection* » ne sont pas toujours positifs comme le montre le commentaire de « *The body hammer* » qui a attribué la note de 0,5 en août 2016 : « *J'ai fait 2 overdoses plus une fois où j'ai failli tomber dans les pommes. Pourquoi ? Car j'ai testé leur blacktar et leur H3[420], toutes coupées à la fentanyl. C'est seulement après avoir lu les commentaires ici sur deepdotweb et m'être renseigné sur les effets de la fentanyl[421] que j'ai fait le rapprochement et compris ce qu'il m'était arrivé. Certaines personnes sont très sensibles à la fentanyl et moi j'ai très mal réagi au produit. The French Connection est un menteur car jamais il ne dit que ses produits sont coupés à la fentanyl. Consommer leurs produits est TRES DANGEREUX. Ne vous fiez pas à leur cool attitude* ».

Un autre marché français jouit d'une bonne popularité, il s'agit du site « *French Freedom Zone* » dont la moyenne générale est de 3.8 : « *le meilleur market du deep, je vous le conseille ça change des autres où c'est que de la merde. Bon les inscriptions sont payantes c'est dommage mais ça vaut le coup vu la qualité des contacts et des vendeurs qu'on y trouve* » a par

[416] TrendMicro est une société japonaise développant des logiciels de sécurité pour les serveurs.
[417] Critiques.
[418] Drogue.
[419] L'héroïne.
[420] Il s'agit de l'héroïne en poudre.
[421] Il s'agit d'un analgésique très puissant.

exemple posté « *Jondodo* » en septembre 2016.

Les produits proposés sont spécifiques aux marchés français, soit parce que la langue utilisée est le français, soit parce que ces produits ne sont prohibés qu'en France. Ainsi, il est possible de se procurer des armes, du gros calibre au simple couteau en forme de carte bleu. Aussi, sont mise en vente des clés universelles qui ouvrent toutes les boîtes aux lettres, des numéros de permis de conduire qui permettent de récupérer des points, des kits de suicide ou d'euthanasie ou encore des « *ransomwares* [422] ». Ces derniers, conçus en français avec des fautes d'orthographe, réclament des sommes pouvant aller jusqu'à 500 euros. Enfin, des sites de paris illégaux ou des casinos en ligne existent sur les marchés français. Bien évidemment, ces services ne sont pas validés par l'ARJEL[423].

Les vendeurs français sont très méfiants et redoutent réellement les infiltrations policières. Ce faisant, le chiffrement est très utilisé en France, et à l'instar des sites américains, l'inscription sur les forums français ne se fait qu'après recommandation. En outre, pour devenir un membre ayant accès à l'ensemble des fonctionnalités, il faut faire ses preuves sur le long terme et améliorer son score. Beaucoup d'individus se demandent s'il est risqué d'acheter sur le Darknet français. La réponse est mitigée. Même en étant vigilant et en utilisant un mixeur ou un *escrow* tout en se fiant aux avis sur le vendeur, il est possible d'être repéré par les autorités en mission d'infiltration ou de voir disparaître les vendeurs avec son argent sans qu'il y ait de réelle possibilité de plainte.

En août 2017, Gal Vellerius[424], un breton de 39 ans, a été arrêté aux Etats-Unis. Les services de police de la DEA le soupçonnent d'être à la tête d'un grand réseau de trafic de drogue sur le Darknet. Présenté par la presse comme « *le baron du Darknet* », il encourt deux fois vingt ans de réclusion ainsi que 1,5 million de dollars d'amende pour « *conspiration en vue de distribuer des substances contrôlées » et « conspiration en vue de blanchiment d'argent* ». En effet, il est

[422] Un *ransomware* est un logiciel de rançon qui prend en otage les données personnelles de l'utilisateur. Les hackers utilisent aussi les *Remote Acesss tool*, des outils d'administration à distance qui permettent la prise de contrôle à distance de l'ordinateur.
[423] L'autorité de régulation des jeux en ligne.
[424] LE MONDE, Gal Vallerius, *Le barbu du dark web, plaide coupable de trafic de stupéfiants*, 12 juin 2018. Disponible à cette adresse : https://www.lemonde.fr/pixels/article/2018/06/12/gal-vallerius-le-barbu-du-dark-web-plaide-coupable-de-trafic-de-stupefiants_5313737_4408996.html, [consulté le 1er septembre 2018].

accusé d'être « *Oxymonster* », un vendeur et modérateur du site *Dream Market*. La sentence est tombée en octobre 2018 et Oxymonster a été condamné à vingt ans de prison.

A une échelle plus locale, à Lille, une mère de famille de 28 ans[425] a été arrêtée en juin 2018. Elle est suspectée d'avoir été à la tête de « *Black Hand*[426] », une plateforme illégale du Darknet qui proposait depuis 2016 de nombreux services et produits illicites tels que des stupéfiants ou des données de cartes bancaires volées[427]. L'intéressée n'est pas la créatrice du forum qu'elle aurait simplement géré. Selon le responsable de l'opération menée par la DNRED[428], son chiffre d'affaires est estimé « *à plusieurs dizaine de milliers d'euros par an*[429] » grâce à des inscriptions payantes[430] et à des *escrow* qui lui permettaient de percevoir entre 2 et 5% de commission.

Dans l'Oise une affaire concerne cette fois la pédopornographie. Un homme de 47 ans a été arrêté après un signalement auprès des agents du FBI et de la police australienne. Le quadragénaire a ensuite fait l'objet d'une surveillance par ces services qui l'ont localisé en France et transmis son dossier à Europol puis à la police judiciaire française. Des mois d'enquêtes ont permis de mettre en cause l'individu « impliqué dans un important réseau de pédopornographie qui sévit sur le Darknet, cette partie d'Internet où l'on peut trouver de tout ». Pour Florent Boura, procureur de la République de Beauvais, des éléments d'enquête « laissent à penser qu'il était non seulement détenteur d'images pédopornographique, mais surtout qu'il ferait partie des administrateurs de plusieurs sites de ce style[431] ».

Les opérations comme celle de Lille ou de l'Oise sont très rares en France. Une quarantaine d'agents de la DNRED, des experts techniques et des maîtres-chiens ont été appelés pour la

[425] 20minutes, *Lille : Une maman sans histoires à la tête d'une plateforme illégale sur le darknet*, 18 juin 2018.
[426] La « *main noire* ».
[427] 20 minutes, Darkweb, le démantèlement plus important, 18 juin 2018. Disponible à cette adresse : https://www.20minutes.fr/societe/2290903-20180616-dark-web-demantelement-plus-importants-forums-illegaux-France, [consulté le 1er septembre 2018].
[428] La Direction nationale du renseignement et des enquêtes douanières ;
[429] Ibid.
[430] Entre 25 et 50 euros.
[431] GAUTRONNEAU V., et DÉCUGIS J-M., Repéré par le FBI, il gérait des sites de pornographie infantile depuis l'Oise, 16 octobre 2018. Disponible à cette adresse : http://www.leparisien.fr/oise-60/oise-un-pedopornographe-interpelle-avec-l-aide-du-fbi-16-10-2018-7920762.php#xtor=AD-1481423552#xtor=AD-1481423551, [consulté le 17 octobre 2018].

mener à bien. Elle a ensuite été confiée à l'OCLCTIC qui est un bureau spécialisé en la matière. Toutefois, peu d'agents travaillent sur l'Internet sombre qui est pourtant un vrai repaire de criminels (§2).

§2) Le Darknet, un repaire de criminels

L'émergence du Darknet a eu des conséquences néfastes et a contribué à l'extension de la cybercriminalité dont les statistiques [432] battent désormais tous les records [433]. Ce net underground qui échapperait à la police aurait changé la face du crime. A l'instar de l'Internet classique, le Darknet connaît deux types de cybercriminalité. La première concerne les infractions de droit commun qui sont facilitées grâce à l'utilisation d'un réseau. Ces infractions existent donc en dehors d'Internet. C'est le cas notamment de l'escroquerie, du terrorisme ou de la pédophilie qui sont entrés dans une nouvelle dimension grâce à Internet et au Darknet. Sur ces réseaux, un pédophile peut être « *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*[434] », il s'agit de la corruption de mineur. Mais, il peut surtout s'agir de pédopornographie, de la pornographie utilisant des enfants. Un pédophile de ce genre possède et partage des photos de mineurs en profitant d'un anonymat. La seconde concerne un nouveau type d'infractions, spécifique à Internet, car elle n'existe pas en dehors du réseau. Elle concerne le piratage informatique et peut consister à une intrusion non autorisée dans un système informatique ou à son sabotage. En effet, sur le Darknet, le *hacking* est devenu un marché lucratif et les sites vendant les services de cybermercenaires se sont multipliés. Il convient alors de traiter les infractions de droit commun qui sont facilités par le Darknet (A) et les infractions qui n'existent que sur Internet et le Darknet (B).

A) Les infractions de droit commun facilitées par le Darknet

Le Darknet est juste un moyen comme un autre de commettre des infractions. Le wiki caché du Darknet propose énormément de drogues : cocaïne, méthamphétamine en cristaux, de la marihuana mais ce n'est pas tout, des armes y sont également en vente. Un utilisateur peut

[432] Disponible à cette adresse : https://www.interpol.int/Crime-areas/Cybercrime/The-threats.
[433] Disponible à cette adresse : https://www.interpol.int/News-and-media/News/2018/N2018-022.
[434] Code pénal Art. 227-22.

obtenir une arme par la poste contre 1500 euros. La vente de contrefaçon de billets existe aussi sur le Darknet. Les billets sont d'excellente qualité et toutes les marques de sécurité sont incluses[435]. Et la liste s'allonge puisqu'il est en plus possible d'y trouver des tueurs à gage et même des offres de dizaines de milliers d'euros pour éliminer des hommes politiques. Par exemple, aux Etats-Unis, le site « *Craiglist*[436] » aurait mis en relation des tueurs à gage et des instigateurs. Il existerait des organisations mafieuses ou militaires proposant des services variés en fonction des tâches proposées : 8500 dollars pour un individu lambda aux USA, 10 000 dollars pour un européen, 17 000 dollars pour un petit homme d'affaire, 42 000 dollars pour un policier, 80 000 dollars pour une petite personnalité politique et 750 000 pour une grande personnalité[437]. En outre, il y aurait des offres plus précises permettant de choisir les modalités de l'assassinat. Ces sites offrent deux possibilités. La première, qui se nomme l'*unfriendly Solution,* permet de trouver quelqu'un qui se chargera de l'assassinat contre le paiement de la somme. Le site *BesaMafia* qui proposait ce genre de service a été dénoncé comme étant une arnaque. La seconde, qui est proposée sur les *prediction market*[438]*,* permet de miser sur la date de mort de personnalités. Un assassin peut participer au jeu et recevoir une récompense s'il décide de passer à l'acte pour gagner le pari. Les instigateurs peuvent évidemment être poursuivis pour complicité d'assassinat lorsque l'infraction est tentée ou consommée. En France, la législation permet même de poursuivre l'instigation non suivie d'effet grâce à l'article 221-5-1 du code pénal qui dispose que « *le fait de faire à une personne des offres ou des promesses ou de lui proposer des dons, présents ou avantages quelconques afin qu'elle commette un assassinat ou un empoisonnement est puni, lorsque ce crime n'a été ni commis ni tenté, de dix ans d'emprisonnement et de 150 000 euros d'amende* ». Les sites de tueurs à gage existent bel et bien sur le Darknet, toutefois, certains se demandent s'il s'agit d'un réel service ou d'une légende permettant de mettre en place des arnaques appelée *scam.* Ainsi, les drogues et les armes ne sont que la surface du Darknet ; il existe de nombreux groupes et forums communautaires qui visent à satisfaire les désirs les plus sombres de l'humanité : les néo-nazis,

[435] MOORE D., RID T., *Cryptopolitik and the Darknet*, Survival : Global Politics and strategy, International Institute for Strategic Studies, volume 58, 2016.
[436] FARREL P., *Inside the darknet : where Australians buy and sell illegal goods*, 4 juillet 2017. Disponible à cette adresse : https://www.theguardian.com/technology/2017/jul/04/inside-the-darknet-where-australians-buy-and-sell-illegal-goods, [consulté le 5 juillet 2017].
[437] Y4N4UDEL, *Tueurs à gages sur le Deep Web : mythe ou réalité ?* 21 mars 2014. Disponible à cette adresse :https://www.undernews.fr/undernews/tueurs-a-gages-sur-le-deep-web-mythe-ou-realite.html, [consulté le 4 mars 2015].
[438] Disponible à cette adresse : https://en.wikipedia.org/wiki/Assassination_market.

les tortionnaires d'animaux, les sites cannibales[439], les terroristes et les pédophiles y ont fait leur place. Ces derniers types de criminalité, pédophilie (1) et terrorisme (2) ont rapidement migré du web visible au Darknet qui leur assure un anonymat.

1. La pédopornographie du Darknet

Même si la pédopornographie existe sur le Darknet, il n'est pas possible de tomber dessus par hasard. Idem pour la nécrophilie[440], la zoophilie[441] et les snuff movies qui mettent en scène le meurtre, la torture ou le viol d'une ou plusieurs personnes. La victime est censée être une vraie personne et non un acteur. Même chose pour les « *redroom* » en direct qui permettent d'interagir avec le bourreau pour lui suggérer des choses. Il est possible de citer Luka Rocco Magnotta[442] qui a filmé, monté et diffusé une vidéo sur le site *bestgore*[443]. Il est présenté comme l'un des premiers tueurs d'Internet. Concernant les pédophiles, ils cherchent l'anonymat et utilisent donc le Darknet qui ne leur était évidemment pas destiné. Néanmoins, selon une étude effectuée à l'Université de *Portsmouth*[444], même si 80% des recherches sur Tor ont un lien avec la pédophilie, ces sites ne représenteraient qu'une infime partie du Web accessible via Tor à tel point qu'il ne faut pas confondre intention et moyen.

L'interdiction de la pédopornographie est un phénomène récent. Durant la révolution sexuelle des années soixante et soixante-dix, la pédopornographie était ouvertement proposée à la vente dans certains États américains. À la fin des années soixante-dix, de nombreux gouvernements ont commencé à adopter une législation plus sévère pour l'éradiquer et, à la fin des années 1980, la pornographie enfantine est devenue très difficile à trouver. Le magazine de pornographie infantile le plus vendu en Amérique du Nord était distribué par une poignée de magasins aux petits réseaux de collecteurs dédiés. Au Royaume-Uni, de nombreux pédophiles traversaient l'Océan Atlantique afin de faire de la contrebande. Les services américains considéraient le problème comme plus ou moins sous contrôle. En 1983, le bureau de la comptabilité générale

[439] Le « *cannibal café* ».
[440] L'attirance sexuelle pour les cadavres.
[441] L'attirance sexuelle pour les animaux.
[442] Disponible à cette adresse : https://fr.wikipedia.org/wiki/Luka_Rocco_Magnotta.
[443] Disponible à cette adresse : https://rationalwiki.org/wiki/Red_room.
[444] GREENBERG A., *Over 80 percent of darkweb visits relate to pedophilia, study finds*, 30 décembre 2014. Disponible à cette adresse : https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/, [consulté le 2 avril 2015].

des États-Unis a déclaré une baisse de la pornographie infantile commerciale et le service des douanes des Etats-Unis n'a pas considéré la pornographie des enfants comme une priorité. Mais, l'arrivée d'Internet a tout bouleversé. En 1990, la « *société nationale pour la prévention de la cruauté envers les enfants*[445] », une organisation britannique de protection des enfants, a estimé qu'il y avait 7000 personnes avec des images de pornographie juvénile en leur possession. Au début des années quatre-vingt-dix, les évolutions numériques ont facilité les échanges de contenu pornographique. A titre d'exemple, en 1993, une opération policière a visé deux sites qui offraient un accès payant à des centaines d'images illégales. Les adresses mails anonymes - « *@binaries. pictures. erotica . Pre-teen* » et « *alt. binaries. pictures . erotica . Schoolgirls* » -ont été utilisées pour partager de la pornographie juvénile à la fin des années 90. En 1996, les membres d'un réseau d'abus d'enfants appelés « *Orchild Club* » commettaient et partageaient des abus en direct à l'aide de webcam connectées directement aux ordinateurs de plusieurs pays. Deux ans plus tard, la police découvre « *the Wonderland club* », un réseau Internet d'échange d'images pédopornographiques. Ses adhérents, qui se trouvaient dans une trentaine de pays différents, utilisaient un puissant logiciel de cryptage pour échanger en secret des images pédopornographiques. Les membres potentiels devaient être présentés par des membres de confiance du réseau et posséder au moins 10 000 images pédopornographiques pour s'y joindre. Lorsque le site a été découvert, la police a trouvé 750 000 images et 1800 vidéos pédopornographiques. En 2001, sept Britanniques ont été condamnés pour leur implication dans le réseau. Avec l'accès à Internet dans de nouveaux pays, les centres de production d'images pédopornographiques se sont multipliés. L'horrible site « *Lolita City* » hébergé en Ukraine, a fourni le Web avec un demi-million d'images pédophiles au début des années 2000, avant sa fermeture en 2004. En 2007, la base de données d'images pédopornographiques d'Interpol, composée d'images saisies par la police, contenait environ un demi-million d'images. En 2010, la base de données de la police Britannique, détenue par le CEOP[446], était composée de plus de 850 000 images pédopornographiques. En 2011, les autorités américaines ont transmis vingt-deux millions d'images et vidéos pédopornographiques au Centre international pour enfants disparus et sexuellement exploités (ICMEC). Selon les estimations de la NSPCC[447], il existe aujourd'hui d'énormes volumes de

[445] National Society for the Prevention of Cruelty to Children (NSPCC).
[446] *CEOP : Child Exploitation & Online Protection Centre*. Ce centre lutte au Royaume-Uni contre les abus sexuels sur les enfants.
[447] *National Society for the Prevention of Cruelty to Children* (Société nationale pour la prévention de la cruauté envers les enfants).

pédopornographie en ligne, facilement accessibles et efficacement distribués. Entre 2006 et 2009, le département de la justice des États-Unis a enregistré 20 millions d'adresses IP informatiques uniques qui partageaient des fichiers de ce genre à l'aide de logiciels de partage P2P. Le CEOP avance des chiffres accablants : au Royaume-Uni, il y aurait plus de 50 000 pédophiles partageant ou regardant des images indécentes d'enfants. Les pirates informatiques qui ont pris le contrôle du wiki caché pendant trois jours en mars 2014 avancent d'autres chiffres impressionnants ; entre le 20 juillet et le 27 août 2013, sur les treize millions de page visionnées sur les services cachés, 600 000 étaient des visites de pages pédopornographiques. Avec de tels chiffres, il est difficile d'établir un profil type du consommateur de pédopornographie. Mais, il existe des tendances générales qui permettent d'affirmer que pour la plupart, il s'agit d'hommes souvent bien éduqués, venant de tous les horizons de la vie. En outre, ces délinquants n'ont pas tous le même rôle. Il y a le pédophile qui ne fait que visionner les images, il y a le collectionneur qui possède énormément d'images et il y a les producteurs qui créent eux-mêmes les images avant de les diffuser. Tous ces délinquants n'ont pas attendu l'avènement d'Internet pour agir, ils en ont juste profité pour faciliter leurs échanges.

Lorsque l'*IWF*[448] a été fondée en 1996, son travail était ciblé sur une centaine de groupes de discussion illégaux. En 2006, ce nombre est passé à plus de 10 000 et à 13 000 en 2013. La fondation et la police sont souvent confrontées à de nouveaux défis. En 2013, la fondation a commencé à recevoir des douzaines de plaintes au sujet d'un site web, mais chaque fois que l'URL était vérifié, ils tombaient sur un site de bricolage. Après un travail approfondi, un ingénieur de la fondation a découvert une sorte de jeu de piste ; l'accès au site se faisait en consultant certains sites dans un ordre précis. Lorsque cet ordre est respecté, un logiciel envoie une version cachée du même site mais avec du contenu pédopornographique. Ce sont les *« disguised cookie site »*. Malgré ces difficultés, leurs opérations sont très fructueuses. En 2013, il n'y en avait plus que 1660. Ils ont été particulièrement efficaces pour fermer les sites basés au Royaume-Uni. Les analystes de l'*IWF* ont récolté plus de sept mille sites contenant des scènes de torture et de viol, souvent sur des mineurs de dix ans. Comment peuvent-ils maintenir leur santé mentale dans de telles circonstances ? Tout le personnel est soumis à un examen psychologique annuel rigoureux. Ils sont encouragés à faire des pauses le plus souvent possible et à partir tôt. Il s'agit de séparer vie privée et professionnelle. Les opérations

[448] *IWF* pour *Internet Watch Foundation*. Elle est chargée de récolter les contenus d'abus sexuels sur enfant mais aussi les contenus de crimes obscènes sur adulte.

effectuées par l'*IWF* le sont majoritairement sur le web visible, contre des sites habituellement hébergés dans des pays où la pédopornographie reste impunie.

De nos jours, une image peut être créée dans un premier pays, stockée sur un serveur ou un site dans un deuxième pays, et être consultée dans un troisième pays. Les compétences juridictionnelles deviennent un casse-tête, surtout lorsque le contenu est hébergé dans un pays qui semble moins préoccupé par ce fléau. Environ un quart des sites porté à la connaissance de l'*IWF* provient de sites commerciaux qui nécessitent un paiement par carte de crédit pour l'accès au contenu. L'*IWF* ne s'intéresse pas au contenu pédopornographique proposé sur le Darknet. Probablement parce qu'il y a peu de dénonciations le concernant. De plus, sur ce dernier les difficultés sont encore plus nombreuses : le fonctionnement de Tor complique l'identification des délinquants en raison d'une distribution de contenu reposant sur un réseau anonyme et décentralisé. Dès qu'un service caché est retiré, la communauté en créé un autre. A titre d'exemple, bien qu'il soit généralement en faveur de la libre expression en ligne, le collectif Anonymous s'oppose fermement à la pédopornographie. Il a réussi à localiser le serveur où certains de ces sites[449] étaient hébergés afin de les mettre hors ligne : c'est « *l'Opération Darknet*[450] ». Toutefois, il n'aura fallu que quelques jours pour que la plupart de ces sites soient remis en ligne grâce à de nouveaux serveurs et avec encore plus de visiteurs. En 2012, un réseau d'exploitation abuse d'enfants et partage des images sur le site hébergeant 2000 vidéos. En juin 2013, « *Lolita City* » est passé à 15 000 membres et propose plus d'un million de photos illégales. En août 2013, à la suite d'une longue enquête, le FBI arrête Eric Eoin Marques, un homme de 28 ans, soupçonné d'avoir organisé l'hébergement de plusieurs des sites les plus visités pour le piratage, le blanchiment d'argent mais aussi pour la pédopornographie. Après ce démantèlement, les principaux sites pédopornographiques n'ont pas disparu. En effet, en février 2015, le FBI met la main sur un site pédopornographique[451] mais au lieu de le désactiver, il décide de l'héberger sur ses propres serveurs pendant deux semaines[452]. Enfin, en septembre

[449] Dont Lolita City.
[450] Disponible à cette adresse : http://knowyourmeme.com/memes/events/operation-darknet, [consulté le 30 avril 2015]. KIM B., *Operation Darknet*, 2012.
[451] ELODIE, *Le FBI pirate le Deep Web pour débusquer des pédophiles*, 8 janvier 2016. Disponible à cette adresse : http://www.journaldugeek.com/2016/01/08/fbi-pirate-deep-web-pedophiles, [consulté le 8 janvier 2016].
[452] MOREIRA E., *Comment le FBI traque les pédophiles sur le dark web*, 30 janvier 2016. Disponible à cette adresse : https://www.lesechos.fr/30/01/2016/lesechos.fr/021642681509_comment-le-fbi-traque-les-pedophiles-sur-le-dark-web.htm, [consulté le 7 février 2016].

2017, le plus gros site pédopornographique du Darknet est fermé par la police australienne qui a réussi à l'infiltrer et à l'administrer[453].

Les liens entre ces abus virtuels et les abus commis dans le monde réel sont incertains. Pour certains hommes, le visionnage de pédopornographie peut les tenter à agir dans le monde réel. Pour d'autres, l'intérêt sexuel pour les enfants reste un fantasme. Nombreux sont ceux qui disent qu'ils ne passeront jamais à l'acte pour des raisons éthiques et morales. Le visionnement de ce genre de contenu serait une sorte d'échappatoire qui les empêcherait de passer aux abus dans le monde réel. En France, l'article 227-23 du Code pénal dispose que « *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 est puni 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* ».

De plus, « *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* ». L'article 6-I- 7 alinéa 3 de la loi dite LCEN renvoie à cette infraction : « *compte tenu de l'intérêt général attaché […] à la pornographie enfantine, […] les personnes mentionnées ci-dessus*[454] *doivent concourir à la lutte contre la diffusion des infractions visées […] aux articles […] 227-23 et 227-24 et 421-2-5 du Code pénal* ». Le législateur assimile donc la lutte contre la pédopornographie à une mission d'intérêt général. Selon le même article, les hébergeurs et fournisseurs d'accès internet « *doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes*

[453] LE MONDE, *Comment la police australienne a infiltré et administré un site pédopornographique*, 19 octobre 2017.
Disponible à cette adresse : http://www.lemonde.fr/pixels/article/2017/10/09/comment-la-police-australienne-a-infiltre-et-administre-un-site-pedopornographique_5198556_4408996.html, [consulté le 20 octobre 2017].
[454] Les hébergeurs et fournisseurs d'accès Internet.

de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites ».

L'anonymat est limité par la nécessaire collaboration entre les autorités publiques et les hébergeurs et fournisseurs d'accès Internet qui est donc justifiée par une mission d'intérêt général. Une telle mesure a également vocation à s'appliquer pour un autre fléau de la société, le terrorisme (2).

2. Le terrorisme facilité par le Darknet

Le cyberterrorisme est considéré comme un acte terrorisme commis via Internet. En effet, l'émergence des nouveaux moyens de communication tels que Internet, a permis au terrorisme de s'adapter. Internet et le Darknet sont des moyens de diffusion de messages et contenus tellement importants qu'ils font désormais office de média. Le Darknet permet également aux terroristes de communiquer entre eux pour leur organisation internet et de recruter de nouveaux partisans. Tor et Telegram sont des services qui leur permettent de recruter et de diffuser leur message.

Dès lors, les terroristes utilisent le Darknet comme outil de communication efficace, pour y faire de la propagande et du renseignement, pour recruter, former, entraîner, récolter des fonds, transférer des fonds, rechercher des cibles, organiser, planifier des opérations et communiquer (a). Mais le Darknet démultiplie également les capacités criminelles et terroristes des individus, sans qu'ils ne soient forcément des as en informatique. Par exemple, ils utilisent Google Earth pour identifier les cibles sans se déplacer, des tutoriels sur Internet pour fabriquer des bombes ou même attaquer en utilisant le Darknet comme une arme (b).

a) Le Darknet, un dispositif de correspondance pour les terroristes

La communication entre terroristes est très délicate pour eux. En effet, les échanges d'informations doivent être sécurisés pour éviter une interception par les autorités. L'architecture du Darknet garantit une telle sécurité grâce à l'anonymisation et au chiffrement

des échanges et complique la tâche des enquêteurs. Dans plusieurs exemples[455], les services de renseignements français ont montré que des membres de Daesh[456] échangeaient par le biais de messages chiffrés grâce à la mise en place d'une « *cellule d'assistance informatique* » accessible 24h/24. Ces « *cyberdjihadistes* » se fournissent des conseils pour crypter leurs échanges sur Internet afin d'éviter les écoutes des renseignements américains et européens. Les systèmes mis en place sont de plus en plus perfectionnés et le sont par des terroristes compétents et diplômés. François Paget, secrétaire adjoint du Clusif[457], précise qu'il « *faut être clair, à partir du moment où le cryptage est réalisé correctement de bout en bout, il n'y a pas de parade. Même avec les super-ordinateurs que les uns ou les autres peuvent avoir, on est aujourd'hui sur des logiciels qui utilisent des cryptages importants et le décryptage de ces messages s'avère impossible* ». Les terroristes peuvent également utiliser la méthode de la « *boîte aux lettres morte virtuelle*[458] » qui leur permet d'échanger secrètement du contenu sans avoir à se rencontrer. Il leur suffit de créer une adresse mail quelconque, de laisser un message dans les brouillons sans l'envoyer et de donner aux membres le nom d'utilisateur ainsi que le mot de passe dans un message chiffré. Mais au delà de cet aspect relatif à la correspondance, le Darknet peut être utilisé comme arme (b).

b) Le Darknet, une arme pour les terroristes

D'après les experts du séminaire sur la cybercriminalité du 31 janvier 2013, « *la cybercriminalité qui a pris des proportions phénoménales est devenue aujourd'hui un terrorisme informatique*[459] ». En effet, le terrorisme actuel a évolué en alliant les méthodes violentes du 20ème siècle aux réalités numériques du 21ème siècle. Certains parlent même de « *cyberattentats* ».

[455] BFM TV, *Une hotline de Daesh pour apprendre à crypter ses messages*, 18 janvier 2016. Disponible à cette l'URL du site de BFM : https://www.bfmtv.com/societe/une-hotline-de-daesh-pour-apprendre-a-crypter-ses-messages-944354.html, [consulté le 9 janvier 2016].
[456] L'acronyme en arabe de l'Etat Islamique, une organisation terroriste.
[457] Club de la sécurité de l'information français.
[458] https://fr.wikipedia.org/wiki/Boîte_aux_lettres_morte.
[459] LECONEWS, *La cybercriminalité est devenue un terrorisme, 31 janvier 2013*. Disponible à cette adresse : http://www.leconews.com/fr/depeches/la-cybercriminalite-est-devenue-un-terrorisme-31-01-2013-161958_312.php, [consulté le 5 mai 2015].

L'exemple du « *défaçage ou défacement*[460] » d'une centaine de sites Internet français à la suite de l'attentat contre Charlie Hebdo[461] prouve que le terrorisme a aussi des conséquences sur Internet. Des hackeurs de Daesh ont pris le contrôle de sites web pour y mettre un fond noir en page d'accueil et des messages comme « *Death to France*[462] » ou « *Death to Charlie*[463] ». Selon, Thierry Karsenti, directeur technique Europe d'une entreprise de sécurité informatique, « *on peut parler de cyberjihad, et le défacement n'est que la partie émergée de l'iceberg et la moins dangereuse aussi, car elle n'a pas d'autres conséquences que l'affichage d'une idéologie (...) en parlant de terrorisme, on a peut-être oublié de parler de cyberterrorisme, et d'actions qui peuvent être bien plus graves et déstabilisantes que du défacement si elles s'en prennent aux infrastructures de communication et de transport d'un Etat. Ce qui est le plus à redouter, c'est la coordination d'attaques de terrorisme et de cyberterrorisme, menées de front* ».

Ce genre d'attaque pourrait avoir des conséquences financières considérables pour les citoyens et les entreprises. En effet, les systèmes informatisés sont très centralisés et touchent à de nombreux domaines comme l'économie, le transport, l'énergie, la santé, la politique si bien qu'ils sont des cibles potentielles pour le cyberterrorisme.

Enfin, à défaut d'être une arme pour les terroristes, le Darknet peut être une aide à la préparation d'un attentat. En effet, sur le Darknet les modes d'emploi pour la fabrication de bombes artisanales sont destinés à toutes les personnes qui pourraient être intéressées et logiquement aux terroristes. En ce sens, l'article 322-6-1 du Code pénal[464] dispose que « *le fait de diffuser par tout moyen, sauf à destination des professionnels, des procédés permettant la fabrication d'engins de destruction élaborés à partir de poudre ou de substances explosives, de matières nucléaires, biologiques ou chimiques, ou à partir de tout autre produit destiné à l'usage*

[460] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 33. « *Le « défaçage » de site Internet consiste à modifier la présentation visuelle d'un site* Web, en le remplaçant, en la modifiant par des images, des slogans, des messages ou des commentaires dégradants.
[461] LEFIGARO, *Charlie Hebdo : des centaines de sites français piratés,* 12 janvier 2015.
Disponible à cette adresse : http://www.lefigaro.fr/culture/2015/01/12/03004-20150112ARTFIG00317--charlie-hebdo-des-centaines-de-sites-francais-pirates.php, [consulté le 13 juillet 2015].
[462] Mort à la France.
[463] Mort à Charlie en référence à Charlie Hebdo.
[464] Instauré par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme et modifié par la loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale qui a aggravé les peines.

domestique, industriel ou agricole, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende ».

En outre, le Darknet permet aux pirates informatiques de s'exprimer pour faire le bien ou pas en profitant d'un meilleur anonymat que sur le web visible (B).

B) Les pirates informatiques du Darknet

Même si le spectre des activités criminelles du Darknet ne se limite pas au « *hacking* », ce dernier est omniprésent sur les réseaux cachés. Dans le monde informatique, le « *hacking* » est défini par le Journal du net[465] comme « *l'activité qui consiste à modifier l'un des éléments d'un logiciel et/ou d'un matériel afin que celui-ci puisse avoir un comportement autre que celui pour lequel il a été conçu. Le terme se rapproche sensiblement du piratage informatique. Il repose majoritairement sur l'activité des hackers qui sont des spécialistes en informatique possédant suffisamment de compétences pour pouvoir dénicher les failles de sécurité d'un logiciel/d'un matériel afin d'en tirer parti* ». Mais, le terme est également entré dans le langage courant puisque le dictionnaire Larousse[466] définit le hackeur comme « *une personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique*[467] ». En raison de ses diverses possibilités, cette activité a réellement évolué dans les années 2000 pour devenir la cible principale des agences de sécurité de police et des agences de renseignements. Les motivations du « *hacking* » peuvent être nombreuses puisqu'un hackeur peut agir pour rechercher de l'argent, pour déstabiliser des personnes physiques ou morales, comme des services publics ou de grandes entreprises ou alors pour relever un défi. Le *hacking* peut même être utilisé comme une arme efficace permettant de mener une guerre psychologique susceptible d'avoir des conséquences concrètes en matière de pertes humaines et matérielles. Les terroristes islamistes utilisent ce genre de technologies et notamment le Darknet pour la préparation d'activités terroristes. Les réseaux cryptés leur offrent un anonymat, des guides pour fabriquer des bombes,

[465] Définition disponible à cette adresse : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203453-hacking-definition-traduction/.
[466] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 32.
[467] Disponible sur le site internet du dictionnaire Larousse : http://www.larousse.fr/dictionnaires/francais/hacker/38812.

s'entraîner à tirer avec des armes à feu[468] et est utilisé pour la diffusion de propagande islamiste. Un réseau comme Tor offre de meilleures garanties que le Web de surface et permet d'effectuer un meilleur recrutement bien moins risqué que sur *Facebook* ou *Twitter*. Toutefois, il existe d'autre type de pirates informatiques agissant sur le Darknet, il convient d'analyser d'une part, les différents types de pirate informatique du Darknet (1) et d'autre part, leurs méthodes pour agir (2).

1. Les différents types de pirates informatiques du Darknet

Les amateurs cyberdélinquants, dont les motivations sont d'ordre social, technique, politique, financier ou étatique, peuvent se reconnaître dans des populations de techniciens animés du désir de maîtriser toujours mieux les technologies. On y trouve des curieux, des immatures, des psychopathes, des mystiques, des rebelles… La motivation sociale trouve fréquemment ses racines dans le besoin de reconnaissance de l'individu par ses pairs, lié généralement à une structure de bande. La motivation financière et l'appât du gain constituent la motivation première des cybercriminels. La motivation technique reste rare, bien qu'elle soit celle de la majorité des « *white hat* » à la recherche des limites de la technologie, pour mieux en comprendre les atouts. La motivation politique consiste à créer un événement propre à alerter les médias pour les focaliser sur un problème grave, en espérant provoquer une prise de conscience collective qui amènera sa résolution. Ainsi la frontière entre l'activisme et le terrorisme reste floue. Enfin, il existe une motivation gouvernementale avec des personnes agissant pour le compte d'organisations étatiques.

Les menaces ne visent pas seulement les équipements, elles visent surtout les informations, à savoir les données personnelles et les transactions elles-mêmes. Elles peuvent être exploitées pour réaliser une action malveillante et avoir par conséquent une valeur marchande. En effet, l'usurpation d'identité sur Internet est plus facile et s'il y a des poursuites judiciaires, l'identification du véritable coupable sera quasiment impossible. Selon Symantec, depuis 2015, les cyberattaques ont créé des dégâts à hauteur de 125 milliards de dollars et le Darknet serait impliqué dans un tiers de celles-ci. A titre d'exemple, en 2016 des sites comme *Spotify*[469],

[468] *HOW to survive in the west : A Mujahid Guide*, 2015. Disponible à cette adresse : https://www.blazingcatfur.ca/wp-content/uploads/2015/04/ISIS-How-to-survive-in-the-west.pdf, [consulté le 3 février 2018].
[469] Spotify est service suédois de streaming musical.

Airbnb[470] ou *eBay* ont été paralysés pendant plusieurs heures ce qui a engendré des millions de pertes[471]. Sur le Darknet, un individu sans vraie connaissance peut acheter ou louer un logiciel malveillant pour identifier la vulnérabilité d'un système, voler une identité, compromettre des serveurs, voler des données afin de causer des dommages importants ou encore mener une attaque informatique ciblée. Pour une centaine d'euros, il est possible d'acheter un kit de piratage complet comprenant un *ransomware*[472], un logiciel permettant d'écouter à distance les appels téléphoniques d'une personne, de lire ses sms, et de déclencher son micro afin d'entendre ce qu'il se passe dans le périmètre d'écoute. Pour cela, il faut accéder au téléphone de la personne et y installer une application. Par ailleurs, également pour une centaine d'euros, il est possible de louer les services d'un hackeur capable d'obtenir le mot de passe *Facebook* d'une personne, bloquer les communications téléphoniques et Internet d'un concurrent ou d'un ennemi et même faire disparaître une personne qui ne sera plus répertoriée nulle part et qui devra effectuer de longues démarches afin de retrouver une identité. Il existe même des cybermercenaires qui fonctionnent comme des entreprises de service avec salariés qui proposent des offres de hack, répondent aux demandent et donnent du travail à ses membres. Pour intégrer ce genre d'organisation il faut faire ses preuves en infiltrant un site et en exposant la méthode. Cela permet de filtrer les débutants et d'éviter les dénonciations puisque tous les membres ont fait quelque chose d'illégale pour joindre la communauté.

Il est courant de classer les cyberdélinquants en deux grandes catégories selon qu'ils sont des professionnels ou non de l'illégalité. Les premiers vivent des activités clandestines rémunératrices, tandis que les seconds sont souvent animés par un fort besoin de reconnaissance sociale. Cette distinction permet de comprendre la majorité de leurs motivations. Quelqu'un qui télécharge de la musique de manière illégale est un cyberdélinquant. Mais les vrais professionnels comparaissent rarement devant les tribunaux. Leur réelle maitrise des technologies ainsi que leur compréhension d'Internet et des méthodes et outils d'investigation policières, leur permettent de laisser peu de trace ou de les masquer. Même dans l'éventualité

[470] Airbnb est une plateforme communautaire payante de location et de réservation de logements de particuliers.
[471] UNTERSINGER M., *Une attaque informatique majeure a paralysée une partie du Web pendant plusieurs heures*, 21 octobre 2016. Disponible à cette adresse : http://www.lemonde.fr/pixels/article/2016/10/21/une-cyber-attaque-massive-perturbe-de-nombreux-sites-internet-aux-etats-unis_5018361_4408996.html, [consulté le 2 novembre 2016].
[472] Un ransomware ou rançongiciel est un logiciel informatique malveillant qui permet de prendre en otage les données en les chiffrant. Une clé de déchiffrage est donnée en échange d'une rançon.

de leur collecte, elles permettent rarement de les identifier avec certitude. Se « *cacher* » sur Internet est toujours possible pour une personne compétente.

Le mot *hacking* trouve son origine dans le vocabulaire de cuisine, signifiant le hachage « *menu-menu* » des aliments. Par extrapolation, il qualifie désormais les activités qui consistent à découper très finement le mode de fonctionnement d'un ordinateur, afin d'en comprendre tous les rouages et éventuellement les détourner. Il subsiste toujours une différence entre le fait de comprendre les limites des protections, de rechercher des failles et celui de les exploiter à des fins malveillantes. La limite peut être ténue ou parfois la tentation est grande. En l'absence d'une typologie formelle des cybercriminels, il faut retenir qu'il existe des individus passionnés d'informatiques qu'il ne faut pas confondre avec des criminels ou des escrocs. Ainsi, les hackeurs sont le plus souvent des véritables experts en informatique, en réseaux et télécommunications ainsi qu'en sécurité informatique et en cryptographie. La motivation qui les anime, pas toujours louable, peut varier en fonction de leur milieu socioculturel ou socioprofessionnel. Selon leur éthique et l'usage qu'ils font de leur connaissance au service ou non de la société, il est courant de qualifier les hackeurs par la couleur d'un chapeau, en référence au chapeau que portaient traditionnellement les détectives privés. Bien qu'il est rare que les hackeurs s'identifient entre eux de cette manière, le chapeau blanc de l'anglais « *white hat* » est associé aux « *gentils* », c'est-à-dire à ceux qui œuvrent pour une meilleure sécurité, alors que le chapeau noir ou « *black hat* » réservé aux méchants et le gris à ceux qui, en fonction des circonstances, sont tantôt blancs, tantôt noirs. Par extension, il existe des chapeaux bleus ou blue hat, personnes spécialisées dans le hacking de Windows et des chapeaux rouges ou red hat, pour les spécialistes d'UNIX. Il n'est pas rare que que les agences gouvernementales, comme les organisations privées fassent appel à des hackeurs blancs ou gris, voire noirs, pour toutes sortes d'opérations comme de la surveillance, de l'espionnage, du renseignement, de la recherche de personnes, de la manipulation d'informations, des enquêtes, de la filature, etc.

Du fait de leur passion pour l'informatique et Internet, certains hackeurs sont parfois qualifiés de geeks. Ils se distinguent des *script kiddi*es qui sont des jeunes pirates informatiques néophytes et qui peuvent être également identifiés de manière péjorative comme étant des « *nerds* ». Ils sont certes passionnés d'informatiques, mais ont des connaissances relativement limitées, notamment en programmation.

Ensuite, les *crackers*, spécialistes du craquage de protections sécuritaires, sont majoritairement des professionnels[473]. Entrent dans cette catégorie notamment des concurrents directs de l'entreprise visée, des fonctionnaires, des mercenaires pouvant agir aussi bien pour le compte d'institutions privées que publiques, des truands de toutes sortes, des terroristes, des activistes qui utilisent le *hacking* comme technique et moyen de protestation, etc. Il convient de distinguer le hackeur (a) des autres types de pirates informatiques (b).

a) Le hackeur

Le terme « *hackeur* » provient de l'anglais « *to hack into* » signifiant « *entrer par effraction* »[474]. Il en existe plusieurs sortes classées en fonction de leurs objectifs. Tout d'abord, il y a les « *white hat* » qui sont des professionnels de la sécurité informatique ayant de bonnes intentions. Ils testent les réseaux afin d'avertir les utilisateurs des différentes vulnérabilités existantes et suggèrent même des corrections. En France, la loi LCEN de 2004 a introduit l'article 323-3-1 du code pénal qui dispose que « *le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

Ainsi, la divulgation publique sur Internet des vulnérabilités ainsi que la possession d'outils utilisés pour le « *hacking* » sont interdites. Ensuite, il y a les « *black hat* » qui sont des cybermercenaires, des cybers escrocs, des cybers terroristes ou des cybers espions. Ils agissent afin de nuire ou de faire de l'argent. Sur le Darknet, les *hackeurs* ont mis en place divers marchés très lucratifs. Il est possible de citer « *TheRealDealMarket* » qui a ouvert en 2015 afin de commercialiser des *Odays*, des failles sécuritaires nécessitant un correctif. De deux choses l'une, soit ils vendent le correctif à l'auteur du logiciel qui pourra supprimer la faille, soit ils le vendent à des concurrents qui pourront l'attaquer en exploitant la brèche Ensuite, le forum

[473] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 33.
[474] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203451-hacker-definition-traduction/.

d'échanges et de logiciels *Dark0de* était très populaire sur le Darknet. Sa bonne image l'a même amené à sélectionner ses nouveaux membres après une recommandation et une étude du profil. Une fois accepté, il existe différents niveaux en fonction du degré de confiance et conférant des privilèges. Les membres du forum ont créé des *malwares* afin de les revendre à prix dérisoire. Certains de ces membres ont été emprisonnés après une opération menée conjointement par le FBI et Europol en juillet 2015. Enfin, il y a les « *grey hat* » qui sont à mi-chemin entre les « *black hat* » et les « *white hat* » et qui transgressent les lois pour des revendications qu'ils trouvent humbles. Les hackeurs ne sont pas les seuls pirates informatiques. Il convient donc d'étudier les différents types de pirates informatiques (b).

b) Les autres pirates informatiques

Il existe des pirates informatiques spécialisés dans le craquage de code d'accès, ce sont les « *cracker*[475] ». Issu du terme anglais « *crack* » qui signifie craquer, le mot *cracker* désigne les spécialistes du cassage de codes en tout genre[476]. Le terme peut aussi désigner un cryptanalyste dont la spécialité est le cassage de code crytographique. Il peut s'agir par exemple d'un code protégeant les copies de logiciel sous licence comme les partagiciels qui supposent une clé d'enregistrement[477]. Contrairement au hackeur, le « *cracker »* se contente d'introduire un système par tous les moyens possibles[478]. Certains les considèrent comme un type particulier de hackeur[479]. Pour faire simple, le « *cracker* » crée un patch[480] qui permettra de craquer un logiciel composé d'une infinité de codes mathématiques ou utilise un générateur de clé qui comprend l'algorithme du logiciel[481]. Les patchs et générateurs sont ensuite vendus sur le Darknet mais certains « *cracker* » ne sont motivés que par le défi. Les concepteurs de logiciels tentent de se défendre en utilisant diverses techniques empêchant les patchs mais dans la pratique il n'y a pas de logiciel infaillible si bien que l'éditeur du logiciel ne fera que ralentir le travail du pirate.

[475] RAYMOND E., *Le Cyberlexis : Dictionnaire du jargon informatique éd. Dunod*, 1997.
[476] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 33.
[477] Cours de Crack n°1 : le cracking. Explication disponible sur le site informatique « *zmaster* » à cette adresse : http://www.zmaster.fr/informatique_article_208.html, [consulté le 29 janvier 2018].
[478] MALKIN GS., *Internet Users' Glossary*, 1993, page 17.
[479] YOGODA B., *A Short History of Hack*, The New Yorker, 6 mars 2014, page 28.
[480] Un patch est une version modifiée du programme cracké qui supprime les restrictions.
[481] Un générateur de clé génère aléatoirement des clés jusqu'à ce qu'il trouve la bonne.

Un autre type de pirate informatique mérite d'être cité, il s'agit du « *crasher* » qui a tendance à se considérer comme un être supérieur du web. Ce type de pirate informatique s'introduit dans un système pour effacer les données. Il se distingue du « *cracker* » car il agit par pur plaisir[482]. Tous deux appartiennent à la famille des hackers, des spécialistes dont le but est de contourner les protections matérielles. Ils peuvent agir pour signaler une faille au propriétaire du système, pour en tirer profit, pour défendre une cause[483] ou simplement pour relever un défi (2).

2. Les agissements des pirates informatiques

Les criminels se spécialisent afin d'avoir un haut degré de compétence dans ces domaines. Sur Internet, les criminels peuvent être organisés et constituer des groupes plus ou moins importants, mais ils peuvent aussi agir de manière isolée. Les criminels sont omniprésents dans le temps et dans l'espace en raison de la multiplication des réseaux et donc des cibles. La dématérialisation des transactions, les facilités de communication ainsi que les solutions de chiffrement et d'anonymat autorisent les liaisons entre criminels sans contact physique. Le criminel agit en étant dans son environnement habituel, contrairement à un braqueur qui doit faire face au stress en raison de sa présence sur les lieux.

Les pirates informatiques utilisent plusieurs méthodes leur permettant d'arriver à leurs fins et exploitent les nouvelles technologies pour enfreindre la loi. Il y a les attaques par déni de service plus connues sous le nom de DDoS[484] qui permettent de rendre inutilisable un service en l'inondant. Créées dans les années 1990[485], elles se sont multipliées avec la Big data puisqu'elles sont opérées en saturant la bande passante du serveur visé en envoyant un paquet de données afin de rendre le serveur injoignable[486]. Les hackeurs utilisent ensuite l'ingénierie sociale qui consiste à exploiter les failles humaines, l'usurpation d'adresse IP afin de marquer

[482] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 33 : « *Le terme « crasher » provient du verbe anglais « to crash » qui signifie « s'écraser ». Ce dernier pénètre à l'intérieur d'un système informatique et détruit ou sabote un de ses éléments par pur plaisir* ».
[483] On parle de hacktivisme. La plupart des hacktivistes se battent pour un internet pour tous, garant des libertés individuelles.
[484] Disponible à cette adresse : https://fr.wikipedia.org/wiki/Attaque_par_déni_de_service.
[485] La première attaque DDoS aurait eu lieu en août 1999.
[486] Disponible à cette adresse : https://www.ovh.com/fr/anti-ddos/principe-anti-ddos.xml.

leur propre identité lors d'une attaque informatique, les logiciels espions[487] et les *malwares*[488] qui comprennent les chevaux de Troie[489], les virus informatiques[490] et les vers informatiques[491]. Il convient de traiter les instruments des pirates informatiques (a) et leurs nouvelles méthodes (b).

a) Les instruments des pirates informatiques

Les pirates informatiques, qu'ils soient hackeur, *crasher* ou *cracher*, ont la possibilité d'utiliser un arsenal complet de logiciels. Il existe les chevaux de Troie, les botnet, les virus, les vers et les logiciels espions. Les premiers, les chevaux de Troie permettent de s'introduire dans un ordinateur afin d'en prendre le contrôle à distance. D'apparence inoffensive, ils permettent d'installer des programmes nocifs qui volent ou détruisent des données. Le mode opératoire classique est l'envoi d'un mail avec une pièce jointe qui, lorsqu'elle sera ouverte par la victime, ouvrira une porte sur l'ordinateur.

Les botnets[492] sont des réseaux de bots[493] informatiques connectés à un réseau Darknet ou à Internet et qui communiquent entre eux afin d'exécuter certaines tâches pouvant être légitimes. Néanmoins, des dérives sont apparues et les cybercriminels ont détourné l'usage des botnets qui sont devenus malveillants. Les pirates informatiques utilisent des chevaux de Troie pour infecter et prendre le contrôle de milliers, voire de millions d'ordinateurs pour maîtriser un immense réseau appelé « *réseau zombie* »[494] capable de lancer une cyberattaque sans être identifiable, de lancer une énorme campagne de spam[495] ou de lancer une attaque de déni de

[487] Ce genre de logiciel s'installe sur un ordinateur ou un téléphone afin d'en récupérer les données.
[488] Un logiciel malveillant permet de nuire à un système informatique sans le consentement de l'utilisateur.
[489] Un cheval de Troie est un logiciel malveillant qui est en apparence légitime mais qui permet d'installer un parasite à l'insu de l'utilisateur. C'est en l'ouvrant que l'utilisateur infecte son ordinateur.
[490] Un virus informatique est un logiciel qui perturbe plus ou moins gravement le fonctionnement la machine infectée. Il a été conçu pour se propager rapidement à d'autres machines.
[491] Un vers informatique fonctionne comme un virus à la différence qu'il n'a pas besoin de support physique pour se propager. Il utilise les réseaux.
[492] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 38 : « Contraction de robot et réseau, un « botnet » un terme générique qui désigne un groupe d'ordinateurs, de quelques milliers à plusieurs millions, contrôlés par un pirate à distance ».
[493] Selon Andrew Leonard, un bot est « *un programme informatique autonome supposé intelligent, doué de personnalité, et qui habituellement, mais pas toujours, rend un service* ».
[494] https://csirt.gouv.bj/les-reseaux-de-zombies-une-menace-permanente/, site consulté le 2 juin 2018.
[495] Un spam est un courriel indésirable.

service distribué[496]. Ces dernières supposent l'envoi multiple de requêtes ayant pour objectif l'entrave de la capacité du site Internet qui ne sera plus capable de les gérer.

Les virus informatiques se propagent par le biais du partage de fichiers par clé USB ou autre, de sites internet infectés ou d'un téléchargement d'une pièce jointe. Une fois qu'il a introduit le système, il reste en veille jusqu'à l'activation du fichier qui lui permettra de se reproduire dans le système. Il y a plusieurs types de virus en fonction de la méthode de propagation. Parfois, l'infection du système peut être discrète pendant une très longue période pouvant aller jusqu'à des mois sans que l'utilisateur ne s'en rende compte[497]. Aujourd'hui, tous les objets connectés tels que les téléphones portables, les tablettes tactiles ou les robots de cuisine multifonction sont des cibles pour les virus. Il est recommandé d'installer des logiciels de protection appelés anti-virus.

Contrairement au virus, le ver informatique n'a pas besoin de programme hôte pour s'activer et se propager[498]. Il est en mesure de se reproduire seul et de se propager par le biais d'un réseau qu'il contaminera également. Sa propagation via Internet est très rapide

Enfin, un logiciel espion est un logiciel qui s'introduit dans un système afin d'obtenir des informations personnelles sur la victime. Il peut obtenir les numéros de carte bancaire ou de sécurité sociale. Les hackeurs s'en prennent à leurs victimes grâce à des attaques orchestrées contre des machines et leurs données sans que cela nécessite de présence physique. Leurs méthodes sont nombreuses (b).

b) Les méthodes des pirates informatiques

Les pirates informatiques utilisent des techniques permettant d'exploiter les failles humaines,

[496] *Distributed Denial of Service*, déni de service distribué.
[497] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 130 : « Pendant cette période, les systèmes informatiques infectés sont contrôlés par les pirates, mais ne montrent aucun signe apparent d'infection : l'utilisateur peut donc utiliser sa machine sans se rendre compte qu'elle est infectée ».
[498] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 54 : « Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Contrairement à un virus informatique, il n'a pas besoin d'un programme hôte pour se répandre ».

c'est l'ingénierie sociale[499].

Le « *pollupostage* » ou SPAM est défini par la CNIL[500]comme « *l'envoi massif, et parfois répété de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière* ». Ce type de méthode est interdite puisque l'article 226-16 du code pénal dispose que « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* ».

Les attaques DoS ou par « *déni de service* » sont des cyberattaques qui visent à rendre indisponible un service en l'inondant de requêtes. Il s'agit alors de bloquer un serveur de fichiers, un site web ou la distribution de courriel.

Le dévoiement ou « *pharming* » est défini par Légifrance comme la « *technique consistant à détourner subrepticement des communications à destination d'un domaine vers une adresse différente de son adresse légitime*[501] ». Il s'agit en fait d'une technique informatique utilisant les vulnérabilités DNS, c'est-à-dire les faiblesses du système informatique permettant à un pirate d'atteindre l'intégrité du système. Concrètement, lors d'une requête de noms de domaine[502], la vraie adresse IP du nom de domaine est remplacée par celle d'un site frauduleux similaire voire identique à l'original[503]. En entrant la bonne adresse web, l'utilisateur est redirigé vers un faux site web qui pourra récupérer ses données[504]. Cette technique est très utilisée pour récupérer les numéros de carte bleue.

Ensuite, l'hameçonnage ou le « *phishing* » est utilisé par les pirates afin d'obtenir des

[499] QUÉMÉNER M., *Cybermenaces, entreprises, Internautes,* Economica, 2008, page 45.
[500] Commission nationale de l'informatique et des libertés.
[501] Définition disponible à cette adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021530619&dateTexte=&categorieLien=id.
[502] Une requête DNS pour Domain Name System soit système de noms de domaine permet d'accéder à un site en traduisant les noms de domaine Internet en adresse IP.
[503] Disponible à cette adresse : http://www.citi.umich.edu/u/provos/papers/ndss08_dns.pdf.
[504] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 41 : « Le Pharming redirige les utilisateurs d'un site Web authentique vers un site Web frauduleux reproduisant à l'identique l'original ».

informations personnelles pour une éventuelle usurpation d'identité. Il s'agit de faire croire à l'individu qu'il échange avec un tiers de confiance – la sécurité sociale, sa banque – pour lui soutirer des informations personnelles comme son numéro de carte de crédit, une photocopie de son passeport ou un mot de passe. Le plus souvent, ce genre d'attaque est réalisé par mail mais la technique du SMS s'est démocratisée, on parle alors de *SMiShing*[505]. A la différence du pharming, le phishing n'exploite pas une vulnérabilité informatique mais la faiblesse humaine[506] puisque l'internaute pense avoir reçu le mail d'une personne sérieuse. Le *phising* est un délit visé par l'article 226-18 du Code pénal disposant que « *le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* » et par l'escroquerie[507].

Enfin, les hackeurs sont capables à distance de prendre le contrôle d'un système informatique afin de le détourner ou de saboter son contenu, il s'agit du « *hijacking*[508] ». La prise de contrôle faite à l'insu de l'utilisateur permet au hackeur d'effacer, modifier ou de récupérer une partie ou la totalité des données, de détourner des fonds, d'usurper l'identité[509]. En se connectant sur le Darknet, un utilisateur non expérimenté s'expose à ce genre de menaces puisque les hackeurs peuvent prendre le contrôle grâce à des failles de sécurité se trouvant sur les différents navigateurs du Darknet. Sur ce dernier, lorsque les hackeurs proposent leurs services, le paiement s'effectue très souvent en bitcoin. Cette cryptomonnaie très critiquée mérite d'être présenter dans la section suivante (section 2).

[505] Disponible à cette adresse : www.definitions-marketing.com/definition/Smishing/?page=article.
[506] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 41 : « C'est une technique d'ingénierie sociale très prisée des cybercriminels puisqu'elle exploite non pas une faille informatique mais la crédulité humaine en dupant les internautes par le biais de courriers électroniques non sollicités semblant provenir d'une entreprise ou d'un service connu, comme sa banque ou un site de commerce dont la victime est cliente ».
[507] Code pénal Art. 313-1.
[508] « *Le hijacking est un mot de la langue anglaise apparu au 20ème siècle pour désigner une action de détournement (détournement d'avion). Le terme s'est ensuite étendu au domaine informatique et s'applique à toute une série de prises de possession illégales ou de bidouillage à but malsain* ». Disponible à cette adresse https://fr.wikipedia.org/wiki/Hijacking, [consulté le 12 décembre 2017].
[509] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 61 : « Le « hijacking » est une prise de possession illégale visant à détourner tout ou partie d'un système informatique, de logiciel ou de données informatiques, ou encore à saboter la connexion Internet d'un ordinateur pour la rediriger vers les sites voulus. Ils désignent donc la modification de force et à l'insu des personnes, de certains réglages ou comportements d'un élément informatique ».

SECTION 2
Le Bitcoin, monnaie du crime ?

Aux enjeux de la cybercriminalité sur le web dissimulé s'ajoute le retentissement en pleine expansion des cryptomonnaies sur la géopolitique et l'économie. Les problématiques affectent à la fois les institutions internationales et les acteurs privés, et touchent à la sécurité, à l'économie, à la politique et au droit.

En 2018, lorsque le cours du bitcoin a explosé il était déjà un sujet d'intérêt important pour les cybercriminels qui l'utilisent pour plusieurs raisons. Cette cryptomonnaie permet de conclure des affaires illégales, de blanchir de l'argent ou d'exploiter les failles d'interfaces fragiles. Par exemple, les attaques peuvent se faire par le biais d'un « *cryptoshuffler* », une sorte de « *malware* » détectant la copie d'une adresse pour la remplacer lors d'un paiement en bitcoin et recevoir la somme.

Présentée comme la monnaie de prédilection des sites de ventes du Darknet, le bitcoin serait le nouvel outil facilitant les activités des différentes mafias et du blanchiment d'argent. Mais, est-ce sa seule fonction ? Quels sont ses autres avantages ? Peut-elle se substituer aux monnaies classiques ?

Une partie des fantaisies du Darknet repose sur cette devise numérique décentralisée dont l'émission est régie par des algorithmes, et le cours par la loi de l'offre et la demande. Néanmoins, les usages ont évolué et sa réputation sulfureuse est sur le point de disparaître. Les entreprises qui acceptent les bitcoins sont de plus en plus nombreuses. Par exemple, le directeur e-commerce de Monoprix, une entreprise française fondée en 1932, a affiché un enthousiasme fort à l'égard du bitcoin[510]. De plus, il est désormais possible de payer sa pizza en bitcoin, son billet de bus[511] ou ses frais universitaires à l'étranger. Il n'est pas anodin que de nombreuses personnalités politiques se soient intéressées au bitcoin. Mais dans la pratique, comme le précise Adi Ashmir, un universitaire israélien et inventeur de l'un des plus importants algorithmes cryptographiques, plus de la moitié des bitcoins dormiraient sur les comptes de leurs

[510] Avant d'y renoncer en 2015.
[511] Sur le site de la compagnie de Bus *Isilines* il est possible de payer en bitcoins : « *Pour vos réservations en ligne, vous pouvez payer par carte bancaire, par PayPal et depuis peu avec des bitcoins* », https://www.isilines.fr/questionsFAQ.

propriétaires.

Créé en 2009 par l'énigmatique Satoshi Nakamoto, le bitcoin a été conçu afin d'échapper au contrôle des banques centrales. Dans notre société économique dépendante des fluctuations économiques, ce genre de cryptomonnaies semble révolutionnaire. Selon Tarkowski Tempelhof[512], créatrice de « *Bitnation*[513] », le bitcoin est une nation, ce qui implique la connexion d'individus partageant des valeurs similaires. Toutefois, la nature singulière de cette monnaie suscite des interrogations quant à la sécurité des dépôts et quant à l'influence des politiques monétaires sur elle.

Souvent pointé du doigt en raison de sa nature spéculative et de sa volatilité excessive, le bitcoin a été présentée au monde en 2009 via un message public sur une liste de diffusion exclusivement réservée aux crypto-anarchistes. Il s'est rapidement développé au point de devenir la monnaie de référence pour les achats illégaux sur *Silkroad.* A la suite de la crise financière mondiale de 2008, un nombre grandissant de personnes, ne faisant plus confiance aux banquiers, a commencé à échanger des dollars en bitcoin. L'augmentation spectaculaire de cette cryptomonnaie a entraîné une explosion d'investissement[514]. De nombreux membres de la communauté Bitcoin ont conclu des négociations complexes avec les gouvernements et les régulateurs sur la façon de faire fonctionner la nouvelle monnaie numérique parallèlement à la traditionnelle. En 2013, la fondation Bitcoin a organisé une conférence appelée « *le futur du paiement* », un titre qui reflète le point de vue de beaucoup de ses utilisateurs. Ce nouvel instrument financier offre de nouvelles possibilités, pour des transactions légales ou non.

Les transactions de bitcoins sont émises et validées grâce aux ordinateurs composant le réseau et fonctionnant selon des chaînes de blocs. Un ordinateur qui valide une transaction grâce à son processeur et à sa capacité de calcul obtient un montant de Bitcoin au prorata de sa participation. C'est donc un ensemble de relais qui attribue de la puissance de calcul permettant le fonctionnement de l'algorithme de transaction de la cryptomonnaie[515].

[512] https://medium.com/@susannetarkowskitempelhof/bitnation-year-1-summary-6a1c40b4ee5a#.pp5p3yqpx.
[513] Bitnation est un projet d'Etat-Nation autonome utilisant la chaîne de bloc.
[514] En 2015, il y avait 15 millions de Bitcoins en circulation soit plus de 3 milliards de dollars.
[515] RENNARD J.-P, *Darknet, Mythes et réalités*, Ellipses, avril 2016.

La lecture du document PDF de Satoshi Nakamoto[516] permet de comprendre le fonctionnement du bitcoin basé sur la *blockchain*[517]. Tout commence par une sorte de livre de compte décrivant des dépenses. Le 1er janvier 2010 à 16h, A paie 300 euros à B ; le 3 janvier 2010 à 20h, B paie 50 euros à C ; le même jour à 20h, A paie 20 euros à C etc. Le Bitcoin serait donc basé sur un livre de compte n'ayant pas besoin de pièces de monnaie. Il s'agit d'une histoire de déduction. Dans l'exemple donné, B a 250 euros puisqu'il a récupéré 300 euros de A et donné 50 euros à C. Lorsqu'un fichier est rempli, un autre résumant le précédent est créé. Ces fichiers sont appelés des « *blocs* », et reliés entre eux ils forment donc une « *chaîne de* blocs » appelée « *blockchain*[518]». Cette dernière est définie par Légifrance comme un « *mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification (...) utilisée dans le domaine de la cybermonnaie, où elle remplit la fonction de registre public des transactions* ».

La blockchain utilise la fonction de « *hachage* » pour pouvoir résumer les fichiers précédents. Utilisée en cryptographie, cette technique permet d'enregistrer un espace de donnée potentiellement grand grâce à une empreinte numérique. Il s'agit d'une « séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message, sans le révéler, dont la valeur unique est produite par un algorithme de hachage, et qu'on utilise pour créer une signature numérique »[519]. La moindre modification du contenu entraînera un changement de l'empreinte numérique.

A titre d'exemple, le contenu du livre « Les Misérables de Victor Hugo » est représenté par ce nombre « 150201d82c6da2cfead6d6ae22243185fd30a23e ». Par conséquent, dans une chaîne de blocs, le bloc 3 contient un hash du bloc 2, qui contient un *hash* du bloc 1. Si le bloc 1 est modifié, l'ensemble de la chaîne sera modifié et compromis[520].

[516] https://bitcoin.org/bitcoin.pdf.
[517] « *Il s'agit d'une technologie de stockage et de transmission d'informations sans organe de contrôle* », https://fr.wikipedia.org/wiki/Blockchain.
[518] Disponible à cette adresse : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26531717.
[519] Disponible à cette adresse : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8371028, [consulté le 15 avril 2018].
[520] *La Blockchain décryptée, les clefs d'une révolution*, 2018. Disponible à cette adresse : https://blockchainfrance.files.wordpress.com/2018/06/la-blockchain-decc81cryptecc81e-les-clefs-dune-recc81volution.pdf, [consulté le 21 juillet 2018].

La première chaîne de bloc est la plus populaire, il s'agit de la cryptomonnaie bitcoin apparue en 2009. Si les deux technologies ont évolué ensemble, la chaîne de blocs est désormais utilisée pour des cas différents de la cryptomonnaie. En effet, les *blockchains* peuvent être divisées en trois catégories selon leur utilisation. Premièrement, elle permet les transferts d'actifs comprenant les cryptomonnaies mais aussi les obligations, titres, actions ou votes via des actifs numériques appelés *tokens*. Deuxièmement, une chaîne de blocs peut être utilisée en tant que registre pour garantir une meilleure traçabilité des échanges. Troisièmement, il y a la possibilité de mettre en place des programmes autonomes permettant l'exécution automatique des termes et conditions d'un contrat, sans intervention humaine, il s'agit des *smart contracts*. Le domaine d'utilisation est démesuré : industrie musicale, énergie, immobilier, vote, assurance, industrie pharmaceutique… Ainsi, les enjeux économiques, juridiques et de gouvernance d'une telle technologie sont nombreux.

L'approche du bitcoin nécessite une présentation préalable de cette technologie *blockchain*. Un premier paragraphe permettra de la présenter (§1) tandis qu'un second sera consacré au bitcoin (§2).

§1) La technologie *blockchain*

Une blockchain, ou chaîne de blocs en français, peut être définie comme « *base de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres, les transactions successives effectuées entre ses utilisateurs depuis sa création* » ou comme « *une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle* ». Le site Légifrance donne la définition suivante : « *mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* » et précise qu'elle « *est notamment utilisée dans le domaine de la cybermonnaie, où elle remplit la fonction de registre public des transactions*[521] ».

[521]https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034795042&categorieLien=id.

Concrètement, une chaîne de blocs constitue une base de données distribuée contenant l'histoire de l'ensemble des échanges opérés par les utilisateurs depuis sa constitution. La vérification de la validité de la chaîne se fait par l'ensemble des utilisateurs, sans intermédiaire[522], puisque la base de données est distribuée et sécurisée. Une *blockchain* peut être publique et être ouverte à tous, ou privée et limité à certains utilisateurs. Les premières peuvent être comparées à un grand livre public, infalsifiable et surtout anonyme. Selon le mathématicien Jean-Paul Delahaye, une chaîne de blocs peut être assimilée à « *un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible* », il définit ici la *blockchain* publique.

Les transactions d'une chaîne sont regroupées par blocs validés par certains utilisateurs du réseau appelés nœuds ou mineurs. Ces derniers utilisent des techniques différentes en fonction du type de chaîne de blocs. Pour le bitcoin, la technique utilisée est nommée « *Proof-of-work* » et passe par la résolution de problèmes algorithmiques par de puissantes machines. Lorsqu'un bloc est confirmé, il est daté et ajouté à la *blockchain* et accessible sur l'ensemble du réseau. Le processus de vérification peut être relativement long et prendre une dizaine de minutes.

Les *blockchains* suscitent l'engouement général et créent des interrogations juridiques et technologiques. En 2018, cette technologie ne s'est pas encore démocratisée, elle est en pleine expérimentation et transition juridiques. Il convient de se demander quelle est la place du droit dans cet environnement qui avait vocation à s'en passer. Il s'agit de présenter le fonctionnement de la blockchain (A) et ses enjeux (B).

A) Le fonctionnement d'une blockchain

Blockchains privée et publique sont très différentes. La *première* ressemble à un intranet plus élaboré qui contrôle et identifie les différents acteurs. Une personne peut modifier les règles et contrôler le bon fonctionnement de cette *blockhain*. La *blockchain publique* permet la transmission de cryptomonnaie comme le Bitcoin et d'actifs appelés *tokens*. Ces derniers sont des jetons numériques qui permettent les échanges sécurisés de droits financiers, politiques ou d'usage. Par exemple, un individu qui a financé une activité peut recevoir un *token*, assimilable

[522] Pour les *blockchains* publiques.

à une part, en échange. Une *blockchain* publique permet également d'enregistrer des informations de manière sécurisée grâce à une traçabilité performante. Une dernière possibilité est offerte par la *blockchain* puisqu'elle crée un automatisme en matière de contrat grâce au *smart contract*. Pour permettre tous ces processus, blockchains privées et publiques (2) utilisent des algorithmes très performants (1).

1. L'utilisation d'algorithmes

Le Professeur[523] Mustapha Mekki, a publié de manière claire sur le sujet[524]. Il présente la *blockchain* qui serait selon lui une révolution plus importante qu'Internet.

Il la définit comme « *une technique de stockage et de conservation d'informations. Il s'agit d'une suite de données, sous forme d'algorithmes, mises en blocs liés les uns aux autres par une empreinte numérique (…) La chaîne de blocs constitue ainsi un gigantesque registre, un immense livre comptable, intégrant un ensemble de transactions validées dans une liste infinie, utilisant différentes techniques de cryptage : clés cryptographiques asymétriques (une clé publique (ex. adresse mail) et une clé privée (mot de passe par ex.), système de péage (filtrage, contrôle) par la preuve de travail ou d'existence, mise en œuvre d'un système de hachage du message… Chaque bloc comporte des écritures. Une fois le bloc achevé, une empreinte numérique lui est rattachée et un autre bloc est créé qui est lié à celui qui le précède par cette empreinte. Ce livre de compte, à la différence des systèmes actuels, n'est tenu, dans l'idéal, par aucun tiers (ex. plateforme numérique telle que Airbnb ou eBay). L'opération est donc décentralisée et ce sont les milliers de personnes de la blockchain, propriétaires d'un simple ordinateur, selon un processus informatique complexe qui consiste à résoudre une énigme mathématique, qui en ont la charge. Chaque ordinateur conserve une copie de la blockchain. Plus le nombre de participants est important plus la sécurité et l'intégrité des blockchains sont garanties. L'intérêt de la blockchain est que tout ce qui est inscrit sur cette chaîne de bloc ne peut pas être modifié ou falsifié* ». Par conséquent, grâce aux algorithmes l'intérêt premier des blockchains est de permettre l'archivage de données de manière sécurisée et quasi-anonyme.

[523] Professeur de droit privé et sciences criminelles à l'Université Paris 13 Villetaneuse.
[524] MEKKI M., *Droits et algorithmes : de la blockchain à la justice prédictive*, 6 juin 2017. Disponible à cette adresse : https://actu.dalloz-etudiant.fr/le-billet/article/droitss-et-algorithmes-de-la-blockchain-a-la-justice-predictive/h/d66e9db5333715c8ff6d88221cf44721.html, [consulté le 1er septembre 2017].

En outre, les algorithmes peuvent être utilisés en matière de justice prédictive. En se basant sur une base de données judiciaire[525], ils analysent des paramètres juridiques et factuels comme des faits, des décisions de justice, de la doctrine afin de prédire les décisions d'un juge. En ce sens, des logiciels sont en mesure de calculer le montant de dommages intérêts permettant la réparation d'un préjudice, la probabilité de gagner une affaire ou d'une prestation compensatoire à la suite d'un divorce. Ainsi, nombreux sont les répercussions que peuvent avoir les différents types de *blockchains* (2).

2. Les différents types de *blockchains*

Les grandes institutions financières ont conscience des enjeux de la *blockchain* pour leurs activités. Mais en 2018, la loi reste floue quant à sa manière de traiter cette technologie. Il est opportun de s'interroger sur la gouvernance de la *blockchain*, c'est-à-dire sur la mise en oeuvre du pouvoir, et sur la force juridique des opérations qui en découlent. En tout état de cause, l'analyse juridique des *blockchains* dépend du type de *blockchain* mise en place, il peut s'agir d'une blockchain ouverte, d'une blockchain fermée ou d'un mélange des deux.

Ainsi, il existe trois types de *blockchain*s. Tout d'abord, une *blockchain* publique est un registre ouvert à tous de manière décentralisée. Il permet aux utilisateurs de participer au processus de consensus en accédant et effectuant des transactions sans passer par un tiers de confiance. C'est la *blockchain* la plus populaire utilisée par le bitcoin qui est correspond à l'idée communautaire ou même alternative de l'économie.

Ensuite, une *blockchain* de *consortium* suppose un contrôle du processus de consensus par un ensemble de nœuds. Il s'agit d'une *blockchain* hybride avec certains nœuds publics et d'autres privés. Concrètement, les participants ont certains droits qui leur permettent de prendre des

[525] Avec la loi n°2016-1321 du 7 octobre 2016 pour une République numérique : « *les données produites par la sphère publique sont souvent très riches, mais tout aussi souvent très confidentielles car du niveau de chaque individu. Leur accès était jusqu'ici dans les faits quasiment impossibles, même pour les besoins de la recherche. Grâce à la #LoiNumérique, un système d'accès sécurisé permettra aux seuls chercheurs et statisticiens publics habilités, dans le cadre d'un projet donné, de pouvoir étudier ces données pour mieux comprendre l'efficacité de nos politiques publiques et évaluer l'effet de futures réformes. Ainsi la compréhension fine de l'impact de la mise en place d'un revenu universel est-t-elle désormais rendue possible* ». Disponible à cette adresse : https://www.economie.gouv.fr/republique-numerique/15-points-cles.

décisions sur la *blockchain*. Chaque membre possède un nœud du réseau et peut autoriser la validation d'une transaction. Pour qu'un bloc soit ajouté à la chaîne, la majorité est nécessaire. Ce type de *blockchain* peut être public ou privé grâce à la mise en place d'un mécanisme de cooptation. Enfin, les *blockchains* privées ou « *permissioned* » sont centralisées dans le réseau. Une entité contrôle et accepte les membres participants dans le réseau.

Les règles de fonctionnement d'une *blockchain* diffèrent en fonction de son degré d'ouverture. Il y aura plus de gouvernance dans une chaîne ouverte que dans une chaîne fermée. Dès lors, une blockchain privée est régie par une institution centralisée qui mettra en place un règlement ou des conditions d'accès, tandis qu'une blockchain publique l'accès sera libre et il n'y aura pas de règle de fonctionnement en dehors de la technologique : « *Code is law* ». Concernant le propriétaire de la *blockchain*, cela dépend également du type de *blockchain* mis en place. Pour une *blockchain* privée, c'est l'organisme en charge de la gestion de la *blockchain* qui est le propriétaire protégé par des droits de propriété intellectuelle, tandis que pour une *blockchain* publique, il n'y a pas de propriétaire de la chaîne.

Une opération traitée sur une *blockchain* peut refléter une transaction extérieure à la chaîne telle qu'une vente d'œuvre d'art dans une chaîne privée, ou constituer elle-même une transaction comme le bitcoin. Se pose pour cette dernière un problème d'opposabilité juridique. En effet, lorsque la *blockchain* est publique, une opération n'a de force juridique qu'entre les participants si bien qu'en dehors de la blockchain l'opération ne devrait pas avoir de valeur légale. Dès lors, l'opération n'est pas opposable aux tiers, elle ne l'est qu'entre acheteur et vendeur. Le droit applicable en cas de litige entre parties est celui désigné par les parties sauf si un consommateur est impliqué.

Au-delà de ses aspects techniques, la technologie blockchain présente des intérêts liés au droit : ce sont les enjeux juridiques de la technologie blockchain qui méritent d'être présentés dans le sous paragraphe suivant (B). Il s'agit notamment d'étudier l'exemple du smart contrat et des tokens.

B) Les enjeux de la technologie *blockchain*

L'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse a permis à la France

d'instaurer le protocole *blockchain* dans le Code monétaire et financier. Cette ordonnance vise à « *moderniser le régime juridique applicable aux bons de caisse et de procéder aux adaptations nécessaires pour permettre l'intermédiation de ces titres sur les plateformes de financement participatif des conseillers en investissements participatifs (CIP) et des prestataires de services d'investissement (PSI)* ». Depuis, les bons de caisse peuvent être inscris dans une *blockchain*. Le législateur semble donc vouloir prendre en compte les évolutions technologiques telles que la blockchain. Pourtant, en 2018, cette technologie est encore incompréhensible pour beaucoup de juristes.

Le droit évolue moins rapidement que la technologie et c'est la raison pour laquelle les *blockchain* sont difficiles à saisir juridiquement. En effet, Internet a métamorphosé certains principes fondamentaux du droit, en matière de propriété intellectuelle, de protection de la vie privée, de criminalité et de contrat. Le monde numérique a créé de nouveaux enjeux juridiques qui ont contraint le droit à s'adapter. Mais aujourd'hui, une innovation juridique et technologique a permis le phénomène inverse : le droit s'est accaparé le numérique. En 2018, nombreux sont les ouvrages juridiques et informatiques à aborder de nouveaux thèmes en utilisant des termes comme *blockchain*, bitcoin, *token* ou *smart contract*. Autant de termes qui touchent à la fois au droit et au numérique qui nécessitent donc des connaissances dans les deux domaines.

Initialement, la technologie *blockchain* aspirait à mettre en place un monde juridique et économique détaché de l'emprise étatique. Mais cette idée de base est en déclin comme le prouve l'exemple du bitcoin qui a été saisi de manière rigoureuse par le droit qui lui applique désormais le régime fiscal des biens meubles incorporels et celui des bénéfices industriels et commerciaux. Aujourd'hui, les enjeux relatifs à cette technologie de stockage et de transmission d'informations sont nombreux. Un premier peut concerner la transmission de monnaie, un deuxième la conservation et la traçabilité de ces données via des registres et un troisième l'automatisation des contrats grâce aux *smart contract* qui seraient très innovants juridiquement et économiquement parlant.

Ainsi, grâce à l'avènement des réseaux chiffrés et des réseaux alternatifs, les monnaies électroniques sont devenues populaires. Elles préoccupent les instances Etatiques en raison de l'absence de contrôle qu'ils ont sur elles et en raison des activités illégales qui sont commises

grâce à elles. Il est possible de citer Monero[526] qui était accepté sur *Alphabay* ou le bitcoin la plus populaire des cryptomonnaies. Mais la *blockchain* n'est pas limitée aux cryptoactifs (1) puisqu'elle offre également d'autres possibilités en matière de propriété intellectuelle ou de contrat (2).

1. Les cryptoactifs

La *blockchain* permet l'échange de cryptomonnaie et de jeton. Les premières sont les unités de valeur du réseau qui permettent de rémunérer les mineurs qui contribuent au fonctionnement et à la sécurité du réseau, et qui peuvent être échangées sur l'ensemble du réseau. Les seconds, appelés *tokens*, permettent l'enregistrement d'opérations et de définir une nouvelle unité dans un réseau existant qui n'a pas été créé pour cette raison. Leur activation est plus simple que pour les cryptomonnaie et leur qualification propre à chaque opération.

Ces unités de valeurs, que ce soit les cryptomonnaies ou les *token*s, sont souvent qualifiées de cryptoactifs pour éviter la référence à la monnaie et le contrôle des banques centrales, et parce qu'ils représentent tous deux des actifs. Au delà de la technologie *blockchain*, les cryptomonnaies et les jetons numériques ont des points communs. Tout d'abord, ils permettent le transfert de propriété d'une unité voire d'une fraction d'unité d'une paire de clés publique et privée à une autre paire de clés. Ensuite, ces cryptoactifs sont des fongibles de telle sorte que chaque unité a la même valeur et est interchangeable. Enfin, ils sont divisibles comme les centimes d'euros. En ce sens, il existe des sous-unités de bitcoin, un millibitcoin représente 10^-3 bitcoin, un bits ou microbitcoin 10^-6 bitcoin et un sathoshi 10^-8 bitcoin. Il s'agit alors de traiter les cryptomonnaies (a), avant de s'intéresser aux jetons numériques appelés *tokens* (b).

a) Les cryptomonnaies

Présenter les cryptomonnaies suppose un très bref développement sur la création de la monnaie. Pour faire simple, avant la création de la monnaie, les échanges se fondaient sur le troc, c'est-à-dire sur des échanges de produits différents. La rareté permettait de déterminer la valeur d'un

[526] https://www.wedemain.fr/404.html.

produit. Un ananas valait deux pommes par exemple. Mais, pour éviter de couper certains produits en deux, des monnaies primitives ont été créées.

Définie par Aristote, la monnaie est une réserve de valeur, un intermédiaire des échanges et une unité de compte[527]. C'est un instrument de paiement utilisé à une époque donnée dans une société. Elle a ensuite évolué et pris diverses formes : il pouvait s'agir d'animaux, de nourriture et de matières comme l'or ou l'argent. Ces dernières étaient rares et ont pris de la valeur. C'est à partir d'elles que des pièces ont été créées afin de visualiser cette valeur. Dès lors, les fabricants d'objets en or ont commencé à conserver l'or des particuliers dans des coffres-forts. En échange de l'or, les orfèvres remettaient un certificat de dépôt afin que les clients récupèrent leur or à tout moment. Toutefois, pour des raisons pratiques les clients ont préféré échanger ces certificats entre eux. Il est plus facile d'échanger un certificat valant bon pour 10 kilogrammes d'or que ces 10 kilogrammes d'or. Ces certificats sont en quelque sorte les ancêtres des billets de banque actuels. Les orfèvres ont remarqué que les clients ne récupéraient plus leur or et ont décidé de diffuser des certificats de dépôt pour de l'or qu'ils n'avaient pas. Ainsi, les orfèvres se sont mis à prêter de l'argent qu'ils n'avaient pas en leur possession. La société moderne est basée sur le même principe. Les espèces ont de la valeur car les individus savent qu'ils pourront acheter des biens avec. Désormais, ce sont les monnaies fiduciaires[528] et scripturales qui sont utilisées. La première représente l'ensemble des pièces et des billets de banque dont la valeur réelle est supérieure à la valeur intrinsèque, tandis que la seconde forme les dépôts bancaires qui circulent grâce à des moyens de paiement comme les virements, les chèques ou les cartes bancaires. Lorsqu'un individu a 500 euros sur son compte, la banque ne les conserve pas en billets dans un coffre-fort. Cela correspond à la dette de la banque envers le client. Les banques génèrent de l'argent grâce aux crédits. Les crises financières peuvent avoir lieu lors d'un « *bank run*[529] », c'est-à-dire une course aux dépôts. L'importance du pouvoir monétaire justifie l'intérêt des Etats qui définissent la devise officielle qui sera une marque de leur puissance. Grâce aux banques centrales les Etats fixent la politique monétaire ayant pour but d'assurer une stabilité des prix. Pendant longtemps, les monnaies étaient définies par rapport à l'or mais depuis 1944, en vertu des accords de *Bretton* Woods seul le dollar américain est convertible en

[527] Une unité de compte permet de mesurer la valeur des stocks.
[528] Définition disponible à cette adresse : http://droit-finances.commentcamarche.net/faq/23872-monnaie-fiduciaire-definition.
[529] Il s'agit d'un phénomène qui voit un grand nombre d'individus se ruer vers les guichets pour retirer leur argent.

or. En 1971, les Etats-Unis abandonnent cette possibilité et désormais toutes les monnaies sont échangeables entre elles sans passer par de l'or réel. Par exemple, en juin 2018, 1 euro vaut 1,17 dollar. Les cryptomonnaies fonctionnent selon le même raisonnement puisqu'il s'agit d'une monnaie digitale disposant de toutes les propriétés de la monnaie physique.

En fondant *ecash*[530]en 1983 et *Digicash* en 1990, le cryptographe David Lee Chaum devient un pionnier en matière de cryptomonnaie. Avant d'être mis en faillite en novembre 1998, la société *Digicash* permettait d'effectuer des transactions en ligne sans traçabilité. A la suite de cet échec, d'autres cryptomonnaies comme *B-money*[531] ou *Bitgold* vont suivre. La première, proposée en novembre 1998 par le *cypherpunk* Wei Dai, est un système de paiement électronique anonyme. Elle est citée par le créateur du bitcoin lorsqu'il diffuse son essai. La seconde, *Bitgold*, a été créée la même année par le juriste et cryptographe Nick Szabo[532]. Elle ne jouit pas d'un large soutien mais est considérée comme le « *précurseur direct à l'architecture bitcoin*[533] ». C'est finalement le bitcoin qui rendra les cryptomonnaies populaires à partir de 2009, année à partir de laquelle les premiers Bitcoins génèrent en connaissant peu de succès. Mais très rapidement, une première bulle spéculative se crée et fait évoluer le cours du Bitcoin qui passe d'un dollar en 2010 à trente dollars en 2011. En 2013, une nouvelle spéculation le fait même évoluer d'une manière incroyable puisqu'il atteint les 244 dollars avant de redescendre à 50 dollars fin 2014[534]. En 2017, malgré les critiques liées à son instabilité, le bitcoin connaît une autre augmentation qui lui permet d'atteindre les 2500 dollars et d'attirer de grands groupes comme *PayPal*. Un site liste même les commerces qui acceptent le bitcoin[535].

En 2018, il y a un réel engouement pour les cryptomonnaies qui en effraient certains[536]. Par

[530] CHAUM D.L., *Blind signatures and untraceable payments, Advances in Cryptology Proceedings*, volume 82, n°3, pages 199-203, 1981.
[531] Disponible à cette adresse : http://weidai.com/bmoney.txt.
[532] E. PECK M., *How Bitcoin brought privacy to electronic transactions,* 30 mai 2012. Disponible à cette adresse : http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash, [consulté le 8 avril 2016].
[533] O'LEARY M., *The Mysterious Disappearance of Satoshi Nakamoto, Founder & Creator of Bitcoin*, 5 août 2015. Disponible à cette adresse : http://www.huffingtonpost.com/martin-oaleary/the-mysterious-disappeara_2_b_7217206.html, [consulté le 2 décembre 2016].
[534] *L'évolution du cours du Bitcoin depuis sa création*. Disponible à cette adresse : https://www.mataf.net/fr/bourse/edu/investissement/l-evolution-du-cours-du-bitcoin-depuis-sa-creation, [consulté le 15 août 2018].
[535] Disponible à cette adresse : https://bitcoin.fr/depenser-ses-bitcoins/.
[536] LES ECHOS, *La Blockchain et la loi*, 21 février 2016. Disponible à cette adresse : http://archives.lesechos.fr/archives/cercle/2016/02/21/cercle_154276.htm, [consulté le 15 mai 2016].

exemple, en Algérie, l'article 117 de la loi des finances 2018 dispose que « *l'achat, la vente, l'utilisation et la détention de la monnaie dite virtuelle est interdit* ». C'est la preuve que juristes, informaticiens, acteurs privés et autorités publiques tentent de maîtriser cette technologie innovante afin d'en diminuer les aspects négatifs.

Utilisés comme unité de compte[537], les cryptomonnaies sont un système de transaction utilisant des protocoles chiffrés et décentralisés. Il s'agit d'un instrument de paiement dont la valeur dépend de la confiance qu'on lui porte. Le marché des cryptomonnaies est très florissant mais également très dangereux. En effet, un individu disposant de connaissances techniques suffisantes peut très facilement créer une cryptomonnaie pour ensuite disparaître avec l'argent échangé. La confiance est de rigueur et il est préférable d'utiliser une cryptomonnaie ayant déjà fait ses preuves comme le bitcoin. Toutefois, des cryptomonnaies alternatives ont succédé au bitcoin, ce sont les « *altcoins* ». Il y a par exemple les « *litecoins* » qui s'inspirent fortement des bitcoins tout en permettant des transactions plus rapides.

En somme, les cryptomonnaies sont des monnaies décentralisées, dématérialisées, en partie anonymes, sécurisées et utilisant la cryptographie et la technologie blockchain. Cette dernière permet un contournement des institutions et la mise en place d'une économie collaborative qui aspire à faire disparaître les intermédiaires. Dès lors, une cryptomonnaie fonctionne selon le principe du *peer-to-peer*, soit directement entre utilisateurs. La chaîne de blocs permet de stocker et de transmettre les informations liées à la monnaie, et ce, de manière infalsifiable. Un tel procédé est également utilisé pour les jetons numériques appelés *tokens* (b).

b) Les jetons numériques

Un *token* « *est un actif numérique émis et échangeable sur une blockchain* » présentant plusieurs possibilités. Concrètement, créé par un *smart contract* fondé sur une chaîne de blocs, un *token* permet de créer un nouveau système de valeurs. A l'instar des cryptomonnaies, son transfert sans duplication se fait sur Internet de manière décentralisée sans qu'un tiers n'intervienne. Il présente également les mêmes attributs que les cryptomonnaies puisqu'il est fondé sur les chaînes de blocs enregistrant chaque échange de manière incorruptible. Dès lors,

[537] « *Une unité de compte permet de mesurer la valeur des flux et des stocks de biens, de services ou d'actifs* », Wikipédia.fr.

un *token* a vocation à être infalsifiable, unique et fiable. Il faut différencier les *security tokens* des *utility tokens*. Les premiers concernent les actifs financiers tandis que les seconds ont vocation à être utilisés dans des applications de l'internet décentralisé. D'un point de vue pratique, le *token* est intéressant car tout internaute est en mesure de le créer et de le personnaliser en fonction de ses besoins. C'est ainsi qu'il peut notamment représenter un droit d'auteur, un droit de vote ou un moyen de paiement utilisable dans un écosystème décentralisé. Le *token* est ensuite achetable ou vendable à un prix déterminé par des plateformes d'échange qui prennent en compte l'offre et la demande.

En 2018, il existe plusieurs services utilisant la technologie *token*. C'est le cas de *Storj*, un service *cloud* décentralisé utilisable grâce au *token* nommé *Storjcoin*. L'utilisateur qui souhaite acheter de l'espace de stockage sur le réseau *Storj* doit utiliser le *token Storjcoin* tandis que celui qui souhaite mettre à disposition l'espace libre de son ordinateur est payé en *token Storjcoin*.

Les acteurs économiques et technologiques du monde manifestent un grand intérêt pour le token. Concrètement, le processus de « *tokenisation* » permet de convertir les droits sur un actif en jeton numérique sur une chaîne de blocs, il s'agit donc de la représentation digitale d'un bien. Le secteur économique est inondé d'actifs tels que les biens immobiliers, l'or, les crédits carbone le pétrole… Toutefois, certains de ces actifs ne peuvent pas être transférés ou subdivisés physiquement si bien qu'en la matière les négociations s'effectuent par papier. Ces accords juridiques sont complexes, difficiles à transférer et limités quant à leur suivi. L'idée est donc d'utiliser un système numérique similaire au bitcoin mais lié aux actifs. Le *token* permettra alors des échanges, des transferts sans intermédiaires et une propriété fragmentaire. Par ailleurs, d'autres possibilités comme l'historique des propriétaires, de la valeur du bien, une liste de ses caractéristiques et des restrictions peuvent être envisagées. Le processus de tokenisation qui se met en place (∂) a des effets juridiques qu'il convient d'étudier (ß).

∂) La tokenisation

La tokenisation « *désigne le processus d'inscription d'un actif et de ses droits sur un token afin d'en permettre la gestion et l'échange en peer-to-peer, de façon instantanée et sécurisée sur une infrastructure blockchain* ». Cela concerne donc les security tokens, ces actifs financiers

digitalisés permettent d'effectuer des transactions quasi instantanées. L'idée nouvelle est de permettre l'acquisition d'une portion de part d'une entreprise car il est impossible d'en détenir 0,25 part. Cela est envisageable grâce à la digitalisation des parts. Par ailleurs, le procédé permet un transfert de propriété quasi instantanée lorsque les contractants respectent les règles du smart contract. Le monde des actifs financiers est ainsi passé de l'ère classique à l'ère de la digitalisation en passant par l'ère électronique. Dans les années 1990, cette dernière a connu la suppression des certificats physiques de propriété qui étaient transférés lors des échanges d'actifs.

Mais, les *security tokens* offrent plus d'avantages. Selon l'investisseur Anthony Pompliano, la *tokenisation* d'actifs financiers réduirait les frais de commission, accélérerait l'exécution des transactions en réduisant le nombre d'acteurs impliqués et en automatisant les transactions et exposerait les transactions à une base mondiale d'investisseurs. C'est ainsi que les marchés pourraient être ouverts à plus de participants et offrir plus d'échanges. En 2017, sur le site du *Nasdaq*, l'exemple fictif donné par l'entrepreneur Addison Cameron Huff. Il met en avant un grossiste de diamants propriétaire de 15 millions de dollars de diamants et un individu qui souhaiterait investir quelques milliers de dollars sans avoir à gérer la logistique qu'impliquerait un transfert physique, mais en ayant la capacité de revendre ses parts à d'autres individus que le propriétaire initial.

Les *tokens* offrent ainsi une démocratisation des actifs financiers. L'étude publiée sur le site du Nasdaq fait la différence entre les actifs incorporels, les actifs corporels fongibles et les actifs corporels non fongibles. Les premiers n'ont pas d'existence physique et peuvent facilement faire l'objet d'une t*okenisation*. Il peut s'agir de brevets ou de droits d'auteur. La conversation des deuxièmes en token est également facile puisqu'ils peuvent être divisés en plusieurs unités. Les troisièmes ne se prêtent pas autant au processus car il n'est pas possible d'échanger un *token* contre une partie du bien.

Les échanges de marchandise se sont déjà passés des documents physiques en utilisant les transactions électroniques qui nécessitent l'intervention de tiers de confiance et supposent de très gros frais généraux. Le *token* semble être la prochaine phase de cette numérisation des actifs. L'objectif est de maximiser la rapidité, la sécurité et la facilité des transferts.

Enfin, les *tokens* sont émis à la suite d'une *ICO* qui est en une sorte de levée de fonds. Pendant une durée déterminée un émetteur attribue des jetons numériques via une blockchain en échange de monnaies physiques ou virtuelles. Des unités numériques spécifiques à un nouveau projet sont alors émises. Ce genre de vente est possible grâce à une large publicité via Internet et le Darknet ou dans des conférences. Intervient alors un acheteur aussi appelé investisseur qui se voit attribuer le jeton numérique après avoir payé ou fourni un service, et un vendeur aussi appelé développeur qui crée le jeton numérique via la *blockchain*. La création d'un jeton numérique et d'une chaîne de blocs a donc des conséquences juridiques non négligeables (ß).

ß) Les conséquences juridiques

Le *token* est un jeton numérique lié à une signature électronique qui fonctionne selon le protocole de la *blockchain* qui permet d'identifier les transactions. Chaque *token* associé à une adresse de la *blockchain* et ne peut être transmis que par le possesseur de la clé privée liée à l'adresse. Ce domaine *sui generis* amène à s'interroger sur le régime juridique applicable et sur sa légalité. En effet, en droit la monnaie est liée au paiement, c'est-à-dire à l'extinction d'une obligation. En France, la monnaie officielle est l'euro. Toutefois les parties peuvent convenir d'utiliser une autre monnaie en dérogeant à cette règle conformément au droit européen.

Le principal enjeu juridique concerne la cohérence des *tokens*. En effet, pour les bitcoins il y a toujours de la cohérence et pas d'exception grâce au respect des règles mises en place par le logiciel. Pour les *tokens* qui représenteraient des valeurs de la vie réelle, la donne est différente. En effet, l'aléa de la vie peut créer des imprévus : des diamants volés, une maison incendiée… Dès lors, il faut que le *token* reste entièrement lié au bien réel. Par exemple, si un lingot d'or est extrait d'un coffre-fort, quelles seront les conséquences pour le *token*. Qui peut garantir que la valeur du token reste liée aux lingots d'or qui sont censés être dans le coffre plutôt que celle de ceux qui se trouvent dans le coffre ? Qui va supporter le risque ?

Le *token* a vocation à être utilisé pour les meubles incorporels tels que les brevets, les noms de marque, les droits d'auteur qui sont des actifs incorporels. Dénués de forme physique, ils peuvent facilement s'intégrer dans un système numérique de chaîne de blocs. Le défi consiste à faire en sorte que le modèle juridique de transfert actuel s'applique au modèle des *blockchain*s. L'idée est de vérifier l'authenticité d'un bien et faciliter la vérification du vrai propriétaire.

Pour les transactions immobilières il permettrait de se passer d'un notaire ou pour les œuvres d'art d'un commissaire-priseur. Pour les biens fongibles[538] comme le blé ou l'eau qui peuvent être divisées en unités, la conversion en *token* est facile dans le mesure où le bien fongible est standardisé et n'a rien d'unique. Les cryptomonnaies sont donc des *tokens* fongibles, un bitcoin peut être échangé avec un autre bitcoin. Mais la conversion des biens non fongibles[539] nécessite une autre approche en raison de leurs caractéristiques uniques. Un collectionneur de timbres connaît la valeur du « *one cent magenta de Guyane britannique* » et ne l'échangerait pas contre un autre timbre quelconque. C'est la même chose pour les *tokens* non fongibles qui sont donc indivisibles. En apparence, les *tokens* non fongibles n'ont pas de réel intérêt. Pourtant, ils commencent à se démocratiser notamment en matière de données administratives. Ils pourraient être utilisés pour combler les lacunes informatiques et les difficultés liées au stockage de papier, pour envisager un archivage sécurisé sur le long terme. Tel pourrait être le cas pour le stockage des diplômes, des certificats de naissance ou autre (2).

2. Le droit saisi par la *blockchain*

Défendre l'idéologie *smart contract* c'est adhérer à une philosophie ultra libérale qui prône une efficacité économique des droits du créancier, une réduction des coûts et surtout un éloignement de l'Homme afin d'écarter les faiblesses humaines et la notion de bonne foi. Il s'agit alors pour le droit d'appréhender un tel concept sans ralentir l'activité économique qu'il est susceptible d'apporter. Une telle approche juridique est nécessaire pour encadrer les conséquences positives et négatives des smart contrat qui ne sont pas encore toutes connues.

Définis par Wikipédia comme des « *protocoles informatiques qui facilitent, vérifient et exécutent la négociation ou l'exécution d'un contrat* », les *smart contracts* permettent une réduction des coûts de transaction des contrats. C'est le juriste et cryptographe américain Nick Szabo qui est à l'origine de l'expression en 1993 mais aussi du « *Bit Gold* », le précurseur du bitcoin. Il aspire alors à faire évoluer le droit des contrats, en concevant et appliquant sur Internet des protocoles de commerce électronique. En s'inspirant de cryptographes comme David Chaum, il souhaite utiliser des mécanismes de sécurité numérique tels que des protocoles

[538] Ce type de bien se caractérise par son appartenance à un genre si bien que chaque unité est interchangeable. Un kilogramme de plomb est interchangeable avec un autre.
[539] Ce sont des biens ayant des attributs communs mais une identité propre.

cryptographiques afin d'exécuter et vérifier une opération contractuelle. Ses travaux ont été bien reçus par la communauté puisque d'autres informaticiens, comme Mark Miller, ont mis en avant l'intérêt des *smart contracts* en ce qui concerne la sécurité et l'identification grâce à la signature électronique.

Concrètement, la mise en place de *smart contracts* s'appuie sur la technologie Blockchain qui permet de garantir l'intégrité des termes et conditions d'un contrat qui s'exécute. L'exécution se fait grâce à un réseau *peer-to-peer* faisant office de registre et exécutant le changement de propriété de manière automatique en fonction des règles prévues initialement. Chaque nœud se charge de vérifier et transmettre l'information aux autres nœuds du réseau et ce sont des données extérieures qui contribuent à la modification des données. En réalité, la cryptomonnaie fonctionne selon ce même principe de registres. La monnaie est considérée comme un titre de propriété transmis intelligemment par contrat. Mais, les *smart contracts* incluent d'autres instruments financiers comme des contrats d'assurance, des obligations, des actions ou des transactions quelconques. En tout état de cause, cela va garantir une surveillance des événements qui conditionnent les règles de ce type de contrat. D'un point de vue juridique, toujours considérés comme de simples protocoles informatiques, les *smart contracts* présentent de multiples intérêts et posent de nombreuses questions ayant amené à des discussions dans plusieurs pays. Par ailleurs, ce genre de contrat peut être exploité par les hackeurs qui seraient capables de détourner des sommes d'argent, ou profiter d'un service sans le payer.

Ainsi, juridiquement les *blockchains* sont très innovantes. Elles offrent de nouvelles possibilités en matière de contrats (a) mais aussi de preuves (b).

a) Les *smart contracts*

Traduit par contrat intelligent, le *smart contract* se fonde sur un syllogisme c'est-à-dire un raisonnement mettant en relations plusieurs propositions[540]. Ce genre de contrat est automatique et ne nécessite pas d'intervention humaine. Ce sont des algorithmes qui vont organiser les relations contractuelles grâce à un programme qui aura préalablement envisagé les différentes possibilités exécutables par le smart contract. Ce dernier ne jouit pas d'une autonomie totale.

[540] If ➔ then. Si ➔ donc.

Fondamentalement le smart contract n'a rien de révolutionnaire, il s'agit juste de l'assemblage de plusieurs technologies qui existent depuis des dizaines d'années (∂). Certains, un peu trop enthousiastes, aimeraient remplacer l'ensemble des contrats par des *smart contracts* et des algorithmes. Toutefois, une éventuelle « *smart contractualisation* » ferait face à des limites juridiques, politiques et technologiques (ß).

∂) Le fonctionnement des *smart contracts*

Les « *ethereum* » permettent la création de smart contrat. Il s'agit de constituer un programme quelconque afin qu'il soit exécuté par l'ensemble des ordinateurs de la *blockchain d'Ethereum*. Par exemple, un programme peut être défini pour la conclusion d'un contrat ou la création d'une entreprise dans la *blockchain*. Dès lors, grâce à un algorithme le programme déterminera les parts de cette entreprise et l'influence de chaque propriétaire de parts. Si un contrat est conclu dans la *blockchain,* il tournera sur l'ensemble du réseau par le biais des ordinateurs. Un programme permettrait de signer un contrat électronique dans la *blockchain* d'*Ethereum* sans passer par un avocat ou un notaire. Cette capacité à gérer de tels contrats sous forme de programmes informatiques permet également à *Ethereum* de faire office de cryptomonnaie.

Premièrement, les *smart contracts* sont autonomes car après leur lancement, les modifications ne sont plus possibles sauf si elles ont été prévues préalablement. Deuxièmement, ils ont un aspect financier puisqu'ils permettent des échanges de fonds. Troisièmement, ils sont traçables puisqu'ils fonctionnent selon un protocole *blockchain*. Toutefois, un programme informatique est incapable de prendre en considération les événements du monde réel. Un *smart contract* est en mesure de vérifier un paiement en bitcoin par exemple, mais incapable de vérifier si un objet a été livré par la poste.

Pour plus d'efficacité, le recours à des oracles de *blockchain* est nécessaire. Il s'agit d'une entité de confiance appartenant au réseau informatique et faisant office d'intermédiaire entre le smart contract et le monde physique. L'objectif est que le contrat ne soit pas limité aux informations de la *blockchain*. Il est possible de citer *Chainlink* ou *Augur* deux réseaux d'oracles décentralisés, et *Oraclize* un réseau d'oracle centralisé. Les premiers sont moins communs en raison du fait qu'il n'est pas possible de vérifier la provenance d'une information mais

permettent d'échapper à la dépendance d'un acteur central tel qu'un gouvernement ou une entreprise privée pouvant modifier les informations envoyées. La confiance en l'oracle dépendra donc de la confiance accordée à cette entité. En tout état de cause, l'entité de confiance et les contrats intelligents ont des conséquences juridiques qu'il convient d'étudier (ß).

ß) Les conséquences juridiques

Les *smart contracts* sont des programmes informatiques autonomes exécutés par un réseau exploitant une blockchain. Ils se sont démocratisés en 2013 grâce à *Ethereum* qui permet la programmation automatique de certaines fonctionnalités. Inéluctablement, ces contrats intelligents, qui aspirent à garantir une exécution autonome des programmes informatiques dans de nombreux domaines, sont liés au droit. La pratique a démontré que les caractéristiques de ces contrats intelligents pouvaient avoir de nombreuses conséquences juridiques. Ces enjeux numériques amènent à se poser des questions concernant les concepts juridiques qui pourront s'adapter, concernant les pratiques qui pourront en découler et concernant les nouvelles règles à adopter ?

Même s'il est encore juridiquement limité par des questions probatoires, le *smart contract* est un sujet du droit qui doit être régulé rapidement. Une phase de transition juridique contraint les entreprises économiques à établir des stratégies de gestion du risque en limitant l'utilisation des *smart contrats* par des clauses. Ces dernières sont nécessaires pour compenser les *smart contracts* qui ne peuvent pas gérer l'imprévisible comme un problème réseau ou un piratage. En outre, les facteurs psychologiques humains ne sont pas pris en compte par les *smart contracts*. C'est notamment le cas pour les notions de bonne foi, de légitime, de manifeste, de raisonnable.

L'innovation suppose d'accorder une chance aux *smart contracts*, et la précaution impose un contrôle et une prise en compte du Droit après l'intervention de l'Etat. Ils méritent d'être élargis en raison de l'optimisation contractuelle qu'ils garantissent à tous les stades du contrat. Le *smart contract* est simplement une modalité d'exécution d'un contrat physique à la différence que c'est un programme informatique qui garantit son exécution de manière autonome. L'article 1127-1 du Code civil dispose que « *quiconque propose à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, met à disposition les*

stipulations contractuelles applicables d'une manière qui permette leur conservation et leur reproduction ». Ce genre de contrat est donc reconnu et autorisé par le droit français. En effet, d'autres règles contractuelles ont vocation à s'y appliquer. Par exemple, en matière civile d'après l'article 1359 du Code civil le contrat « *portant sur une somme ou une valeur excédant un montant fixé par décret doit être prouvé par écrit sous signature privée ou authentique* ». Or, l'article 1365 du Code civil précise que « *l'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support* ». Logiquement, les programmes informatiques *des smart contracts* sont assimilables à la précision apportée par ce texte.

Au stade de la formation du contrat, ils permettent de réduire les coûts, les délais et garantissent une plus grande sécurité grâce à l'utilisation de la technologie *blockchain*. Cette dernière permet d'attester la remise d'un document à un moment précis à l'instant où il entre dans la chaîne de bloc. Ce genre de mécanisme peut par exemple être utile pour établir le point de départ d'un délai de rétraction.

Au stade de l'exécution du contrat, l'entrée d'une information dans la chaîne de bloc autorise la transmission automatique de fonds, sans intervention humaine. Tel pourrait être le cas pour un architecte mandaté par une grande entreprise qui aurait besoin de matériels. Il lui suffirait de mettre la facture dans la chaîne de blocs pour enclencher l'envoi des fonds. Même principe, pour l'envoi automatique de fonds à une date prédéterminée.

Enfin, le fait que le *smart contract* ne puisse pas être modifié après son lancement amène également à des questions juridiques. En effet, en matière de contrat des situations telles que la rétraction d'une des parties, la mauvaise exécution ou l'inexécution sont récurrentes. Dès lors, pour cette dernière, les articles 1217 et suivants du Code civil ont-ils vocation à s'appliquer ou au contraire, faut-il envisager un cadre spécifique aux smart contracts ? En outre, le fait de se baser sur un programme peut amener à des dysfonctionnements techniques qui seraient susceptibles d'engager la responsabilité des programmeurs informatiques. En droit des contrats les nouvelles technologies ont donc un rôle à jouer. C'est également le cas en matière de preuve (b).

b) Une finalité probatoire

Les possibilités offertes par la technologie *blockchain* sont incroyables. Par exemple, en matière de droit d'auteur, « *l'auteur d'une oeuvre de l'esprit jouit sur cette oeuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous* », mais le titulaire de ce droit doit être en mesure de prouver qu'il est à l'origine de l'œuvre. Cela peut s'avérer indispensable lorsque l'œuvre est contrefaite par exemple. Le premier auteur devra prouver que c'est lui qui est victime de contrefaçon et non l'inverse. Dans ce contexte, les règles classiques du droit de la preuve ont vocation à s'appliquer : « *celui qui réclame l'exécution d'une obligation doit la prouver* » et « *qu'il incombe à chaque partie de prouver, conformément à la loi, les faits nécessaires au succès de ses prétentions* ». Or, l'article 113-1 du Code de propriété intellectuelle prévoit que « *la qualité d'auteur appartient, sauf preuve contraire, à celui ou à ceux sous le nom de qui l'œuvre est divulguée* ». Ainsi, le vrai auteur devra prouver par tous moyens qu'il est à l'origine de l'œuvre. Généralement la preuve se fait par le biais d'un formaliste lourd impliquant des officiers ministériels et des agents assermentés. Une meilleure fluidité pourrait alors être envisagée grâce à la technologie *blockchain*. Les protocoles *blockchain*s fonctionnent selon une fonction mathématique à sens unique qui établit à partir d'une valeur d'entrée, une valeur de sortie appelée « *hash* » qui est en fait un enchaînement de caractères alphanumériques qui ne semblent rien dire. Cette technique dite de hachage permettrait d'intégrer une œuvre dans la blockchain et de n'en conserver dans que le *hash*. Une seule modification de ce dernier entraîne une valeur de sortie distincte de la valeur initiale. Il suffira alors de vérifier le *hash* et l'œuvre pour s'assurer de son intégrité.

Ensuite, une *blockchain* publique représente toutes les transactions effectuées en donnant l'heure et la date de celles-ci. Toutefois, l'article 1377 du Code civil prévoit que « *l'acte sous signature privée n'acquiert date certaine à l'égard des tiers que du jour où il a été enregistré, du jour de la mort d'un signataire, ou du jour où sa substance est constatée dans un acte authentique* ». Dès lors, en la matière le droit civil a vocation à évoluer. L'auteur de l'œuvre pourra établir la date de l'intégration de l'œuvre dans la chaîne de blocs même si cela ne garantit pas qu'il est à l'origine de cette œuvre. Une telle démarche pourrait en revanche garantir une traçabilité de tous les actes juridiques postérieurs comme un prêt, un don, ou une cession de droit. Par ailleurs, une sûreté qui porterait sur l'œuvre pourrait être intégrée dans la chaîne pour garantir une meilleure publicité. Logiquement, l'utilisation d'un tel protocole permettrait de se

passer de personnes extérieures comme des huissiers ou des sociétés privées et assurer une diminution des coûts de transaction.

En 2018, la b*lockchain* n'a pas encore été reconnue comme preuve légale ou judiciaire. Elle est intégrée à la preuve littérale et aux dispositions du Code civil qui la régissent. Dès lors, la *blockchain* pourrait être assimilée à l'écrit électronique qui selon l'article 1366 du Code civil « *a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane* ». Cela suppose donc que l'auteur de l'écrit soit identifiable et que l'écrit électronique ait été « *conservé dans des conditions de nature à en garantir l'intégrité* ». Cette dernière pourrait être assurée grâce au hachage. Toutefois, il est difficile de garantir l'identité de l'auteur de la transaction dans la mesure où la *blockchain* se fond sur un anonymat grâce aux clés privées et publiques. Ces dernières permettent une authentification de l'auteur mais pas une identification.

L'authentification est également possible grâce à la signature électronique qui s'est aujourd'hui démocratisée. Cela amène à se demander si l'article 1367 alinéa 2 du Code civil permet de donner une valeur juridique à la signature électronique via une blockchain. Là encore, le Code civil fait part d'un « *procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* », ce qui pose problème pour les *blockchains* publiques. Par conséquent, de telles règles de preuve méritent d'être adaptée à la technologie *blockchain*. Néanmoins, les opérations de la chaîne de blocs dépassant les frontières, les modalités de détermination d'un tel régime supposent une élaboration par le biais d'une convention internationale. Sans accord, il est possible de redouter la mainmise juridique d'une puissance étatique sur les *blockchains*. L'exemple des Etats-Unis et de leur appropriation d'Internet devrait pousser la communauté internationale à légiférer en la matière.

Finalement, pour toutes ces raisons la technologie *blockchain* s'avère utile juridiquement. Cependant, en 2018, elle n'a pas encore vocation à remplacer les règles de droit existantes, notamment en ce qui concerne la preuve. Le législateur dispose aujourd'hui d'une grande marge de manœuvre pour fixer un cadre sans limiter les innovations offertes par la *blockchain*. Le

bitcoin n'échappe pas à ce cadre juridique[541] (§2).

§2) La plus populaire des cryptomonnaies : le bitcoin

Le bitcoin est un terme anglais composé des mots « *bit* » et « *coin* » désignant respectivement l'alternative binaire entre 0 et 1 et la pièce de monnaie. Il s'agit d'une cryptomonnaie fondée sur un système de paiement *peer-to-peer*.

En 1992, Tim May est également un précurseur puisque dans son Manifeste crypto-anarchiste il avance que « *la décennie prochaine apportera suffisamment de vitesse en plus pour rendre cela économiquement faisable et impossible à stopper* ».

L'aspect pratique du bitcoin est réel. Grâce à cette cryptomonnaie, il est possible de payer n'importe où dans le monde sans frais de change et avec des frais de transaction très faibles comparés aux frais bancaires liés aux paiements électroniques. Un autre avantage découle de cela puisque le faible montant des frais liés aux opérations permet d'envisager la multiplication des micropaiements. Ce paragraphe permettra de présenter le bitcoin (A) et d'en expliquer le fonctionnement (B).

A) La présentation du bitcoin

L'argent n'est qu'un système de comptabilité. C'est un moyen de savoir qui doit quoi à qui, d'enregistrer des transactions, de la valeur en numérique. Il fallait quelqu'un pour être le fournisseur central, une tierce personne qui garantit que l'argent est réel. Depuis des centaines d'années ce sont les Etats qui émettent l'argent. Le bitcoin est le premier à vraiment faire fonctionner l'échange de valeurs décentralisées. Tout est enregistré dans un grand livre ouvert dans un système de consensus collectif qui permet d'éviter les frais mais aussi tous les risques qu'impliquent de centraliser des informations comme la corruption par exemple. Le bitcoin prend la fonction de tierce personne et l'automatise pour la mettre dans un grand livre comptable mis en ligne, c'est la *blockchain*. Chaque bitcoin est comptabilisé si bien qu'il ne

[541] CASTRO V., *Impôts & bitcoin : comment bien déclarer ses cryptomonnaies, notre guide en 10 questions*, 2 février 2018. Disponible à cette adresse : https://www.numerama.com/business/325205-impots-bitcoin-comment-bien-declarer-ses-cryptomonnaies-notre-guide-en-10-questions.html.

peut pas y avoir de contrefaçon. L'approvisionnement d'argent est contrôlé par un nœud faisant partie de la *blockchain* qui est entièrement distribuée et décentralisée. Il n'y a pas de dépôt central de l'information puisque la *blockchain* est sur des milliers d'ordinateurs. Chaque transaction est enregistrée de manière permanente sur la *blockchain* et ne peut plus être modifiée, les identités des possesseurs sont dissimulées, les portefeuilles cryptés. En somme, il n'est pas possible de savoir qui dépense ses bitcoins. Toutefois, chaque bitcoin a un historique comportant l'ensemble des adresses par lequel il est passé. L'une des fonctions permettant l'activité du bitcoin est le minage. Il s'agit de la maintenance des *blockchain*s effectuée par de nombreux ordinateurs situés à travers le monde. Ils vérifient l'information, l'actualisent et s'assurent de sa fiabilité. Pour ce faire, ils sont soumis à un test informatique très compliqué qui consiste à trouver un nombre en étant en compétition avec tous les autres ordinateurs. Toutes les dix minutes, les ordinateurs les plus performants sont alors récompensés en bitcoin. L'information est ensuite transmise à l'ensemble des ordinateurs indépendants faisant partie du réseau qui vont à leur tour contrôler la véracité de l'information. Le plus important ce n'est pas la monnaie mais la *blockchain*.

Selon Charlie Shrem le cofondateur de *BitInstant* et vice-président de la fondation Bitcoin, « *le Bitcoin c'est du cash avec des ailes, c'est la possibilité de prendre une transaction locale et de la rendre globale. Et c'est pourquoi le Bitcoin va renverser l'infarctus financier* ». Il y a beaucoup de risques légaux autour des transmissions d'argent. Selon Satoshi Nakamoto, la circulation totale de bitcoin programmée dans le système est de 21 000 000 bitcoins mais chaque bitcoin peut lui-même être divisé en plusieurs parties différentes et s'étendre avec son usage.

Pouvoir transférer de l'argent de manière électronique est un acquis pour les possesseurs d'un compte bancaire mais permet également de faire entrer les autres dans le système financier par le biais d'un téléphone portable ou d'un ordinateur. Dans certains pays, l'envoi d'argent est impossible et c'est la raison pour laquelle les personnes utilisent *Western Union*, une entreprise spécialisée dans le transfert d'argent. Mais, ces transferts sont très coûteux : entre 5 et 10% de la somme envoyée est prélevée. Le Bitcoin ne prend pas en compte les frontières si bien que l'envoi de monnaie est possible d'un pays à un autre. Il s'agit d'une des principales options du bitcoin. Toutefois, contrairement aux transferts standards qui sont instantanés, une *blockchain* nécessite des vérifications qui prennent environ quinze minutes pour que la transaction soit

validée par le réseau. Ce sous-paragraphe permettra de présenter l'histoire du bitcoin (1) et sa réputation sulfureuse (2).

1. L'histoire du bitcoin

Bill Gates, le fondateur de Microsoft, a qualifié le bitcoin de « *tour de force technologique* », mais le projet n'a pas été facile à concrétiser. Le créateur du bitcoin, Satoshi Nakamoto, est une énigme toujours pas résolue puisque à ce jour son identité n'a toujours pas été dévoilée.

Apparu de nulle part en 2008, il s'agit pour certains d'une personne, et pour d'autres d'un groupe lié aux *cypherpunks*. Il s'est fait connaître grâce à une liste d'e-mails cryptés qu'il a utilisée pour promouvoir le bitcoin et a énormément communiqué pendant quelques années durant lesquelles il a été considéré comme quelqu'un qui avait la folie des grandeurs. Au départ, peu de personnes s'intéressent au projet et c'est la raison pour laquelle l'identité du créateur n'est pas connue. En tout état de cause, il s'agit d'une personne très douée en cryptographie qui a tout fait pour séparer le bitcoin de tout ce qui pouvait l'identifier. Hal Finney, un développeur de *PGP* embauché juste après Phil Zimmerman, a été le premier à croire au bitcoin et a travaillé avec Nakamoto. Pendant des semaines, ils travaillent ensemble et montent le système qui va permettre à Nakamoto d'envoyer la toute première transaction bitcoin à Hal Finney. Le fait de ne pas connaître l'identité du créateur a permis aux utilisateurs d'avoir une meilleure liberté et d'utiliser le Bitcoin comme ils le souhaitaient. Le 31 octobre 2008, Satoshi Nakamoto publie sur le site *metzdowd.com* un manifeste de huit pages mettant en avant cette nouvelle monnaie qu'est le bitcoin. Il s'agirait d'une nouvelle technologie aspirant à changer le monde. Le 3 janvier 2009, le block 0 de la *blockchain* est créée et le premier bitcoin exploité. Il s'agit de la date officielle de la création du bitcoin. Le 12 janvier 2009, la première transaction est conclue entre Satoshi Nakamoto et Hal Finney. Le 6 février 2010, *DWDOLLAR* devient le premier marché réel du bitcoin et donne une valeur à la monnaie. Le 22 mai 2010, un programmeur nommé Hanyecz échange 10 000 Bitcoins contre deux pizzas chez Papa John's en Floride. A cette période, le taux de change de cette monnaie presque inconnue était ridicule puisqu'un bitcoin équivalait à quelques centimes de dollars, 0,003 pour être précis. L'idée d'échanger 10 000 unités de code informatique contre des pizzas a été perçu comme une réelle avancée. L'année 2010 connaît une multiplication du nombre des transactions et la valeur totale du Bitcoin dépasse le million de dollars le 6 novembre.

Fin 2011, grâce à *BitPay* un fournisseur de services, des milliers de partenariats sont conclus entre des marchands et le bitcoin. La cryptomonnaie se démocratise et sa valeur augmente. Au départ, ce sont uniquement des investisseurs de la Silicon Valley qui s'y intéressent mais la dynamique décolle rapidement et les libertaires, les informaticiens et les utilisateurs sont impliqués dans le réseau. Plus il y avait de monde, plus le réseau était fort. A l'automne 2013, sa valeur passe de 125$ à 1100$. La valeur de sa capitalisation boursière augmente de manière exponentielle entre octobre et décembre 2013, passant de 1,5 milliard de dollars à 13,5.

En 2014, le bitcoin perd la confiance des utilisateurs en raison du manque de sécurité dû aux vols de bitcoin et de la mauvaise gestion des fonds. La volatilité du prix du bitcoin a attiré l'attention. Le cours s'effondre durant toute l'année 2014 jusqu'au 11 décembre date à laquelle *Microsoft* annonce son partenariat avec *BitPay* en acceptant le bitcoin comme mode de paiement. Dans un communiqué, le plus grand distributeur d'ordinateurs au monde déclare que « *nous nous attendons à ce que cette croissance se poursuive et que les gens puissent utiliser Bitcoin pour acheter nos produits et services, ce qui nous permet d'être à la pointe de cette tendance* ». Le timing est parfait puisque le système était dans une mauvaise posture. Le bitcoin a été contraint d'accepter que ceux qui dirigent le monde ait leur point de vue à donner. Des garde-fous réglementaires ont été nécessaires pour l'ensemble des cryptomonnaies. Pour les moins libertaires, la régulation a été cruciale pour la survie des monnaies virtuelles. Pour autres qui veulent un monde où les transactions seraient mondialisées et gratuites, les Etats ne devraient pas intervenir. Les régulations empêchent les innovations mais elles permettent d'accroître la confiance qu'un utilisateur peut accorder à un système ; c'est ce qui s'est passé avec le bitcoin. Les utilisateurs ont souhaité une saine régulation permettant d'utiliser le bitcoin de manière productive. Au printemps 2015, le bureau du procureur de New York Benjamin Lawsky annonce une version finale de la licence bitcoin, la *BitLicence.* Désormais, une entreprise doit demander une approbation pour pouvoir faire du profit grâce au bitcoin. Il y a une volonté de protéger l'utilisateur, de garantir une cybersécurité efficace et de s'assurer que les sociétés soient capitalisées afin qu'elle subsiste sur la durée. Cette régulation a donné de la légitimité au projet bitcoin. Finalement la *BitLicence* retire le doute consistant à se demander comment ce secteur allait être régulé. Une telle légitimité est nécessaire dans le mesure où cette cryptomonnaie ne jouit pas d'une bonne réputation (2).

2. Une réputation sulfureuse

En 2011, un nouveau chapitre est ouvert avec le marché *Silkroad* qui est considéré comme le *Big Bang du bitcoin* qui a monétisé le Darknet. Ce site du Darknet à l'interface simplifiée utilisait le bitcoin en raison de son anonymat et en trois ans des millions de bitcoins ont été échangés contre des services et des articles illégaux. En théorie, il s'agit d'un site d'échange anonyme utilisant une monnaie anonyme. Alors qu'est arrêté à San Francisco et que ses serveurs sont à l'étranger, Ulbricht est jugé dans le district sud de New York. Cette singularité procédurale est certainement liée au bitcoin. En effet, New York est la ville dans laquelle la majorité des régulations financières est traitée, et dans laquelle le procureur Preet Bharara et le sénateur Charles Schumer ont fermement combattu le bitcoin. D'aucuns estiment que le procès d'Ulbricht est le procès du bitcoin. La menace pour les marchés était trop importante. Cette monnaie permettant d'effectuer des transactions librement, sans régulation ou contrôle, effrayait. Ulbricht fait figure d'exemple en étant condamné à la prison à vie. Cette sentence est sévère pour dissuader les autres utilisateurs d'utiliser des marchés non régulés. Des millions de bitcoins sont alors saisis par l'Etat américain afin d'être revendus aux enchères. Cette procédure a légitimité l'utilisation du bitcoin en tant que monnaie.

Les bitcoins, notamment avec le système d'*escrow*, permettent-ils de faciliter le blanchiment d'argent à tel point qu'il faudrait les interdire. Nombreux sont les discours extrêmement alarmistes mais ce n'est pas l'outil qui doit être condamné mais l'usage qu'il en est fait. Le bitcoin permet l'achat de drogue donc selon certains il faudrait l'interdire. La poste permet la livraison, faudrait-il pour autant interdire la poste ?

En 2014, Charlie Shrem est accusé de blanchiment d'argent après qu'il a permis à des utilisateurs de transférer des bitcoins en dollars par le biais de sa société *BitInstant,* et de trafic de drogue en achetant de la drogue en ligne sur le Darknet. Il a en fait vendu des bitcoins à Ulbricht qui les a revendus à des trafiquants de drogue de *Silkroad*. Pour cette raison, Charlie Shrem encourt une peine de 20 ans de prison. Le lendemain de son arrestation, une conférence sur le bitcoin a lieu à New York pour annoncer la mise en place d'un cadre pour les entreprises de New York utilisant le bitcoin. Les autorités veulent éviter un 11 septembre 2.0 qui serait en partie causé à cause du bitcoin. Le terrorisme peut utiliser le bitcoin, mais tout le monde le peut, comme pour les téléphones portables, les voitures ou Internet. Il n'est donc pas nécessaire

d'étouffer la croissance de ce secteur. En effet, il paraît difficile de limiter l'expansion de cette cryptomonnaie qui fonctionne de la même manière que les autres chaînes de blocs (B).

B) Le fonctionnement du bitcoin

La *blockchain* du bitcoin est partagée par l'ensemble du réseau, elle est publique. Il est possible d'en télécharger une copie avec le logiciel *Bitcoin Core* ou de la parcourir via des sites comme *blockchain.info.* Sur ce dernier, on apprend par exemple qu'il y a des dizaines de milliards de bitcoins en circulation et qu'en juin 2018 un Bitcoin vaut à peu près 7300 dollars américains alors qu'il en valait 10 début 2011. L'accueil du site blockchain.info montre les derniers blocs du réseau. Le 13 juin 2018, la *blockchain* du bitcoin, le livre de compte du bitcoin en est au bloc, au livre n°527192 avec 892 transactions pour un total de 3000 bitcoins échangés. Lorsqu'un bloc fait 1Mo, il est plein et un mineur doit créer un nouveau bloc.

En 2018, il est très facile d'acheter des bitcoins. Le site « *How to Buy Bitcoins*[542] » référence les marchés permettant d'en acheter ou d'en vendre. A titre d'exemple, le site *Paymium*[543] est un marché français, le site *Kraken*[544] est l'un des plus populaires, le site *Coinbase*[545] permet d'acheter des bitcoins par carte de crédit et il en reste plein d'autres. Sur *Coinbase* il suffit de créer un compte soit sur son ordinateur, soit sur son téléphone portable, et d'ajouter une méthode de paiement, soit par virement bancaire, soit par carte bancaire. Une fois le choix de la méthode de paiement effectué, il suffit de se rendre sur la page « *achat/vente*[546] », choisir une cryptomonnaie, sélectionner sa méthode de paiement et indiquer le nombre de bitcoins voulu. Des frais seront prélevés par le site pour chaque opération. Ensuite, les bitcoins ou bits[547] pourront être stockés sur les différents portefeuilles hébergés par le site. Il faut en effet conserver ses bitcoins sur l'équivalent d'un portefeuille au format électronique. Ces portefeuilles ne stockent pas réellement des bitcoins mais des paires de clés qui vont garantir l'accès à l'argent. Le site officiel du bitcoin[548] explique de manière très claire le fonctionnement des portefeuilles et les divise en quatre catégories. La première, comprend les portefeuilles

[542] Disponible à cette adresse : https://howtobuybitcoins.info/#!/EUR.
[543] Disponible à cette adresse : https://www.paymium.com/.
[544] Disponible à cette adresse : https://www.kraken.com/.
[545] Disponible à cette adresse : https://www.coinbase.com/.
[546] « *Buy/sell* ».
[547] 1 Bit = 0,000001 Bitcoin.
[548] Explications disponibles à cette adresse : https://bitcoin.org/fr/choisir-votre-porte-monnaie.

accessibles via une application mobile, la deuxième ceux accessibles via un ordinateur de bureau, la troisième ceux accessibles sur une sorte de clé USB et la dernière ceux accessibles en ligne comme sur *Coinbase*. La troisième semble très sécurisée puisque personne ne peut se connecter au portefeuille sans le support matériel qu'est la clé USB tandis que la dernière très pratique mais peu sécurisée sur des sites en ligne vulnérables.

À titre d'exemple, *Electrum*[549] est un portefeuille accessible via un ordinateur de bureau proposant plusieurs types de portefeuilles. Il y a le « *standard wallet* » qui est un portefeuille normal mais peu sécurisé, le « *wallet with two-factor authentification* » qui permet d'activer une double authentification en utilisant un service externe payant « *Trustedcoin*[550] » et le « *multi-signature wallet* », un portefeuille verrouillé par trois clés au lieu d'une seule. En tout état de cause, *Electrum* génère une clé publique communicable à tout le monde et une clé privée permettant de signer les transactions et de prouver son identité. Cette clé privée, générée à partir d'une liste de mots, est également sécurisée par un mot de passe. Concrètement, la personne qui connaît la liste de mots, a accès aux clés et donc de l'argent. Sur *Electrum* s'affiche ensuite une interface avec l'ensemble des transactions faites avec ce portefeuille, la quantité d'argent stocké dans ce portefeuille et la possibilité d'envoyer de l'argent. Pour ce faire, il suffit de copier l'adresse du destinataire, de fixer le montant de l'envoi et des frais. Plus l'utilisateur paie de fais, plus vite sa transaction sera traitée par l'ensemble des nœuds du réseau. S'il décide de ne pas payer de frais, la prise en compte de la transaction pourrait être longue. Lors d'une transaction, le paiement doit être confirmé par au moins six nœuds du réseau, plusieurs blocs doivent être ajoutés à la chaîne. A défaut, le paiement est considéré comme douteux. La liste des sites acceptant les bitcoins est donné sur http://usebitcoins.info.

En France, l'achat de bitcoin peut se faire sur bitboat.net une plateforme d'échange de Bitcoins en allant payer au bureau de poste le plus proche mais il existe d'autres sites d'achat. Il est nécessaire de créer un compte avec un nom d'utilisateur et un mot de passe. Une fois les Bitcoins obtenus, l'utilisateur les transfert sur son portefeuille (1) et peut les utiliser après une validation de la transaction grâce à une paire de clés privée et publique (2).

[549] Disponible à cette adresse : https://electrum.org/#home.
[550] *Trustedcoin*.

1. L'utilisation d'un portefeuille

Le fonctionnement des bitcoins semble complexe. Sathoshi Nakamoto précise dans son texte original[551] : « *une pièce électronique est définie comme une chaîne de signatures numériques. Chaque propriétaire transfère la pièce au suivant en signant numériquement une empreinte de la transaction précédente et de la clé publique du propriétaire suivant, et en l'ajoutant à la fin de la pièce. Tout bénéficiaire peut vérifier les signatures pour s'assurer de la chaîne de propriétés*[552] ».

Le protocole Bitcoin repose donc sur deux mécanismes : le chiffrement à clé publique et sur un algorithme complexe[553]. Toutefois, les bitcoins ne sont pas anonymes et c'est la raison pour laquelle Satoshi Nakamoto conseille d'utiliser des adresses différentes pour chaque réception de bitcoins. L'usage de *Bitcoin mixer* est également recommandé.

Ainsi, les bitcoins fonctionnent selon un protocole d'échanges chiffrés et authentifiés. Pour s'en procurer il faut obtenir une adresse bitcoin qui fera office de compte. Il s'agit de générer une clé publique et une clé privée afin de s'authentifier sans ambiguïté.

Ensuite, la gestion du compte se fait en utilisant un portefeuille à choisir parmi la multitude qui existe. Le choix de ce dernier est délicat car c'est lui qui permet l'accès permanent au compte et qui est gardien du capital. La confiance technique est donc primordiale dans un monde où les attaques informatiques sont régulières. La prudence est de rigueur. Ce faisant, il est conseillé d'utiliser les plateformes les plus importantes, enregistrées en tant qu'entreprise et de ne pas y mettre de sommes trop importantes car le risque zéro n'existe pas. La création d'un portefeuille se fait après avoir créé un compte en utilisant une adresse mail et un mot de passe. L'identité de l'utilisateur est vérifiée[554], il est nécessaire d'envoyer une photocopie de sa pièce d'identité et d'un justificatif de domicile. Une fois l'identité de l'utilisateur vérifié, il lui est alors possible d'acheter des Bitcoins en utilisant un service d'*Exchange* pour remplir son portefeuille et en

[551] NAKAMOTO, S., *Bitcoin : A Peer-to-Peer Electronic Cash System*, 2009.
[552]« *We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership* ».
[553] L'algorithme SHA256.
[554] Il existe des entreprises de vérification d'identité comme *Jumio* qui a créé *Bitcoin Identity Security Open Network.*

utilisant une paire de clés (2).

2. L'utilisation d'une paire de clés privée et publique

Le bitcoin est un protocole qui n'est pas entièrement anonyme. En effet, les utilisateurs sont identifiés grâce à une adresse qui ne donne pas d'information sur leur identité réelle. Toutefois, l'adresse n'est pas dissimulée si bien qu'il est possible de voir toutes leurs transactions ce qui peut amener à une identification. Dès lors, il existe des techniques de chiffrement permettant de réduire les chances de suivi des paiements d'un portefeuille bitcoin. Des clé privées et publiques sont alors utilisées pour chiffrer et déchiffrer les données du portefeuille. Seules les personnes détentrices de la clé privée pourront accéder aux données en clair.

A l'instar des principes *peer-to-peer* ou *friend-to-friend*, la technologie bitcoin suppose une décentralisation et une absence de serveur central. De puissants algorithmes vont permettre à chaque nœud de vérifier l'historique de la chaîne de blocs et ainsi devenir des garants de son intégrité. Pour ce faire, les ordinateurs utilisent le *hash* qui leur permet d'analyser l'historique des transactions et garantir que A a payé 50 bitcoins à B le 16 avril 2018. N'importe quel utilisateur peut devenir un nœud en ajoutant son ordinateur au réseau, il suffit d'utiliser le logiciel « *Bitcoin Core*[555] », un logiciel publié par Satoshi Nakamoto[556]. Dès lors, si la mémoire le permet, l'ordinateur récupérera l'ensemble volumineux de la *blockchain*.

Lors d'un paiement en bitcoin, comment le vendeur peut-il s'assurer que l'acheteur possède réellement la somme d'argent alors qu'il n'y a pas de point central faisant office de tiers de confiance comme une banque qui refuserait un paiement pour un acheteur n'ayant pas la somme sur son compte. Pour le bitcoin c'est le réseau d'ordinateurs qui décide à la majorité si le paiement peut s'effectuer. Pour cela, contrairement à un paiement par carte bancaire, un paiement bitcoin n'est pas instantané et doit être vérifié. Il faut que plusieurs blocs soient ajoutés à la chaîne afin que la transaction soit confirmée et cela peut prendre une dizaine de minutes. Ainsi, lors d'un paiement, le vendeur attend des nouveaux blocs pour s'assurer qu'il n'a pas été trompé. De plus, chaque transaction doit être signée électroniquement dans la Blockchain. Il s'agit d'une signature électronique par clé asymétrique. Cela permet de s'assurer de l'identité

[555] *Bitcoin Core* est le logiciel de référence des nœuds constituant le réseau bitcoin.
[556] Disponible à cette adresse : https://bitcoin.org/en/release/v0.9.0#rebranding-to-bitcoin-core.

de l'émetteur du message grâce aux clés privées et publiques qui sont liées entre elles. Par exemple, si A décide de donner 100 bitcoins à B, le message « *je donne 100 BTC à B* » sera chiffré grâce à sa clé privée. B utilisera alors la clé publique de A et s'il arrive à déchiffrer le message, il pourra être sûr que la clé publique correspond bien à la clé privée de A et qu'il s'agit bien de lui. Ainsi, seul A peut dépenser son argent en bitcoin puisqu'il est le seul à posséder sa clé privée. Cette dernière doit absolument être protégée. Dans une *blockchain*, l'argent ne se transmet pas d'un nom à un autre, mais d'une adresse à une autre. Si A génère une clé privée et une clé publique, il génère automatiquement une adresse à partir de sa clé publique. Cette adresse sera communiquée aux tiers afin que A puisse être payé. En réalité, les portefeuilles de bitcoins ne stockent pas d'argent mais les paires de clés. Enfin, il est conseillé de n'utiliser une adresse qu'une fois par paiement et de générer une nouvelle paire de clés pour chaque nouveau paiement. Ce sont les logiciels portefeuilles de bitcoins qui génèrent ces paires de clés à partir d'une série de mots.

CONCLUSION DU TITRE II
LE CONTENU DU DARKNET

Même si l'opacité qui existe sur le Darknet est utilisée par des personnes malveillantes pour commetre des crimes et des délits, les réseaux alternatifs constituent quand même une évolution technologie positive. Certains individus sont prêts à sacrifier certains de leurs droits fondamentaux afin d'arriver à un besoin social de sécurité maximale tandis que d'autres tentent de combattre les pratiques de renseignements de certains pays comme les États-Unis qui conservent les données personnelles des internautes. La création d'un darknet permet avant toute chose d'échapper au contrôle et la traçabilité, peu importe la raison. À l'origine les réseaux darknets aspiraient à protéger la vie privée de ses utilisateurs. Le fait que les cybercriminels se sont accaparés cette zone de liberté est un fâcheux contrecoup qui en vaut la peine compte tenu de la liberté qu'elle promet.

Dès lors, en tant que réseau sombre, le Darknet ne porte pas bien son nom. Loin d'être réduit à la cybercriminalité, il permet d'envisager une face d'Internet qui aspire à se dessiner dans les années à venir : un Internet décentralisé, anonymisé, sécurisé et libéré de l'emprise des Etats, en somme, un espace de liberté.

Le déploiement et le succès des réseaux darknets posent de nouvelles problématiques politiques et juridiques notamment quant à la gouvernance d'Internet qui suscite encore aujourd'hui de sérieux débats au sein de l'ICANN. L'émergence et la démocratisation de ces réseaux alternatifs a changé la donne et apporté de nouvelles possibilités non négligeables. En effet, l'opposition entre gouvernements et certaines communautés d'utilisateurs s'est accentuée avec l'apparition du Darknet. Les premiers exigent qu'Internet et le Darknet soient adaptés aux législations nationales tandis que les seconds exploitent la cryptographie pour faire sécession. Alors que la fragmentation d'Internet n'existait pas en raison de l'utilisation commune du protocole TCP/IP, l'apparition de nouveaux sites en .onion est venue altérer ce principe en créant de nouveaux espaces utilisant des protocoles différents.

D'aucuns redoutent que cette fragmentation d'Internet soit intensifiée par la volonté des Etats de contrôler Internet avec des noms de domaines nationaux fonctionnant comme les indicatifs téléphoniques. Un fractionnement pourrait être créé entre les zones de non-droit numériques et

un Internet contrôlé par les Etats. Dans ce contexte de gouvernance, le Darknet a un rôle à jouer pour offrir de nouvelles possibilités aux utilisateurs. Ainsi, il participe à l'évolution des technologies liées au numérique et concerne directement des problématiques importantes liées à la cybersécurité et aux contraintes législatives et juridiques que les Etats souhaitent imposer à Internet et que le Darknet semble pouvoir éviter.

CONCLUSION DE LA 1ère PARTIE
LA FACE SOMBRE D'INTERNET, LES ASPECTS PRATIQUES

En 2018, les profils de la nouvelle génération d'individus surfant sur le Darknet sont divers. Certains individus accèdent au Darknet afin de protéger leur vie privée et préserver leurs libertés individuelles, faire des achats sur le *Deep Web*, surfer sur le Web à partir d'une dictature comme la Corée du Nord où les réseaux sociaux sont interdits, ou éviter d'être constamment surveillés à cause des objets connectés, de la technologie du numérique et de la captation de données personnelles. En effet, initialement, les réseaux alternatifs ont été créés afin que les journalistes et les dissidents puissent combattre la censure dans certains pays autoritaires. En ce sens, les darknets ce sont multipliées. Pour les plus connus, *Freenet* en 2000, et Tor en 2006, tout est allé très vite. C'est en partie grâce à ces deux réseaux que l'accès au web sombre a été facilité au point de s'être démocratisé. L'usage du logiciel *Web2Tor* permet même d'accès au Darknet à partir d'un navigateur classique sans avoir à utiliser le navigateur *Tor2Web*. De plus, la différence entre l'Internet visible et l'Internet sombre s'est clairement amoindrie avec le réseau Tor qui permet, via un proxy, de basculer de l'Internet au Darknet et inversement.

D'autres individus accèdent à l'Internet sombre dans le dessein d'y commettre des infractions. Par exemple, les personnes qui sympathisent avec l'Etat Islamique peuvent communiquer ou même rechercher des financements via le web sombre. En outre, il existe d'infâmes marchés noirs comme *Silk Road* qui permettent aux individus d'acheter et de vendre des armes, de la drogue ou de consulter des imagines pédopornographiques.

De manière générale, les infractions commises sur l'Internet sombre peuvent être divisées en plusieurs catégories. Premièrement, il existe des cybermarchés noirs sur lesquels il est possible de trouver des contrefaçons, des drogues, des numéros de cartes bancaires, des armes, etc, payables en cryptomonnaie. Deuxièmement, des échanges de contenus choquants et illégaux sont effectués sur le web sombre. Dès lors il est possible d'avoir accès à des images pédopornographiques, de torture, de cannibalisme, de sexe violent, etc. Enfin, des services illégaux permettent de faire appel à un tueur à gage, de transporter des organes, d'acheter des logiciels malveillants, etc. Toutes ces infractions sont liées aux formes de criminalité « traditionnelles », qui ont été facilitées par les nouvelles technologies de l'information et de la

communication au point de constituer un nouveau vecteur de criminalité. Quatrièmement, des hackeurs sévissent sur le Darknet afin de commettre des infractions qui n'existaient pas avant l'apparition d'Internet.

Sur le plan juridique, le Darknet présente de multiples intérêts et pose de nombreuses questions, la principale étant de savoir dans quelle mesure la répression peut-elle avoir lieu et comment peut s'organiser la lutte contre cette forme de cybercriminalité. Les réseaux alternatifs conduisent notamment à se demander comment la loi pénale doit s'appliquer dans l'espace numérique, de quelle manière le droit international peut appréhender efficacement le phénomène, comment coordonner la répression entre les différents États et quelles règles de procédure appliquer, la question se posant encore de savoir si des infractions spéciales devraient être créées ou si, au contraire, les incriminations de droit commun sont suffisantes pour permettre une répression efficace.

Le sujet touche donc de nombreux thèmes essentiels du droit pénal général, du droit pénal spécial, de la procédure pénale et du droit pénal international qu'il convient d'aborder dans une seconde partie (Partie 2).

2nde PARTIE
LA FACE SOMBRE D'INTERNET, LES ASPECTS JURIDIQUES

Le jeudi 29 février 2013 à Gennevilliers, le Premier Ministre Jean-Marc Ayrault se prononce lors du séminaire gouvernemental sur le numérique. Il présente les 18 mesures du projet gouvernemental en matière de politique numérique, dans le cadre des objectifs fixés par la « *stratégie numérique pour l'Europe en 2020* ». La feuille de route du Gouvernement est articulée autour de 3 axes, la jeunesse[557], la compétitivité[558] et les valeurs[559].

À la suite de ce séminaire gouvernemental, les ministres de la Justice, de l'Économie et des finances, de l'intérieur, ainsi que la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'Économie numérique constituent un groupe de travail interministériel chargé de faire des propositions en matière de lutte contre la cybercriminalité. Le groupe interministériel s'est penché sur la cybercriminalité, en évinçant les questions qui ont déjà été soumises à l'examen d'autres instances[560]. Cela a nécessité des mois de travail, durant lesquels se sont tenues treize séances plénières, des dizaines d'auditions en comité restreint et de nombreux entretiens et visites réalisés par son président. L'idée c'est qu'il faut rechercher une association entre la lutte contre la cybercriminalité, la cyberdéfense et la cybersécurité. Ce groupe est composé de généralistes du droit pénal tels que des avocats ou procureurs, mais aussi de spécialistes policiers, gendarmes et douaniers. Il s'agit d'élaborer une stratégie globale de lutte contre la cybercriminalité en prenant en compte les questions de prévention et de sensibilisation du public. Un constat s'est alors imposé. Premièrement, la

[557] « *Faire du numérique une chance pour la jeunesse : outre la loi d'orientation et de programmation pour la refondation de l'école qui vise à généraliser les usages du numérique de l'école au lycée, le Gouvernement engage un plan de formation, sur deux ans, de 150 000 enseignants à l'usage pédagogique des technologies de l'information et de la communication* ».
[558] « *Renforcer la compétitivité de nos entreprises grâce au numérique. Afin d'accroître la visibilité de l'écosystème "numérique" français, des quartiers numériques locaux seront identifiés ou créés dans 15 villes ou territoires. Ces quartiers numériques seront labellisés et bénéficieront d'une exposition majeure international. Un premier "quartier numérique" devrait voir le jour d'ici la fin de l'année à Paris ou en proche banlieue pour offrir une vitrine au dynamisme du tissu numérique national* ».
[559] « *Promouvoir nos valeurs dans la société et l'économie numériques : le Gouvernement consolidera la protection des libertés fondamentales sur internet. Un projet de loi sur la protection des droits et libertés numériques sera proposé au Parlement début 2014 au plus tard* ».
[560] Tel est le cas s'agissant de la protection des données nominatives traitée par la Commission nationale de l'informatique ou s'agissant de la contrefaçon commerciale.

question de la cybercriminalité a un véritable caractère transversal dans la mesure où elle intéresse énormément d'acteurs, aussi bien publics, que privés. Dès lors, le groupe a effectué de nombreuses auditions afin de mieux comprendre les attentes de chacun, et a par ailleurs été sollicité à plusieurs reprises par des associations et des chercheurs. Néanmoins, il faudrait une enquête généralisée auprès de l'ensemble des administrations de l'État, pour appréhender de manière exhaustive les dispositifs existants et les attentes sectorielles. Deuxièmement, l'actualité en la matière étant riche, le groupe est contraint de réexaminer certaines questions dont il était saisi, tout en élargissant son mandat. En effet, les normes concernant la lutte contre la cybercriminalité ne cessent d'évoluer, et certaines questions qui étaient à l'étude sont désormais concrétisées. Même chose d'un point de vue juridictionnelle puisque nombreux sont les arrêts rendus par la chambre criminelle de la Cour de cassation dans le cadre du contrôle de la conventionnalité pour les réquisitions informatiques, mais aussi pour la géo-localisation en temps réel. Par conséquent, eu égard à cette riche actualité juridique, le groupe doit établir une stratégie globale et une grille juridique cohérentes. Troisièmement, au-delà de la réaction française, il existe de nombreux travaux européens en matière de lutte contre la cybercriminalité. Ainsi, de nombreux projets sont en discussion tandis que des règlements et directives sont entrés en vigueur. De plus, le groupe a consulté certains responsables internationaux et spécialistes de la coopération internationale et du droit comparé. Par conséquent, même si la cybercriminalité est apparue comme une affaire de spécialistes, elle affecte tout le monde et c'est la raison pour laquelle le groupe a décidé de s'adapter aux attentes de tous les usagers et consommateurs.

À la demande du groupe interministériel, un pôle d'évaluation des politiques pénales a été mis place par la DACG[561] afin d'apporter son soutien aux parquets. Ce pôle *a mis en place une table NATINF[562] recensant toutes infractions relatives à la cybercriminalité prévues par la norme française [563]* . Les membres du pôle ont compté 248 infractions qui concernent la

[561] « *Au sein du ministère de la Justice, la direction des affaires criminelles et des grâces, qui a célébré son bicentenaire en 2014, est la direction de la norme et de la justice pénales ; elle comprend près de 370 personnes, dont plus de 60 magistrats de l'ordre judiciaire, répartis sur trois sites : place Vendôme à Paris, où se trouvent les trois sous-directions pénales, à Nanterre, où se trouve une antenne du bureau de l'entraide pénale internationale, et à Nantes, siège de casier judiciaire national de 1982* ». Définition disponible à cette adresse : http://www.justice.gouv.fr/le-ministere-de-la-justice-10017/direction-des-affaires-criminelles-et-des-graces-10024/.
[562] NATure d'INFractions.
[563] Loi, décret-loi, ordonnance, décret.

cybercriminalité *« soit par leur objet, soit parce que leur mode de commission est saisi par la loi, le plus souvent au titre des circonstances aggravantes* ».

Les formes de criminalité liées à l'utilisation des nouvelles technologies de l'information et de la communication sont abordées par l'Observatoire national de la délinquance et des réponses pénales par deux approches différentes : les infractions portées à la connaissance des administrations d'une part et les enquêtes effectuées auprès de la population d'autre part.

Pour la première approche, l'infraction est enregistrée à travers un outil appelé « *état 4001* », géré par la direction centrale de la police judiciaire. iL permet d'analyser l'évolution des différents phénomènes criminels. Une nomenclature de 103 index, classés de 1 à 107, permet d'enregistrer les faits constatés en les classant par type. Néanmoins, cette nomenclature ne donne pas une mesure précise des phénomènes ayant un lien avec la cybercriminalité. En effet, certains index comprennent les infractions qui ont été commises ou facilitées par l'utilisation des nouvelles technologies de l'information et de la communication sans être totalement dédiés à ce genre d'infractions. A titre d'exemple, l'index 01, des « *escroqueries et abus de confiances (199 408 faits constatés en 2011)* » recense tous les types d'escroqueries et pas seulement celles liées à l'utilisation de numéro de carte bancaire sur Internet. De plus, les « *atteintes aux systèmes de traitement automatisé des données* » n'ont pas d'index spécifique et sont intégrées à l'index 107 « *autres délits* »[564]. Enfin, pour les infractions commises ou facilitées par les nouvelles technologies de l'information et de la communication, l'utilisation de ces dernières n'est qu'accessoire et ne constitue pas l'infraction principale du fait constaté. Ainsi, pour une atteinte sexuelle commise sur un mineur de 15 ans par un majeur ayant rencontré sa victime sur Internet, l'infraction retenue sera « *l'atteinte sexuelle* »[565] et non « *l'utilisation d'un service de discussion en ligne* ». Même si les statistiques extraites ne représentent qu'une partie du phénomène, elles peuvent utiles sur les plans qualitatif et opérationnel en listant les méthodes utilisées par les « *cybercriminels* ».

Pour la seconde approche statistique, l'Observatoire national de la délinquance et des réponses pénales utilise une enquête dite « *Cadre vie et sécurité* », ou « *enquête de victimation* », menée

[564] Ceci est justifié par le fait que la dernière révision de la nomenclature de l'état 4001 a eu lieu en 1996, à une époque où Internet n'était pas généralisée.
[565] Index 50.

depuis 2007 avec l'INSEE[566]. Dès lors, chaque année 17 000 ménages et individus français sont interrogés sur les atteintes dont ils auraient pu être victimes, même s'il n'y a pas eu dépôt de plainte auprès des forces de l'ordre. Ces enquêtes de « *victimation* » comportent aussi une partie propre aux infractions liées à la cybercriminalité. Toutefois, dans la plupart des cas, les individus n'ont pas conscience d'être des victimes dans la mesure où certaines formes de cybercriminalité peuvent être transparentes pour l'utilisateur. Toutefois, en 2018 l'index « *Darknet* » n'existe toujours pas et cette partie du Web semble négligée par les enquêtes et par les autorités.

Les cybercriminels étendent leur emprise en même temps que le développement d'Internet. Leur force réside dans le fait qu'ils ne sont pas visibles de sorte qu'il est difficile de les connaître. Chaque utilisateur d'Internet s'expose à une menace et peut, malgré lui, devenir la cible d'un délit. Les conséquences sont importantes pour les individus, les organisations mais aussi pour l'État. Cette invisibilité s'accentue lorsque les cybercriminels utilisent des moyens d'anonymisation tels que le Darknet.

Face à cette menace, les modifications du code pénal se sont multipliées avec des dispositions liées aux nouvelles technologies de l'information et de la communication. L'émergence de nouvelles pratiques facilitées par le numérique a créé une inflation des normes relatives à la cybercriminalité. Cette dernière a fait l'objet d'une multiplication de règles techniques, complexes et contradictoires si bien que les mondes juridiques et numériques ne semblent pas compatibles. Pourtant, les usages des internautes ont modifié la donne et la démocratisation d'Internet a contraint les professionnels du droit à s'acclimater au phénomène en traduisant les faits en droit et en créant des règles idoines. En effet, les cybercriminels n'ont pas attendu longtemps avant d'exploiter les failles techniques et juridiques offertes par Internet et les magistrats ont dû s'adapter afin de retenir la qualification idéale pour des infractions ayant généralement des effets dématérialisés. La commission de certaines infractions est très simple mais leurs effets et préjudices sont très graves. Internet offre aux cyberdélinquants des possibilités infinies de commettre des infractions en étant animés par un réel sentiment d'impunité. Pour toutes ces raisons, la cybercriminalité qui n'est pas similaire aux autres criminalités mérite une étude singulière.

[566] Institut national des statistiques et des études économiques.

En 2018, en faisant un bilan relatif à l'encadrement de la cybercriminalité, il est possible d'établir plusieurs constats. Il existe un réel arsenal répressif en matière de cybercriminalité à un niveau interne, mais également à un niveau international (Titre I). Toutefois, le système juridique est encore inadapté à la cybercriminalité de manière générale et à la cybercriminalité dissimulée en raison de leurs singularités. Dès lors, les règles existantes sont inefficaces et supposeraient des modifications prenant en compte le Darknet (Titre II).

TITRE I
L'ARSENAL REPRESSIF EN MATIERE DE CYBERCRIMINALITE

En France, pour qu'une répression soit envisageable, il faut un texte la prévoyant, et le plus souvent que l'infraction ait un lien avec la République. C'est le principe de légalité criminelle souvent synthétisé par la formule latine du 19ème siècle : « *nullum crimen, nulla poena sine lege* ». Ce principe est inscrit dans la Déclaration des droits de l'homme et du citoyen de 1789, dans le Code pénal français et consacré par la CESDH ainsi que par le Pacte international sur les droits civils et politiques. Ensuite, nul ne peut être condamné pour un fait qui, le jour où il a été commis, ne constituait pas une infraction selon le droit alors en vigueur, c'est le principe de non-rétroactivité de la loi pénale, corollaire du principe de légalité en droit pénal.

Par ailleurs, le thème des sources du droit pénal reste essentiel dans la matière répressive dans la mesure où la mise en œuvre du droit pénal touche aux libertés individuelles. Tous les citoyens ont des droits et la rigoureuse procédure pénale française ne facilite pas toujours le travail des enquêteurs, dans un contexte où les délinquants ont l'avantage. La lutte contre la criminalité amène à se demander quel est le prix à payer pour lutter de manière efficace contre les comportements antisociaux. De plus, la loi n'étant ni atemporelle, ni universelle, le juge répressif doit veiller à ce que les faits poursuivis entrent bien dans le champ d'application de la loi pénale, en prenant en compte le moment et le lieu où ils ont été commis. La jurisprudence retient l'aspect psychologique du délinquant mais aussi son activité physique. En effet pour la chambre criminelle de la Cour de cassation c'est « *l'acte qui tend directement et immédiatement à la consommation de l'infraction et qui est accompli dans l'intention de la consommer*[567] ». Les actes qui ne correspondent pas à cette définition sont donc des actes préparatoires non punissables. L'idée est de réprimer assez haut sur le chemin criminel tout en évitant des condamnations arbitraires basées sur de simples suppositions.

Il convient également de se demander si l'utilisation d'Internet ou du Darknet peut constituer une circonstance aggravante. En soi leur utilisation n'a rien de défavorable ou d'aggravant, il s'agit juste d'une modalité de commission de l'infraction. Mais, dans certains cas, Internet

[567] Cour de cassation, chambre criminelle, 3 janvier 1973, n°71-91820.

permet d'accroître l'amplitude d'une diffusion de contenu grâce à une publication sur un site ou un réseau social. En rendant plus importante la portée du message, Internet ou le Darknet peut aggraver les conséquences d'une infraction et devenir une circonstance aggravante. À titre d'exemple, en matière de pédopornographie, l'article 227-23 du Code pénal dispose que « *les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques* ». Pour que cette circonstance aggravante soit applicable il faut que soit utilisé un réseau de communications électroniques, à destination d'un public non déterminé pour de la diffusion de contenu pédopornographique. Est ainsi visée la diffusion d'images ou vidéos pornographiques sur un réseau *friend-to-friend* ou sur un forum du Darknet. Mais la terminologie « *un réseau de communications électroniques* » de l'article 227-23 du Code pénal trouve également à s'appliquer à énormément de situations si bien qu'il serait opportun de la réutiliser dans un contexte d'harmonisation de toutes les circonstances aggravantes relatives à Internet. À titre d'exemple, la circonstance aggravante du délit d'apologie du terrorisme[568] utilise les termes « *service de communication au public en ligne* » tandis que celle du délit de recours à la prostitution de mineurs[569] les termes de « *réseau de communication* ». Aussi, cette circonstance aggravante pourrait être appliquée pour d'autres infractions comme l'extorsion[570] d'argent qui s'amplifie grâce à l'utilisation de logiciels malveillants vendus sur le Darknet. Le quantum de peine est adaptable en cas d'utilisation de technique d'anonymisation ou de chiffrement des données.

En France, il existe donc un arsenal juridique pour la lutte contre toutes les sortes d'infractions liées à la cybercriminalité. Le Code pénal a permis l'élargissement de plusieurs infractions existantes afin de prendre en compte les infractions cybercriminelles (Chapitre 1). Toutefois, la pratique a révélé de nouveaux défis dans la mesure où une infraction peut impliquer plusieurs États. Or, les différents systèmes juridiques ne se sont pas nécessairement adaptés de la même manière à ce nouveau phénomène. Par conséquent, une coopération entre Etats a été nécessaire

[568] Code pénal art. 421-2-5 : « *Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende. Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne »*
[569] Code pénal art. 225-12-2.
[570] Code pénal art. 312-1 : « *L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ».

afin d'agir de manière concertée contre le cyberespace qui n'a aucune frontière. Des initiatives de coopération à l'échelle européenne ou internationale se sont mises en place pour lutter contre la cybercriminalité. La Convention de Budapest sur la cybercriminalité en est le parfait exemple (Chapitre 2).

CHAPITRE 1
LES DISPOSITIONS NATIONALES EN MATIÈRE DE CYBERCRIMINALITÉ DISSIMULÉE

Dans le langage courant, la cybercriminalité est définie comme « *l'ensemble des infractions pénales commises sur les réseaux de télécommunications, en particulier Internet* »[571].

Selon, Jorick Guillaneuf, chargé d'étude statistiques à l'Observatoire national de la délinquance et des réponses pénales, la cybercriminalité regroupe « *l'ensemble des infractions susceptibles d'être commises ou facilitées par l'utilisation d'un système informatique, généralement connecté à un réseau* ». Dès lors, elle peut viser des infractions diverses qui sont susceptibles d'êtres distinguées de plusieurs manières. Par exemple, dans son analyse de 2012, Jorick Guillaneuf envisage deux sortes d'infractions cybercriminelles. D'une part, il expose « *les infractions liées aux systèmes d'informations et aux systèmes de traitement automatisés des données, engendrées par le développement des réseaux informatiques tel que Internet* ». C'est le cas notamment pour les accès frauduleux, pour les altérations d'un système ou encore pour les attaques par déni de service… Ces atteintes aux systèmes et réseaux informatiques n'existaient pas avant l'arrivée d'Internet. D'autre part il expose, « *les infractions liées aux formes de criminalité traditionnelles* », qui ont subi une évolution en raison de l'apparition des nouvelles technologies de l'information et de la communication de sorte qu'elles constituent désormais un nouveau vecteur de criminalité. À titre d'exemple, l'escroquerie est comprise dans cette seconde catégorie avec de nouvelles formes comme l'usage frauduleux de cartes bancaires en ligne ou encore le « *hameçonnage* »[572]. De même pour les injures de toutes sortes qui peuvent être diffusées via les nouveaux moyens de communication électronique, ou pour la diffusion d'images pédopornographiques pouvant elle aussi être facilitée par les réseaux.

Par conséquent, la cybercriminalité comprend tous les délits possibles réalisables par le biais de l'informatique et des technologies Internet. C'est la raison pour laquelle, les cybercrimes sont dits de haute technologie et supposent un certain niveau de compétence technique et des outils technologiques pour le réaliser. Avec le Darknet les criminels ont trouvé un nouveau

[571] Définition issue de www.Larousse.fr.
[572] L'hameçonnage est utilisé par les fraudeurs qui souhaitent obtenir des informations personnelles de leurs victimes en se faisant passer pour un tiers de confiance comme la Caisse primaire d'assurance maladie. Cette technique est aussi appelée « *phishing* ».

moyen de développer leurs activités grâce à l'anonymat qui y est préservé et aux échanges matériels et immatériels infinis. Étudier les infractions du Darknet suppose l'étude des incriminations prévues par la loi, de l'élément matériel et de l'élément moral. Une première section sera consacrée à la répression des infractions qui n'existaient pas avant l'apparition d'Internet (Section 1) et une seconde section à celles dont la commission est facilitée par Internet et le Darknet (Section 2).

SECTION 1
La répression des infractions dirigées contre les systèmes d'information

D'aucuns confondent parfois les termes délinquants informatiques et cyberdélinquants ou encore les termes cybercriminalité et criminalité informatique. Ces derniers sont analogues mais nécessitent une démarche différente puisque la cybercriminalité est souvent « *considérée comme une variante de la criminalité informatique dans la mesure où elle s'exprime sur et à travers les réseaux et les systèmes de communication, contrairement aux autres délits informatiques qui ne nécessitent pas d'interaction avec les systèmes et les réseaux de télécommunication*[573] ».

Dès lors, la cybercriminalité semble plus large que la criminalité informatique en ce qu'elle englobe les atteintes perpétrées contre les systèmes informatiques au moyen d'Internet ainsi que les atteintes aux personnes et aux biens effectuées grâce au réseau. Or, « *toute infraction commise au moyen d'un réseau de télécommunication n'est pas systématiquement une infraction informatique*[574] ».

Le développement d'Internet et du Darknet a permis le renforcement de la « *délinquance informatique* » qui est définie comme « *ensemble des délits et actes criminels commis à l'aide ou à l'encontre des réseaux informatiques*[575] ». Pourtant, le terme délinquant désigne de manière stricte l'individu qui commet un délit conformément à la classification légale des infractions. L'article 111-1 du Code pénal dispose que « *les infractions pénales sont classées, suivant leur gravité, en crimes, délits et contraventions* ». Ainsi, pour connaître la nature de l'infraction, il faut regarder la peine encourue et se baser sur l'échelle des peines, prévue aux articles 131-1 et suivants du Code pénal, qui définit les différentes sanctions criminelles, correctionnelles et contraventionnelles. Cette classification tripartite a des conséquences en droit pénal de fond et en procédure pénale. À titre d'exemple, les règles relatives à la tentative dépendent de la nature de l'infraction : elle est toujours punissable pour un crime et l'est pour les délits que lorsque la loi le prévoit expressément. Elle a aussi une incidence sur la complicité, la récidive, les juridictions compétences ou encore l'action publique… Ainsi, il faudrait utiliser le terme cyberdélinquant pour les délits commis au moyen d'Internet et cybercriminel pour les

[573] CHAWKI M., *Essai sur la notion de cybercriminalité*, IEHEI, 2006, page 25.
[574] CHAWKI M., *Combattre la cybercriminalité*, édition Saint-Amans, 2008, page 47.
[575] Disponible à cette adresse :http://dictionnaire.sensagent.leparisien.fr/délinquance%20informatique/fr-fr/.

crimes.

Les cybermenaces, sont des menaces liées au fait que des ordinateurs peuvent constituer des cibles en étant visés par des attaques informatiques . Ces menaces sont évaluées en fonction de l'ampleur et de l'importance des dégâts qu'elles peuvent occasionner. Selon Solange Ghernaouti-Hélie[576], cela s'exprime par un degré de dangerosité catégorisable en trois niveaux : faible, moyen et élevé. Les premières ne seraient pas fondamentalement graves mais peuvent selon les circonstances devenir très préjudiciables. Un système peut être la cible d'une menace lorsqu'il est connecté à internet sans un antivirus efficace. Plus longtemps il est connecté à Internet, plus il a de chances de créer une faille exploitable, mais son comportement peut aussi avoir des conséquences. Ainsi, un utilisateur qui active des logiciels infectés en les ayant piratés au lieu de les payer, ou qui se connectent régulièrement sur des sites pornographiques rend sont ordinateur plus vulnérable. En se connectant à un réseau Darknet tel que Tor, il faut que l'utilisateur ait conscience du danger auquel il est confronté. Le faible niveau de dangerosité relève souvent de la nuisance comme pour les spams, appelés pourriels, qui peuvent surcharger la boîte aux lettres électroniques des usagers. Toutefois, dans certains cas les spams sont utilisés afin de faciliter des escroqueries. Tel est le cas lorsque des individus font croire à leurs victimes qu'elles ont gagné une grosse somme d'argent qui ne peut être débloquée que si elles avancent de l'argent. Les moyens classiques utilisés sont : la réception d'un mel envoyé par le représentant officiel d'un gouvernement étranger, de l'héritage d'un parent jusqu'alors inconnu ou du premier prix d'une loterie. Les conséquences pouvant être graves, une lutte contre les spammeurs a dû être mise en place. En France, au sens de la loi, spammer consiste à envoyer un courriel à une personne physique sans son consentement préalable, librement et explicitement obtenu. Cette pratique est prévue par le Code pénal et la CNIL est compétente pour recevoir les plaintes et constater les infractions. Les articles 226-16 et 226-18 du Code pénal disposent respectivement 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 est puni de trois ans d'emprisonnement et de 45 000 euros d'amende* » et que « *le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations*

[576] GHERNAOUTI-HÉLIE S., *La cybercriminalité, le visible et l'invisible*, presses polytechniques et universitaires romandes, 2009, page 87.

nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

Les menaces de moyenne dangerosité sont celles qui nécessitent une intervention mais dont les conséquences sont maîtrisables. C'est le cas par exemple pour le « *cheval de Troie* » qui une fois déclenché, permet à des utilisateurs externes de contrôler l'ordinateur infecté afin d'espionner, voler, détruire des données ou lancer des attaques informatiques sur d'autres systèmes. L'évaluation de niveau de dangerosité se fait en fonction des conséquences. Ainsi, les menaces d'un niveau élevé entrainent des dégâts qui vont avoir des coûts importants pour les victimes. Ces menaces sont souvent liées à des fuites d'informations ou à des contrôles de système.

Pour le Darknet, tous les articles du Code pénal relatifs à la criminalité ou à la délinquance informatique ont vocation à s'appliquer. Par exemple, tel est le cas pour l'article 226-18 du Code pénal en ce qui concerne la collecte « *des données à caractère personnel par un moyen frauduleux, déloyal ou illicite* » sur le Darknet. En outre, La loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi « *Godfrain* » est la première loi qui réprime les actes de piratage et de criminalité informatique. Elle instaure dans le code pénal un chapitre intitulé « *Des atteintes aux systèmes de traitement automatisé de données* » qui incrimine l'accès et le maintien frauduleux dans un système de traitement automatisé de données. Les articles 323-1 à 323-7 du Code pénal incriminent des faits relatifs à la fraude informatique comme notamment le fait de s'introduire frauduleusement dans un système informatique, le fait d'introduire frauduleusement des données dan un système informatique ou d'en supprimer les données qu'il contient. Il convient de traiter dans une première section la répression de l'intrusion informatique (§1) et dans une seconde section celle du sabotage informatique (§2).

§1) L'intrusion informatique

Dans son ouvrage intitulé « *les infractions commises sur Internet* », A. JABBER évoque les différentes formes que l'intrusion informatique peut prendre selon la méthode utilisée par les hackeurs qui peuvent créer ou exploiter les vulnérabilités existantes[577]. Ainsi, une intrusion informatique peut prendre plusieurs formes en fonction de la méthode utilisée par l'individu. En outre, il faut différencier les intrusions simples avec un accès ou un maintien frauduleux dans le système, de celle avec dommage.

Sur le Darknet, nombreux sont les pirates informatiques à proposer leur service d'intrusion informatique pour diverses raisons. Lorsque la cible est fixée, le pirate effectue un travail de repérage afin d'obtenir le plus de renseignements sur la victime. Ensuite, plusieurs moyens s'offrent au pirate pour arriver à ses fins. Il peut usurper l'identité numérique de sa victime en utilisant ses informations de connexion ou introduire un programme qui se cache lui-même dans un autre programme afin de contaminer le système et en prendre le contrôle.

Même s'il existe de nombreux moyens pour se protéger comme des logiciels de protection contre les intrusions ou de détection des intrusions, un cadre juridique est nécessaire. En ce sens, il existe une incrimination relative à l'intrusion informatique (A) mais quid de la criminalité informatique organisée (B) ?

A) L'intrusion informatique

La loi distingue l'accès et le maintien frauduleux dans un système informatique. Le premier est possible sans le second mais l'inverse n'est pas possible. En tout état de cause, l'accès (1) et le maintien frauduleux (2) présentent des similitudes.

1. L'accès frauduleux

En France, l'article 323-1 alinéa 1er du Code pénal[578] dispose que « *le fait d'accéder ou de se*

[577] JABBER A., Les infractions commises sur Internet, l'Harmattan, 2009, pages 24 à 26.
[578] Cet article est créé par la loi dite « *Godfrain* » du 5 janvier 1988 et modifié par l'article 4 de la loi n°2015-912 du 24 juillet 2015. Il se trouve dans le chapitre relatif aux « *atteintes aux systèmes de traitement automatisé de données* ». Il ne vise que les altérations involontaires car les entraves volontaires sont prévues par les articles 323-2 et 323-3 du Code pénal.

maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende ». Cet « *accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication* ».[579] Concernant la nécessité d'une violation des mesures de sécurité, la Cour d'appel de Paris le 30 octobre 2002, a estimé « *que la possibilité d'accéder à des données stockées sur un site avec un simple navigateur, en présence de nombreuses failles de sécurité, n'est pas répréhensible* ». Cette décision va dans le sens de l'article 226-17 du Code pénal qui dispose que « *le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* ».

Il y a plusieurs modalités d'attaque informatique qui dépendent de la méthode utilisée et de la perte engendrée. Les attaques par intrusion informatique se sont développées grâce au Darknet qui offre la possibilité d'acheter des logiciels permettant à des utilisateurs de s'introduire de manière non autorisée et frauduleuse dans un système informatique.

Le « *cheval de Troie* » est le mécanisme le plus utilisé pour les intrusions de ce type. Il permet au pirate informatique d'ouvrir une brèche[580] dans un système informatique afin d'en prendre le contrôle. Pour ce faire, il introduit un fichier infecté par le biais d'une clé USB ou d'un courrier électronique[581]. Lorsque ce dernier est ouvert, le pirate peut contrôler à distance le système piraté et mettre en place un projet illégal. L'utilisation d'un tel programme est sanctionnée par l'article 323-1 du Code pénal mais aussi par l'article 323-2 du Code pénal qui vise le fait de « *fausser le fonctionnement d'un système de traitement automatisé de données* » ou encore l'article 323-3 du Code pénal qui vise « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé* ».

[579] Cour d'appel de Paris, 5 avril 1994, D. 1994. IR 130.
[580] https://web.maths.unsw.edu.au/~lafaye/CCM/virus/trojan.htm: « Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur ».
[581] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 78 : « *Le courrier électronique, avec l'envoi d'une pièce jointe infectée, est la méthode d'entrée des pirates la plus utilisée, car elle est à la base de la génération des adresses IP* ».

Les pirates informatiques utilisent également l'usurpation d'identité afin de se faire passer pour la victime. À titre d'exemple, dans un même réseau ils peuvent usurper l'adresse IP d'une victime afin de remplacer celle de l'expéditeur d'un paquet IP par celle d'une autre machine. Dès lors, le pirate pourra envoyer un paquet de données à une machine du réseau en se faisant passer pour une autre machine du réseau. Sans cette usurpation, le paquet aurait été rejeté par le pare-feu du réseau. Une fois le paquet de données envoyé, le pirate pour ouvrir une brèche dans le réseau afin d'en prendre le contrôle[582].

L'article 323-1 alinéa 1er du Code pénal prévoit que le « *fait d'accéder (...) frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* » est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Initialement créé pour le minitel, cet article a vocation à s'appliquer à Internet mais également au Darknet. Un tel accès pourrait en effet se faire à partir de la face cachée d'Internet. Le législateur ne fait pas de distinction entre les différents mode d'accès, le plus important reste la cible qui doit nécessairement être « *un système de traitement automatisé de données* ». Il peut s'agit d'un site Internet, d'un ordinateur ou d'un système informatique connecté.

Toutefois, l'accès « *frauduleux* » suppose une manœuvre de la part du pirate informatique qui pourrait alors utiliser un cheval de Troie envoyé du Darknet ou usurper l'identité de la victime. L'accès doit en effet être volontaire[583], ce qui suppose que le pirate informatique ait conscience de l'irrégularité de son acte. En effet, la doctrine et la jurisprudence font valoir que l'adverbe « f*rauduleusement* » signifie que le délinquant a conscience que l'accès ne lui est pas autorisé. L'attitude volontaire et l'intention de nuire ne sont pas nécessaires. Il s'agit de l'élément moral de l'infraction qui exclut donc l'intrusion par erreur[584]. Néanmoins, l'intrusion sans autorisation[585] afin de tester la sécurité d'un réseau entre dans le cadre de l'incrimination d'accès frauduleux. Ainsi, la révélation de l'existence de failles de sécurité dans le réseau de Sciences Po Paris a valu une condamnation de son auteur[586]. Les hackeurs de ce genre sont

[582] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 79.
[583] LUCAS A., DEVEZE J., et FRAYSSINET, Droit de l'informatique et de l'Internet, 2001, page 47.
[584] Cour d'Appel de Douai, 7 octobre 1992, Gazette du Palais, 1993, n°22, page 326.
[585] L'intrusion peut être autorisée par le maître du système afin que des spécialistes du piratage informatique trouvent les failles du système. Dès lors, l'incrimination n'est pas caractérisée.
[586] RABBIN DES BOIS, *Lève-toi et code- Confessions d'un hacker*, 16 mai 2018.

capables de s'introduire dans un système informatique mais également de s'y maintenir frauduleusement (2).

2. Le maintien frauduleux

Un individu qui se maintient frauduleusement ou irrégulièrement dans un système de traitement automatisé de donnée entre également sous l'empire de l'article 323-1 du Code pénal. Le maintien suppose une durée de connexion plus longue. Toutefois, une question se pose quant à la distinction entre accès et maintien frauduleux : à quel moment l'accès frauduleux devient-il maintien frauduleux ? Concernant le point de départ du maintien frauduleux, « il apparaît que la loi n'est pas claire sur le point de départ de l'infraction du maintien frauduleux[587] ». La doctrine estime que le maintien est réalisé lorsque le hackeur commence à exploiter l'accès frauduleux.

Certains professionnels de l'informatique tentent de détecter les failles afin de contribuer à la sécurité des systèmes. Il convient de s'interroger sur leur situation à l'égard du droit pénal. Certains hackeurs sont engagés par des entreprises afin de détecter les failles de sécurités. Leur mission s'inscrit dans le cadre d'un contrat qui fixe les limites de temps et d'espace du hackeur qui agit dans un cadre juridique prédéfini. D'autres hackeurs agissent en toute autonomie pour pénétrer et se maintenir dans des systèmes informatiques conformément à ce qui est prévu par la loi du 5 janvier 1988, dite Godfrain. Durant les débats parlementaires de deux lois de 2016[588], les élus ont envisagé une dispense de peine pour les hackeurs qui avertiraient les autorités judiciaires ou administratives d'un risque d'atteinte au fonctionnement du système ou aux données afin de protéger les données pour l'avenir. Désormais, l'article 47 de la loi du 7 octobre 2016 pour une République numérique dispose que « *pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale*[589] *n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de*

[587] BOOS R. La lutte contre la cybercriminalité au regard de l'action des États, Université de Lorraine, 2016, page 85.
[588] La première est la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, et la seconde la loi n°2016-1321 du 7 octobre 2016 pour une République numérique.
[589] « *Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* ».

sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données[590] ». Concrètement, lorsqu'un hackeur de bonne foi saisit l'autorité nationale de sécurité des systèmes d'informatique pour lui transmettre une information liée à la sécurité d'un système d'information, elle n'est pas tenue de le dénoncer tel que le prévoit l'article 40 du Code de procédure pénale. Elle utilise alors les informations reçues afin d'avertir le responsable du système en question. Cependant, cette absence de dénonciation n'empêche pas la mise en mouvement de l'action publique par le parquet qui a la possibilité de poursuivre en cas de plainte de la victime ou s'il estime que les éléments constitutifs de l'infraction sont réunis[591]. Par conséquent, un hackeur de bonne foi, souhaitant dénoncer une faille de sécurité, ne pourra faire l'objet d'aucune garantie absolue. Même chose pour un internaute qui ne penserait pas à contacter l'autorité nationale de sécurité des systèmes d'informatique. À titre d'exemple, dans l'affaire « *Tati contre Kitetoa*[592] », en première instance un internaute est déclaré coupable « *d'accès frauduleux dans un système de traitement automatisé de données (…) infraction prévue par l'article 323-1 alinéa 1 du Code pénal*[593] » avant que la Cour d'appel le relaxe. Sans le vouloir, le prévenu a trouvé la faille de sécurité d'un site web et a averti le responsable du site. Ce dernier a porté plainte pour accès frauduleux au système. Evidemment, ce genre de mésaventure n'incite pas à dénoncer les éventuelles failles de sécurité des systèmes d'information.

Par moment, des groupes de hackeurs du Darknet peuvent s'unir pour mettre en place des intrusions organisées. Cette criminalité informatique organisée est prise en compte en tant que circonstance aggravante (B).

[590] Code de la défense art. L.2321-4.
[591] En ce sens l'article 40-1 du Code de procédure pénale dispose que « *lorsqu'il estime que les faits qui ont été portés à sa connaissance en application des dispositions de l'article 40 constituent une infraction commise par une personne dont l'identité et le domicile sont connus et pour laquelle aucune disposition légale ne fait obstacle à la mise en mouvement de l'action publique, le procureur de la République territorialement compétent décide s'il est opportun : 1° Soit d'engager des poursuites ; 2° Soit de mettre en oeuvre une procédure alternative aux poursuites en application des dispositions des articles 41-1, 41-1-2 ou 41-2 ; 3° Soit de classer sans suite la procédure dès lors que les circonstances particulières liées à la commission des faits le justifient* ».
[592] Cour d'appel de Paris, 30 octobre 2002, 12ème chambre.
Disponible à cette adresse : https://www.legalis.net/jurisprudences/cour-dappel-de-paris-12eme-chambre-section-a-arret-du-30-octobre-2002, [consulté le 16 novembre 2015].
[593] Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

B) La criminalité informatique organisée

Il convient de se demander si les règles relatives à la criminalité organisée sont applicables de manières opportunes dans la lutte contre la cybercriminalité dissimulée. L'instauration de l'Agence nationale de la sécurité des systèmes d'information[594] n'a pas été suffisante. Le Darknet a montré à quel point la cybercriminalité pouvait être organisée. En effet, les attaques informatiques ont évolué et se sont complexifiées. Les entreprises peuvent être visées par le vol de données sensibles ou le cyber espionnage et la cybercriminalité de manière générale relève du crime organisé.

Sur Internet et plus particulièrement sur le Darknet, le législateur est confronté à de nombreuses formes de criminalités comme le trafic de stupéfiants, le terrorisme, la pédopornographie ou encore les infractions liées au traitement automatisé des données. Depuis une vingtaine d'années, ces infractions sont génératrices de troubles à l'ordre public conséquents. Dans ce contexte, les moyens d'investigation habituels, confiés aux enquêteurs, ne sont pas suffisants. Pour qu'enquêteurs et délinquants ou criminels puissent combattre à armes égales, la loi s'est rapidement adaptée. Par exemple, la loi n° 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme[595] a permis l'introduction des infractions relative au terrorisme dans le Code de procédure pénale, avant qu'elles soient transférées dans le Code pénal de 1994. Désormais, les règles dérogatoires sont nombreuses et peuvent s'ajouter de manière ponctuelle au gré du législateur et de ses interventions. La loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité[596] a modifié les dispositifs en place en créant une procédure dérogatoire pour la délinquance et la criminalité organisées, en abrogeant certains textes redondants et en généralisant plusieurs infractions comme le terrorisme, le trafic de stupéfiants et le proxénétisme à cette forme de criminalité. Cette politique législative a permis la mise en place d'une procédure pénale spéciale comparable au droit pénal spécial. Il en résulte un cadre procédural moins protecteurs des libertés individuelles en matières de délinquance et criminalité organisées. Pourtant, le Conseil constitutionnel ne censure pas souvent les règles procédurales relatives à la criminalité organisée. Cela s'explique par le fait qu'elle cause un trouble à l'ordre public non négligeable. Dès lors, Le législateur a la possibilité

[594] L'ANSSI est un service français créé par décret en juillet 2009.
[595] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000693912.
[596] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995.

d'envisager des mesures d'investigations particulières afin de découvrir et poursuivre des délits et des crimes d'une gravité et d'une complexité extrêmes, lorsque qu'elles sont conduites conformément aux prérogatives de l'autorité judiciaire, qui veille au respect des libertés individuelles et lorsque les entorses procédurales sont proportionnées à la complexité et à la gravité des infractions, nécessaires à la manifestation de la vérité et ne créent pas de discriminations non justifiées.

Le droit pénal français envisage deux possibilités de criminalité organisée pour les infractions d'atteinte aux STAD. Premièrement, l'article 323-4 du code pénal dispose que « *la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1*[597] *à 323-3-1*[598] *est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ». Ainsi, le Code pénal vise les personnes qui s'entendent pour commettre une atteinte à un système de traitement automatisé de données.

Secondement, l'article 323-4-1 du Code pénal dispose que « *lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende* ».

L'attaque informatique par intrusion n'est pas la plus destructrice en termes de matériel. En effet, d'autres attaquent exploitent les faiblesses informatiques et peuvent avoir de lourdes conséquences. Le fait de saboter les systèmes informatiques en est le parfait exemple (§ 2).

§2) La répression du sabotage informatique

Les systèmes informatiques sont vulnérables et peuvent faire l'objet d'atteintes orchestrées par des hackeurs très performants. Ces attaques auxquelles tous les utilisateurs sont confrontés

[597] Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.
[598] Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

visent aussi bien les données que les systèmes informatiques et peuvent engendrer de nombreuses pertes financières.

Le sabotage informatique englobe un certain nombres d'actes illégaux. Le terme sabotage est défini comme l'acte « *qui a pour but de détériorer ou de détruire intentionnellement du matériel*[599] ». Dans le milieu informatique, le sabotage est utilisé par des pirates qui s'attaquent à un système informatique. Les victimes peuvent être des particuliers mais sont le plus souvent des entreprises. Avec l'essor d'Internet, elles sont devenues très vulnérables aux attaques internes. En effet, la criminalité informatique a évolué grâce à l'absence de frontières sur Internet et le sabotage informatique est à la portée de tout hackeur souhaitant exploiter les caractéristiques d'Internet : universalité, accessibilité, centralisation…

Grâce à de nombreuses techniques comme le « *DDOS* » ou déni de service, les hackeurs sabotent et déstabilisent des systèmes informatiques. Mais, entreprises et particuliers subissent également le sabotage des données informatiques stockées sur les systèmes. Elles peuvent être supprimées, détériorées ou modifiées à la suite d'une intrusion dans un système informatique alors que le sabotage d'un système informatique peut être effectué depuis l'extérieur sans intrusion grâce à l'utilisation d'un virus informatique. En tout état de cause, le sabotage d'un système informatique peut entraîner indirectement la perte de données qui s'y trouvaient.

Avec la loi dite Godfrain le législateur a voulu donner un cadre juridique à la sécurisation des systèmes informatiques. Il a donc visé le sabotage des systèmes informatiques (A) ainsi que celui des données informatiques (B).

A) Le sabotage contre les systèmes informatiques

Les formes du sabotage informatique sont nombreuses. Il peut s'agir d'une destruction, d'une détérioration, d'une modification ou d'une saturation via un déni de service etc. Le code pénal vise le sabotage effectué à la suite d'une intrusion ou d'un maintien frauduleuse dans le système informatique (1) et le sabotage informatique volontaire (2).

[599] Définition disponible à cette adresse : https://www.larousse.fr/dictionnaires/francais/sabotage/70379.

1. Le sabotage involontaire contre les systèmes informatiques postérieur à une intrusion

L'alinéa 2 de l'article 323-1 du Code pénal concerne le sabotage des systèmes informatiques : « *Lorsqu'il en est résulté (...) une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende* ».

Le législateur a souhaité encadrer les atteintes involontaires aux systèmes de données en aggravant la peine de l'accès et du maintien frauduleux à un système informatique lorsque cet acte est suivi d'une atteinte involontaire. Pour la doctrine cet alinéa concerne les atteintes de sabotage involontaires puisque l'article 323-2 du Code pénal vise les mêmes faits commis volontairement. Il y a une différence entre le sabotage involontaire et le sabotage recherché : « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende* ». Ainsi, le sabotage prévu à l'alinéa 2 de l'article 323-1 du Code pénal est une conséquence de l'acte d'intrusion d'un hackeur si bien qu'il ne peut qu'être involontaire. Dès lors, l'élément moral n'a pas à être recherché. En effet, dans ce genre d'hypothèses, l'individu a souhaité l'accès frauduleux au système informatique mais n'a pas voulu l'altération du système en cause. Un tel sabotage serait alors dû à une maladresse ou à une sécurité automatique. Dans une optique répressive, le législateur a érigé en circonstance aggravante le sabotage involontaire d'un système informatique effectué à la suite d'une intrusion volontaire. Dès lors, l'élément moral du sabotage involontaire d'un système informatique résulte de la matérialité de l'acte. Le législateur a mis en place un régime très protecteur protégeant les systèmes informatiques des attaques involontaires mais aussi volontaires (2).

2. Le sabotage volontaire contre les systèmes informatiques

L'article 323-2 du Code pénal dispose que « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende* ». Cet article a vocation à incriminer les attaques de sabotage volontaires contre les systèmes informatiques. Ce genre d'attaque peut porter atteinte aux particuliers et aux entreprises et constituent une menace singulière pouvant avoir d'énormes conséquences matérielles.

Le législateur est resté très vague en ce qui concerne la matérialité du texte comme le prouve les termes utilisés : « *entraver* » et « *fausser* ». Utiliser pour d'autres infractions comme l'entrave à la justice[600] par exemple , l'entrave est définie dans le langage courant comme « *ce qui retient*[601] », et dans le langage informatique comme ce qui perturbe « *le fonctionnement du système de traitement automatisé de données de manière non irréversible et temporaire, sans que la nature de ce fonctionnement soit affectée*[602] ». Ainsi, l'élément matériel du sabotage d'un système informatique est très large et peut supposer une dégradation, une modification, une perturbation ou même une suppression.

Pour la jurisprudence, l'entrave est un acte positif qui vise directement le fonctionnement du système de traitement automatisé de données afin de ralentir sa capacité[603]. Concernant la différence entre le fait de fausser et le fait d'entraver, elle porte sur l'idée que le fait de fausser à des conséquences irréversibles tandis que l'entrave est un acte temporaire[604].

Contrairement à l'acte de sabotage prévue par l'article 323-1 alinéa 1er du Code pénal, le sabotage volontaire sera constitué nonobstant le caractère autorisé ou non de l'accès. En effet, il ne s'agit pas de la conséquence d'un accès frauduleux mais il s'agit d'un acte qui constitue en soi une infraction. Le hackeur doit avoir la volonté et la conscience de commettre le délit mais l'élément moral étant présumé, c'est l'élément matériel qui le révèle. Outre le sabotage des systèmes informatiques, la loi réprime le délit de sabotage visant les données (B).

B) Le sabotage visant les données

Le législateur a pris le soin de déterminer plusieurs infractions afin de séparer les atteintes aux systèmes informatiques des attaques aux données qu'ils contiennent. Ces dernières font également l'objet d'une protection distincte de celle des systèmes informatiques puisqu'un

[600] Code pénal art. 434-1.
[601] Définition disponible à cette adresse : https://www.notrefamille.com/dictionnaire/definition/entrave.
[602] CASILE J-F., *Le Code pénal à l'épreuve de la délinquance informatique*, Presses Universitaires d'Aix-Marseille- P.U.A.M, 2002, page 130.
[603] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 70 : « *Dans cet arrêt, la Cour adopte donc une interprétation restrictive de la notion d'entrave, conduisant à admettre que l'acte d'entrave ne peut être caractérisé que par une action positive visant directement le fonctionnement d'un système informatique, dont le résultat est la création d'un état de ralentissement de la capacité du système en cause* ».
[604] CASILE J-F, Ibid., page 128.

système peut être atteint sans que ses données soient visées et à l'inverse, les données peuvent être visées sans que le système soit atteint.

Lorsque le sabotage informatique vise les données, plusieurs articles ont vocation à s'appliquer. Il y a l'article 323-1 alinéa 2 du Code pénal qui vise « *(...) la suppression ou la modification de données contenues dans le système (...)* », et l'article 323-3 du Code pénal qui vise « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* ». Pour ce dernier article la peine est de cinq ans d'emprisonnement et de 150 000 euros d'amende alors que la peine pour l'alinéa 2 de l'article 313-1 du Code pénal de trois ans d'emprisonnement et de 45 000 euros d'amende.

Néanmoins, ces textes s'appliquent aux mêmes situations puisque l'alinéa 2 de l'article 323-1 du Code pénal ne vise que le sabotage de données postérieur à l'accès et/ou au maintien frauduleux (1) alors que l'article 323-3 du Code pénal concerne seulement le sabotage de données (2). C'est au juge de vérifier si les faits permettent l'application de l'un ou de l'autre article même si dans la pratique ce n'est pas si simple.

1. Le sabotage involontaire de données postérieur à une intrusion

Le texte de l'article 323-1 alinéa 2 du Code pénal dispose que : « *Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système (...) la peine est de trois ans d'emprisonnement et de 100 000 € d'amende* ». Ce texte incrimine de manière claire le sabotage de données à la suite d'une intrusion frauduleuse dans un système informatique. La formule « *données contenus dans le système* » semble englober l'ensemble des données à savoir les données traitées par les ordinateurs qui n'influencent pas leur fonctionnement, et les données informatiques qui permettent de les faire fonctionner. Le sabotage des premières n'a aucune conséquence sur le fonctionnement du système contrairement au sabotage des secondes. Néanmoins, pour la doctrine, une incertitude réside quant au champ d'application de cet article. D'aucuns estiment que les données informatiques sont indissociables du système informatique si bien que leur perte crée une « *altération du fonctionnement du système* ». En effet, la plupart de ces altérations sont dues à une suppression ou à une modification de données essentielles au bon fonctionnement du système informatique. Le législateur n'est pas intervenu et a préféré

envisagé un concours de qualifications entre plusieurs incriminations comme le suggérait la doctrine[605].

Selon cette dernière, à l'instar du sabotage informatique, pour cet article l'atteinte aux données n'est qu'une conséquence involontaire du délit d'accès ou de maintien frauduleux prévu à l'alinéa 1er. Une telle conséquence n'est pas érigée en infraction autonome mais en circonstance aggravante lorsqu'à la suite d'une intrusion le pirate affecte les données du système informatique. Néanmoins, d'aucuns se demandent comment la justice pourrait faire la différence entre le sabotage volontaire et le sabotage involontaire sachant qu'un pirate informatique pourrait se prévaloir de l'article 323-1 alinéa 2 du Code pénal pour échapper à la peine plus élevée de l'article 323-3 du Code pénal[606]. En réalité, la présence de ces deux textes est nécessaire en ce qu'elle permet la répression des atteintes involontaires aux données tandis que l'article 323-3 du Code pénal tend à assurer une protection des données contre les actes volontaires de sabotage (2).

2. Le sabotage de données volontaires

L'article 323-3 du Code pénal dispose que « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende* ». Il vise donc à punir les atteintes frauduleuses c'est-à-dire les atteintes volontaires aux données qui peuvent désormais avoir une valeur élevée. Toutefois, certaines victimes préfèrent agir en dehors du cadre législatif. En effet, des groupes de travail vont tenter de récupérer des données importantes qui ont fuité sans attendre l'intervention des autorités qui peut être très longue.

Le commerce de données existe sur le Darknet. Ces données deviennent illicites lorsqu'elles sont issues de vols ou d'autres incriminations. Le vol de données est un délit qui a été consacré

[605] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 73.
[606] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 72 : « Par ailleurs, la tâche qui incombe aux juges du fond semble délicate dans la mesure où la caractérisation de l'élément moral semble être difficile ».

par la Cour de cassation le 20 mai 2015[607] avant d'être consacré par la loi du 13 novembre 2014 modifiant l'article 323-3 du Code pénal. Le trafic de données illicites peut également être qualifié de recel, un délit puni de cinq ans d'emprisonnement et de 375 000 euros d'amende. En effet, l'article 321-1 du Code pénal dispose que « *le recel est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit* ». Il faut donc que les données soient détenues ou transmises en sachant qu'elles proviennent d'une infraction. Ainsi, le recel peut concerner l'individu qui fera du commerce avec les données et l'individu qui en bénéficiera. Les transactions de données illicites sur le Darknet sont visées par cet article.

Par ailleurs, l'informatique facilite également les atteintes aux organisations. Ce sont les actes réalisés par le biais d'Internet et qui portent atteintes aux institutions privées. C'est le cas pour l'espionnage industriel, les attaques concurrentielles, pour la falsification, la défiguration de sites web, pour le piratage de logiciels, les atteintes au droit d'auteur, à la propriété intellectuelle, au droit des marques, pour les intrusions non autorisées dans les systèmes informatiques, l'indisponibilité des services, pour l'usage de l'infrastructure informatique de l'entreprise, pour la réalisation de crimes économiques, pour le chantage consécutif à la prise en otage des ressources informatiques ou pour la manipulation d'information.

Face à de tels risques, les entreprises préfèrent agir indépendamment des autorités. En effet, des programmes informatiques comme *CybelAngel*[608] permettent de scanner le Darknet. La start-up française propose une solution intéressante pour lutter contre la vente d'informations sur le Darknet. Erwan Keraudy, cofondateur de *CybelAngel* donne des précisions concernant les méthodes utilisées : « *Pour ce qui est du dark Web, nous utilisons un système de crawling : notre machine analyse le contenu qui y est indexé page après page. On retrouve ainsi des millions de cartes bleues, de mails dérobés et des bases de données entières*[609] ». L'entreprise est capable de repérer des centaines de millions de documents par jour, en accès libre sur Internet et le Darknet. Lorsqu'elle découvre une fuite de documents, l'entreprise avertit ses

[607] Dans l'affaire « *Bluetouff* » elle confirme la condamnation d'un blogueur pour « *maintien frauduleux dans un système de traitement automatisé de données* » et pour le vol de données.
[608] Disponible à cette adresse : https://www.cybelangel.com/?lang=fr.
[609] TRUJILLO E., *CybelAngel lève 3 millions d'euros pour surveiller le dark Web et les objets connectés*, 7 juin 2017. Disponible à cette adresse : http://www.lefigaro.fr/secteur/high-tech/start-up/2017/06/07/32004-20170607ARTFIG00003-cybelangel-leve-3-millions-d-euros-pour-surveiller-le-dark-web-et-les-objets-connectes.php, [consulté le 8 juillet 2017].

clients qui peuvent ainsi éviter une utilisation malveillante. L'impact négatif de l'informatique ne se limite malheureusement pas à la criminalité informatique car la cybercriminalité est une notion plus large. Comme ce fut le cas avec Internet, l'émergence du Darknet affecte énormément le domaine de la criminalité en offrant notamment à ses acteurs une rapidité d'action, la possibilité de se former et un anonymat. La cybercriminalité concerne également les infractions qui existaient avant son apparition. Ces infractions classiques qui ont été facilitées grâce à Internet le sont encore plus avec le Darknet. Il convient d'étudier la répression de ces infractions que la loi encadre comme si elles avaient été commises sur Internet puisqu'aucun texte ne fait référence au Darknet (Section 2).

SECTION 2
LA REPRESSION D'INFRACTIONS ANCIENNES COMMISES SUR LE DARKNET

La criminalité organisée classique s'est sans réelle difficulté adaptée à la mondialisation et à l'essor d'Internet et du Darknet. Il convient de se demander si le droit pénal a su contrôler cette nouvelle criminalité, en adoptant des règles spécifiques, ou s'il s'est contenté de lui appliquer des règles anciennes. Ainsi, l'objectif de cette section est de montrer dans quelles mesures la loi pénale française s'applique à la répression des infractions dites de droit commun commises sur Internet, et aux particularités frappant les infractions commises sur le web dissimulé.

Les conséquences considérables des infractions commises sur le Darknet concernent plusieurs types d'infractions classiques comme le trafic d'armes, le recours à un tueur à gage, l'escroquerie, la pédopornographie, le trafic de stupéfiants ou le terrorisme. Cette section sera consacrée à ces trois derniers phénomènes. Il s'agira de traiter d'une part la répression des menaces contre la société (§1) et d'autre part, la répression des menaces contre les enfants (§2).

§1) La répression des menaces contre la société

La criminalité organisée a saisi les opportunités offertes par le Darknet en utilisant toutes ses caractéristiques pour mettre en place des supermarchés de la drogue. Le réseau sombre a permis à certains cybercriminels de se moderniser et de profiter de l'anonymat, de la clandestinité, du chiffrement, de la décentralisation, des cryptomonnaies et de l'absence de frontière.

Ce paragraphe examinera la répression de deux des plus grosses menaces du Darknet, le trafic de stupéfiants (A) et le terrorisme (B).

A) Les infractions à la législation sur les stupéfiants

Selon un rapport de l'Observatoire européen des drogues et des toxicomanies, les morts par overdose ont augmenté de 6% entre 2014 et 2015[610] en Europe. De 7950 victimes en 2014 on

[610] FRANCE TV INFO, *Drogues : le nombre de morts par overdose,* le 6 juin 2017. Disponible à cette adresse : https://www.francetvinfo.fr/societe/drogue/drogues-le-nombre-de-morts-par-overdose-augmente-en-europe_2224935.html, [consulté le 9 octobre 2017].

est passé à 8441 en 2015. Face à la consommation croissante de substances telles que la morphine ou l'héroïne, certains experts américains parlent de niveau épidémique.

Le Darknet a permis la naissance de nouveaux marchés de la drogue tels que *Silkroad* ou *Alphabay* et les transactions illicites entre clients et trafiquants de drogues se sont multipliées. En effet, protégé par la cryptologie, l'anonymat et la rapidité du transfert de données, les trafiquants agissent avec un sentiment d'impunité et les clients sont rassurés par les méthodes d'envoi. L'Observatoire européen des drogues et des toxicomanies met en avant l'usage croissant du Darknet dans les échanges illicites de stupéfiants. Dès lors, les autorités nationales qui tentent d'intercepter les colis postaux saisissent d'importantes quantités de drogue.

Les sites du Darknet sont de différentes natures, certains proposent de la drogue de manière non équivoque et assument leur qualité de dealer tandis que d'autres mettent en place des pharmacies virtuelles pour un commerce en apparence légal. Sur d'autres sites, des militants échangent sur des thèmes mélangeant drogue et santé ou proposent des sites dits « *instructifs* » afin de donner des recettes pour la fabrication de drogue ou d'en promouvoir la consommation et la production. En tout état de cause, avec ces marchés, on assiste à une vulgarisation de la drogue et à la défense d'un usage et d'un commerce libres. Les consommateurs ont accès à toutes les instructions nécessaires à la fabrication de drogues de synthèse, à plusieurs sites de mauvaises médecines et à des services de prescriptions médicales en ligne à payer en bitcoin.

Toutefois, ces marchés de la drogue sont fragilisés par une donnée qu'il faut garder à l'esprit. Certes les échanges sont anonymes et dématérialisés, mais une opération de livraison de drogues nécessite une intervention physique du vendeur qui doit livrer le produit et de l'acheteur, qui doit le récupérer. C'est dans ce contexte que les enquêteurs arrivent à mettre la main sur trafiquants et clients[611], et que la loi pénale à vocation à s'appliquer.

En France, la législation en matière de stupéfiants est très sévère : sont interdits l'usage, l'acquisition, la cession, l'offre, la détention, le transport, l'exportation, l'importation, la fabrication et la production de stupéfiants. La lutte contre ce fléau est un réel défi auquel sont

[611] BFM TV, *Il commande de la drogue sur Internet, les douaniers lui livrent son colis*, 21 mai 2017. Disponible à cette adresse : https://www.bfmtv.com/police-justice/il-commande-de-la-drogue-sur-internet-les-douaniers-lui-livrent-son-colis-1168716.html, [consulté le 7 octobre 2017].

confrontés législateur et forces de police. Il convient d'étudier la notion de stupéfiants (1), et les différentes incriminations (2).

1. La notion de stupéfiants

Alors qu'elle était prévue dans le code de la santé publique[612], la législation relative au trafic de stupéfiants a été intégrée au sein du code pénal dans le droit commun des atteintes volontaires à l'intégrité physique ou psychique de la personne humaine. Le législateur a d'ailleurs saisi cette occasion pour incorporer de nouvelles infractions au sein de ce même code. Toutefois, l'intégration n'a pas été totale puisque les infractions d'usage illicite de stupéfiants et de provocation à l'usage ou au trafic de stupéfiants demeurent dans le code de la santé publique respectivement aux articles L.3421-1 et L.3421-4.

D'après l'article 222-41 du Code pénal « *constituent des stupéfiants au sens des dispositions de la présente section les substances ou plantes classées comme stupéfiants en application de l'article L. 5132-7 du code de la santé publique* ». Il y a donc un renvoi au Code de la santé publique pour la définition de la notion de stupéfiants dans la mesure où elle est l'œuvre du pouvoir réglementaire[613]. Pour exemple, il est possible de citer le cannabis, les champignons hallucinogènes, le LSD, les amphétamines, la cocaïne, l'héroïne, la morphine ou encore l'opium. Toutes ces substances se trouvent en vente libre sur le Darknet. La politique française en matière de répression des stupéfiants est très récente. C'est la loi n°70-1320 du 31 décembre 1970 relative aux mesures sanitaires de lutte contre la toxicomanie, et à la répression du trafic et de l'usage illicite des substances vénéneuses[614] qui va définir le cadre légal. Elle réprime alors l'usage et le trafic illicite de produits stupéfiants en créant une dualité de définition entre le trafiquant d'un côté et le consommateur de l'autre, qui est à la fois malade et délinquant. Ce qui amène alors à traiter les différentes incriminations relatives aux infractions en matière de stupéfiants (2).

2. Les différentes incriminations

[612] Code de la Santé publique Art. L.627 et suivants.
[613] Par arrêté du ministre chargé de la santé pris sur proposition du directeur général de l'Agence française de sécurité sanitaire des produits de santé.
[614] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000321402.

Le législateur a affirmé une volonté rigoureuse en matière de lutte contre le trafic de drogue en adoptant plusieurs textes. D'autres dispositions ont suivi la loi du 31 décembre 1970 précitée en faisant évoluer le cadre légal. Il est possible de citer la loi n°86-76 du 17 janvier 1986 portant diverses dispositions d'ordre social[615], la loi n°87-1157 du 31 décembre 1987 relative à la lutte contre le trafic de stupéfiants et modifiant certaines dispositions du Code pénal[616], la loi n°90-614 du 12 juillet 1990 relative à la participation des organismes financiers à la lutte contre le blanchiment des capitaux provenant du trafic des stupéfiants, la loi n°90-1010 du 14 novembre 1990 portant adaptation de la législation française aux dispositions de l'article 5 de la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes, fait à Ville le 20 décembre 1988, et la loi n°91-1264 du 19 décembre 1991 relative au renforcement de la lutte contre le trafic des stupéfiants. Ensuite, le nouveau code pénal durcit la législation en incriminant le « *trafic organisé* » et en criminalisant certains délits. De plus, à l'exception de l'usage de stupéfiant, toutes les dispositions relatives à la lutte contre la drogue issues du code de la santé publique sont reprises par le code pénal.

Dix ans plus tard, le législateur adopte la loi n°2004-204 du 9 mars 2004 portant sur l'adaptation de la justice aux évolutions de la criminalité[617] dite Perben II, afin de lutter contre la criminalité organisée. Elle ajoute de nouvelles dispositions en matière de lutte contre la drogue et opère une distinction entre la criminalité organisée grave et celle qui l'est moins. En matière de lutte contre le trafic de stupéfiants des règles de procédures particulières sont prévues[618].

Concernant le trafic de stupéfiants sur Internet et le Darknet, le code pénal reste muet. Il n'y a pas de référence aux réseaux. Dès lors, il faut en déduire que la répression du trafic de stupéfiants commis via le Darknet relève de l'application du droit pénal commun et de l'ensemble des lois annexes. Le Code pénal prévoit plusieurs dispositions réprimant ce genre de trafic nonobstant le moyen utilisé. Ces infractions peuvent être de nature criminelle (a) ou délictuelle (b). Evidemment, seul le trafic illicite est pénalement sanctionné. Cela exclut le personnel médical ou les pharmaciens qui sont habilités par la loi à faire du commerce de produits de cette nature. C'est également le cas pour les agents qui procèdent à des opérations

[615] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000317532.
[616] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000512241.
[617] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995&dateTexte=&categorieLien=id.
[618] Elles seront abordées dans la Partie II, Titre II, Chapitre II.

d'infiltration dans le cadre des articles 706-81 et suivants du code de procédure pénale et qui ne pourront pas être poursuivis pour l'acquisition, la détention ou le transport de substances stupéfiantes.

a) Les qualifications criminelles

Tout d'abord, « *le fait de diriger ou d'organiser un groupement ayant pour objet la production, la fabrication, l'importation, l'exportation, le transport, la détention, l'offre, la cession, l'acquisition ou l'emploi illicites de stupéfiants* » est puni par l'article 222-34 du code pénal « *de la réclusion criminelle à perpétuité et de 7 500 000 euros d'amende* ». Il s'agit de la direction ou de l'organisation d'un groupement. Cette infraction ne se conçoit pas lorsqu'il y a l'utilisation de groupements ou de structures déjà existantes pour faciliter la commission de l'infraction. Elle suppose en réalité la création ou la direction de groupements, destinés spécialement à l'accomplissement d'une ou plusieurs modalités de trafic de stupéfiants visé par le code pénal. Ensuite, « *la production ou la fabrication illicites de stupéfiants sont punies* » par l'article 222-35 du Code pénal « *de vingt ans de réclusion criminelle et de 7 500 000 euros d'amende* ». Il s'agit de la production ou de la fabrication illicites. Cette disposition vise directement les membres de l'organisation chargée de produire ou de fabriquer les stupéfiants, comme les chimistes qui transforment les matières premières ou les plantes de champs de cannabis. Enfin, constitue un crime puni de trente ans de réclusion et de 7,5 millions d'euros d'amende, l'importation ou l'exportation illicite de stupéfiants commises en bande organisée[619]. Outre ces qualifications criminelles, il y a aussi des qualifications délictuelles (b).

b) Les qualifications délictuelles

Plusieurs formes de trafic sont sanctionnées par le Code pénal comme délits. Ainsi, l'article 222-36 alinéa 1er dispose que « *l'importation ou l'exportation illicites de stupéfiants sont punies de dix ans d'emprisonnement et de 7 500 000 euros d'amende* ». Ces faits n'ont pas de qualification criminelle lorsqu'ils n'ont pas été commis en bande organisée. Ensuite, l'article 222-37 alinéa 1er du Code pénal punit des mêmes peines que ci-dessus « *le transport, la détention, l'offre, la cession, l'acquisition ou l'emploi illicites de stupéfiant* ». Ces termes

[619] Code pénal art. 222-36 alinéa 2.

permettent de poursuivre l'activité des intermédiaires, grossistes, semi-grossistes ou vendeurs au détail. C'est ce type de profil qui se retrouve le plus sur le Darknet. La jurisprudence refuse de faire une différence selon la quantité du produit saisie[620].

En outre, le Code pénal, à l'article 222-37 alinéa 2, incrimine les procédés destinés à « *faciliter, par quelque moyen que ce soit, l'usage illicite de stupéfiants, de se faire délivrer des stupéfiants au moyen d'ordonnances fictives ou de complaisance, ou de délivrer des stupéfiants sur la présentation de telles ordonnances en connaissant leur caractère fictif ou complaisant* ». Ce texte permet de sanctionner les individus qui apportent sciemment leur aide à l'usage de stupéfiants, comme un gérant de discothèque ou le médecin qui délivre une fausse ordonnance.

L'article 222-39 du Code pénal punit la vente au détail de cinq ans d'emprisonnement et de 75 000 euros d'amende : « *la cession ou l'offre illicites de stupéfiants à une personne en vue de sa consommation personnelle sont punies de cinq ans d'emprisonnement et de 75 000 euros d'amende* ». Le législateur entend punir le trafiquant qui se situe en bout de chaîne, le petit dealer qui vend au détail quelques doses. Enfin, le Code de la santé publique punit l'usage illicite de stupéfiants d'un an d'emprisonnement et de 3 750 euros d'amende[621]. La Cour de cassation[622] a jugé que la qualification d'usage illicite exclut celle de détention si les produits n'étaient destinés qu'à l'usage personnel du prévenu. L'article L.3421-4 du même code incrimine « *la provocation au délit prévu par l'article L.3421-1 ou à l'une des infractions prévues par les articles 222-34 à 222-39 du code pénal, alors même que cette provocation n'a pas été suivie d'effet* ». Ainsi, ce texte punit toute provocation à la fabrication, à l'importation, à l'exportation, à la production, à la détention, au transport, à l'acquisition, à la cession, à l'offre, à l'usage illicite organisé ou non organisé de stupéfiants mais aussi « *le fait de présenter ces infractions sous un jour favorable* ». Par exemple, le fait de publier sur le Darknet des informations relatives aux lieux de disponibilité de stupéfiants ou des recettes pour la fabrication de drogue de synthèse entre dans le champ de cet article.

[620] Cour de cassation, chambre criminelle, 17 octobre 1994, Bulletin criminel n°334.
[621] Code de la santé publique Art. L.3421-1.
[622] Cour de cassation, chambre criminelle, 14 mars 2017, n°16-81805 : « *en réprimant spécifiquement l'usage illicite de stupéfiants, pour consommation personnelle, le législateur a entendu ne pas sanctionner lesdits usagers pour les délits de l'article 222-37 du code pénal sur le trafic de stupéfiants dès lors que tout consommateur est nécessairement tenu d'acquérir et de transporter ces stupéfiants* ».

L'achat de drogue hors-ligne est conditionné par des critères géographiques et relationnels. Mais, sur le Darknet les paramètres sont différents dans la mesure où les fournisseurs sont des milliers à opérer à travers le monde. Pour le trafic de stupéfiants facilité par le Darknet, les peines encourues sont les mêmes dans la mesure où il n'y pas de circonstance aggravante lorsque l'infraction est commise au moyen d'un réseau d'information et de communication. Ces dispositions ont vocation à s'appliquer « *aux infractions commises sur le territoire de la République*[623] ». Par exemple, le créateur de *Silkroad 2.0* Blake Benthall a été visé par une enquête menée par les autorités de cinq pays, dont la France. S'il avait été jugé en France, il aurait encouru la peine prévue par l'article 222-34 du Code pénal pour le crime de direction et d'organisation d'un groupement dont le but est d'importer, d'exporter, d'offrir et d'acquérir des produits stupéfiants.

Pour les marchés français, un vendeur régulier isolé encourt dix ans d'emprisonnement et 7,5 millions d'euros d'amende[624] alors qu'un vendeur, acheteur occasionnel de petites quantité encourt cinq ans et 75 000 euros d'amende,[625] lorsque la transaction est faite en vue de la consommation personnelle du client. Enfin, l'acheteur isolé qui ne souhaite participer à aucun trafic, et qui achète sa drogue sur le Darknet pour sa consommation personnelle, encourt un an d'emprisonnement et 3750 euros d'amende[626].

Un autre sujet d'actualité a vocation à être étudié : le terrorisme. Il exploite les réseaux du Darknet afin de mettre en place des opérations. Des cellules secrètes, appartenant à des groupes terroristes comme Daesh échangent électroniquement sur le Darknet qui leur garantit un anonymat et un chiffrement quasi-absolus. La France a tenté de lutter contre ce fléau en mettant en place une politique très répressive dont il sera question dans le sous-paragraphe suivant (B).

B) La répression du terrorisme sur le Darknet

La première partie a montré que le Darknet est un facteur essentiel pour le progrès relatif à la liberté d'expression, à la censure ou encore à la vie privée. L'émergence de ce réseau de réseaux qui a profondément affecté l'Internet classique de manière positive a également une facette un

[623] Code pénal art. 113-2 alinéa 1er.
[624] Code pénal art. 222-37 alinéa 1er.
[625] Code pénal art. 222-39.
[626] Code de la santé publique art. L.3421-1.

peu plus sombre. En effet, le Darknet a été exploité par des criminels qui ont su commettre des infractions qui existaient bien avant l'arrivée du réseau sombre. Ces cybercriminels ont tiré parti de cette mutation d'Internet pour développer leurs activités criminelles. L'inquiétant exemple du terrorisme prouve que les cybercriminels ont su s'adapter aux nouvelles technologies. Le terme controversé de « *cyberterrorisme*[627] » a même fait son apparition à une époque où ce thème est constamment d'actualité. Le terrorisme classique a laissé place au terrorisme 2.0 qui utilise Internet et le Darknet comme moyens d'action. À titre d'exemple, les terroristes d'Al-Qaïda utilisaient des systèmes de messageries électroniques en les associant à des techniques de chiffrements pour garantir la confidentialité de leurs échanges lors de la préparation des attentats du 11 septembre[628].

Ces terribles attentats du 11 septembre 2001 ont entraîné une réaction quasi-immédiate de la communauté internationale qui a multiplié ses efforts pour prévenir et combattre le terrorisme. Face à la menace terroriste, les Etats ont décidé d'aménager leur droit pénal et leur procédure pénale afin de faire face aux spécificités de ce type de violence extrême. Récemment, à la suite des attentats commis sur le sol français[629], la France a modifié sa législation via des adaptions s'inscrivant dans le cadre général du droit pénal, refusant toute législation d'exception.

Le cyberterrorisme est considéré comme un acte terroriste commis via Internet. En effet, l'émergence des nouveaux moyens de communication tels que Internet, a permis au terrorisme de s'adapter. Internet et le Darknet sont des moyens de diffusion de messages et contenus tellement importants qu'ils font désormais office de média. Le Darknet permet également aux terroristes de communiquer entre eux pour leur organisation et de recruter de nouveaux partisans. Tor et *Telegram* sont des services qui leur permettent de recruter et de diffuser leur message.

[627] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 95 : « le cyberterrorisme peut être analysé comme l'activité d'un groupe terroriste dont l'objet est de commettre, par le biais d'Internet, dans la sphère nationale ou internationale, des actes qui ne couvrent pas seulement une catégorie d'infraction clairement définie comme terroriste, mais également un ensemble plus ou moins flou d'activités illicites en lien avec l'objectif terroriste. C'est une prolongation moderne via Internet de l'activité terroriste se déroulant sur le terrain réel ».
[628] BOOS R. La lutte contre la cybercriminalité au regard de l'action des États, Université de Lorraine, 2016, page 97.
[629] Il y a notamment eu l'attentat contre Charlie Hebdo du 7 janvier 2015, l'attentat du 13 novembre 2015 et l'attentat de Nice le 14 juillet 2016.

Les réseaux terroristes ont saisi les opportunités du Darknet et s'y sont adaptés pour poursuivre de la meilleure des manières leurs objectifs informationnels et offensifs. En effet, le Darknet est utilisé comme un moyen de propagande, comme un outil offensif mais aussi comme un moyen pour la collecte de fonds. En effet, le Darknet et les cryptomonnaies sont utilisés pour la mise en place de collecte de fonds. L'argent est le nerf de la guerre et aucun groupe ne peut subsister sans financement.

En tant qu'outil de propagande terroriste, le Darknet est utilisé comme un support média permettant la diffusion de messages, de contenu violent, de revendication d'attentats. Les terroristes le savent, l'information a un rôle stratégique dans un monde où la technologie est omniprésente. Conscients du rôle stratégique que les réseaux ont dans cette guerre, les terroristes exploitent le Darknet pour y diffuser des images par le biais de celui-ci. En tant que média sur lequel l'anonymat est préservé, il offre aux terroristes une transmission sécurisée, rapide et une couverture presque illimitée dans la mesure où ce contenu est très souvent repris sur le web visible. Les sites du Darknet sont de différentes sortes. Certains sont élaborés par des activistes ou même des des dirigeants de groupes terroristes, afin de paraître crédibles. Ainsi, leur but est informationnel et leurs discours bien étudiés. Ces sites aspirent à être les plus crédibles possibles, et ne veulent pas se faire passer pour des sites terroristes. Par exemple, pour Daesh ces sites permettent aux utilisateurs de consulter du contenu lié à l'Islam : feuilletage en ligne du Coran, écoute de chants musulmans… En réalité, ces sites vont permettre de filtrer un bon nombre d'individus. C'est à ce moment qu'entrent en scène les autres sites. Ces derniers sont non équivoques et montrent des images de crimes, de massacres de « *mécréants* » et incitent les extrémistes à commettre des crimes et des délits. Les conséquences de ces sites sont dévastatrices. En effet, les images véhiculées sont à dessein choquantes. A l'instar des productions Hollywoodiennes, les groupes terroristes misent sur le sensationnel. Il s'agit d'influer sur le moral du public et de motiver les futurs adhérents qui souhaiteraient mourir en martyre afin d'accéder au paradis[630].

Ensuite, le Darknet a un rôle essentiel dans la communication terroriste. En effet, son architecture décentralisée - basée sur le *friend-to-friend*, la rapidité des échanges, l'anonymat et le chiffrement des données - regroupe des caractéristiques conciliables avec le mode de

[630] En réalité, en Islam le suicide est interdit : « *Et ne vous tuez-pas vous-mêmes* » (Coran, Sourate 4, Verset 29).

fonctionnement des groupes terroristes. Ces derniers utilisent le potentiel du Darknet en matière de communication afin d'échanger à l'écrit par le biais de courriers électroniques ou d'applications chiffrées, et à l'oral via un darknet comme Freenet.

Enfin, de nouvelles menaces sont apparues puisque le terrorisme peut également utiliser Internet comme une arme offensive. Ainsi, le cyberterrorisme menace aussi bien le monde virtuel que le monde réel. Il convient de traiter dans un premier temps l'arsenal répressif en matière de cyberterrorisme (1), et dans un second temps, l'émergence de nouvelles infractions sur Internet (2).

1. L'arsenal répressif en matière de cyberterrorisme

Le cadre juridique français relatif au terrorisme a vocation à concilier plusieurs éléments essentiels dans un État de Droit comme la France, la répression et la prévention pour garantir la « *sûreté* » des citoyens d'un côté, et le respect des libertés individuelles de l'autre. La recherche de cet équilibre est l'un des principaux enjeux du terrorisme (a) qui fait l'objet de règles spécifiques de procédure pénale (b).

a) L'apologie du terrorisme

En matière d'apologie du terrorisme, la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a été votée afin de combler les lacunes mises en avant par les récents attentats. Elle compense les imperfections de la loi du 29 juillet 1881 sur la liberté de la presse qui n'est pas adaptée au numérique en y retirant les délits de provocation au terrorisme et d'apologie au terrorisme[631] pour les introduire dans le Code pénal à l'article 421-2-5 qui dispose que « *le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende* » ; « *les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne* ».

[631] Voir l'article 5 de la loi disponible à cette adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id.

Cette aggravation de la peine est applicable au Darknet qui est un « service de communication en ligne » ayant un « *effet démultiplicateur*[632] ». Désormais, les délits d'apologie de terrorisme et de provocation au terrorisme se voient appliquer le délai de prescription de l'action publique de droit commun qui est de trois ans[633] alors que ceux des délits de presse étaient de seulement trois mois.

Ensuite, toujours en matière d'apologie du terrorisme, la loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé a vocation à accentuer l'efficacité de la lutte contre le crime organisé qui comprend le terrorisme. Cette loi qui est une riposte à la menace terroriste consolide la cadre juridique pour une lutte plus efficace. En ce sens, l'article 421-2-5-1 du Code pénal dispose que « *le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes afin d'entraver, en connaissance de cause, l'efficacité des procédures prévues à l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou à l'article 706-23 du code de procédure pénale est puni de cinq ans d'emprisonnement et de 75 000 € d'amende* ». Il s'agit de punir les individus qui contribueraient à l'apologie du terrorisme en reprenant les propos des auteurs directs d'apologie du terrorisme ou en les consultant. Il s'agit d'une sorte de complicité ou de recel d'apologie du terrorisme. D'aucuns parlent même « *d'apologie de conséquence* ».

L'instrument juridique qui permet aux autorités administratives « *d'ordonner aux fournisseurs d'accès à Internet, le blocage de l'accès aux sites Internet incitant à commettre des actes terroristes ou en faisant l'apologie*[634] » a été introduit par l'article 9 de la loi du 13 novembre 2014 susmentionnée. Similaire au dispositif relevant de la pédopornographie[635], ce mécanisme

[632] Projet de loi n°2110 renforçant les dispositions relatives à la lutte contre le terrorisme, procédure accélérée, page 7. Disponible en PDF : http://www.assemblee-nationale.fr/14/pdf/projets/pl2110.pdf.
[633] La loi n°2017-242 du 27 février 2017 portant réforme de la prescription en matière pénale a modifié le délai de prescription de l'action publique des délits qui est de six ans.
[634] Projet de loi n°2110 renforçant les dispositions relatives à la lutte contre le terrorisme, procédure accélérée, page 9. Disponible en PDF: http://www.assemblee-nationale.fr/14/pdf/projets/pl2110.pdf.
[635] Article 4 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure modifiant l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique *« lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en* ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai ».

qui consiste à bloquer l'accès à un site Internet a été critiqué. En effet, dans un souci de célérité, cette compétence a été donnée aux autorités administratives plutôt qu'aux autorités judiciaires, qui auraient été plus légitimes compte tenu du fait qu'elles sont habilitées à poursuivre et réprimer les infractions. La Commission nationale consultative des droits de l'Homme estime qu'un tel mécanisme aurait dû « *relever de la compétence du juge des libertés, qui statuerait dans un délai bref de 48 ou 72 heures, sur saisine du parquet compétent*[636] ». Pour lutter contre la propagation de la menace terroriste, la consultation de site terroriste est également réprimée (b).

b) La consultation de site terroriste

La consultation de site faisant l'apologie du terrorisme n'est envisagée que par l'article 421-2-6 du code pénal lorsqu'elle est en relation avec la préparation d'une infraction terroriste.

Intégré par la loi n°2016-731 du 3 juin 2016, l'article 421-2-5-2 du code pénal a été abrogé par le Conseil constitutionnel. Il incriminait[637]« *le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende. Le présent article n'est pas applicable lorsque la consultation est effectuée de bonne foi, résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice* ».

La numérotation de cette incrimination montre l'ardeur législative relative à la lutte contre le terrorisme. Une première fois, le 20 février 2017, elle a été jugée contraire à la Constitution à la suite d'une QPC datant du 29 novembre 2016. Quelques jours plus tard, le Parlement s'est obstiné en votant un texte presque[638] similaire[639] que le Conseil Constitutionnel abrogera

[636] CNCDH, *Avis sur la refondation de l'enquête pénale*, Journal officiel du 10 mai 2014, texte n°84.
[637] Avant sa double abrogation par le Conseil constitutionnel le 10 février 2017 et le 15 décembre 2017.
[638] La notion d'absence de motif légitime a été ajoutée.
[639] Par la loi n° 2017-258 sur la sécurité intérieure du 28 février 2017 publiée le 1er mars 2017 au journal officiel comme suite : « *le fait de consulter habituellement et sans motif légitime un service de*

définitivement le 15 décembre 2017. Cette loi visait à prévenir l'endoctrinement de personnes disposées à commettre des actes terroristes à la suite de ce genre de consultation. Compte tenu du contexte actuel, une telle disposition aurait pu paraître fondée. Toutefois, le pouvoir législatif est tenu de respecter le principe de nécessité[640].

Selon le Conseil constitutionnel, il existe d'autres infractions poursuivant le même but. Les sages visent l'article 421-2-6 du Code pénal qui incrimine la préparation d'un acte terroriste et dont la matérialité peut s'envisager dans la consultation habituelle d'un « *ou plusieurs services de communication au public en ligne (...) provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie* ». Dès lors, pour le Conseil constitutionnel l'article 421-2-5-2 du Code pénal n'a pas semblé nécessaire à l'ordre juridique français.

En outre le Conseil constitutionnel a effectué un contrôle de proportionnalité[641] et a mis en avant une autre carence du législateur. En effet, l'atteinte à la liberté de communication n'était pas justifiée puisque le texte n'imposait pas assez de liens avec la commission d'actes terroristes. Aucune volonté de commettre des actes terroristes ou preuve d'adhésion à l'idéologie terroriste n'était imposée par le texte d'incrimination. D'aucuns estiment que ces carences auraient pu être compensées par l'alinéa 2 qui prévoyait que l'article n'était pas applicable lorsque la consultation était *« effectuée de bonne foi* », résultait « *de l'exercice normal d'une profession ayant pour objet d'informer le public* », intervenait « *dans le cadre de recherches scientifiques » ou était « réalisée afin de servir de preuve en justice* ». Cependant, il est compliqué de comprendre comment une consultation de site terroriste aurait pu être effectuée de « *bonne foi* » d'autant plus que l'incrimination ne requérait pas d'intention

communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directe- ment à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service.
Constitue notamment un motif légitime tel que défini au premier alinéa la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes ».

[640] « *En Droit, le principe de nécessité correspond à la conception qu'une norme ne cherchera à s'appliquer que si aucune autre solution ne peut être trouvée* » : https://fr.wikipedia.org/wiki/Principe_de_nécessité.

[641] « *Le principe de proportionnalité implique que la peine prononcée soit fonction de la gravité de l'infraction, de la situation du délinquant et de ses capacités de réinsertion* » : https://fr.wikipedia.org/wiki/Principe_de_proportionnalité.

terroriste au titre de son élément moral. En somme, la disposition manquait réellement de précision et de clarté.

Cependant, le législateur a persisté en réintroduisant l'article 421-2-5-2 dans le Code pénal : « *le fait de consulter habituellement et sans motif légitime un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service* ». En essayant d'aller dans le sens du Conseil constitutionnel il a pris la peine de préciser dans un second alinéa ce qu'il entendait par « *motif légitime* » ; « *constitue notamment un motif légitime tel que défini au premier alinéa la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes* ».

Ce nouvel article a également fait l'objet d'un renvoi en QPC par un arrêt du 4 octobre 2017[642]. Le Conseil constitutionnel a de nouveau effectué un contrôle de la constitutionnalité de l'atteinte supposée à la liberté de communication. Il estime que l'ajout de l'élément constitutif supposant la « *manifestation de l'adhésion à l'idéologie exprimée* » sur le site terroriste, ne suffit pas à caractériser formellement la volonté de commettre un acte terroriste. En somme, l'atteinte à la liberté de communication n'est pas proportionnée à la répression de ce qui semble s'apparenter à un acte de nature terroriste. Si le législateur souhaite toujours instaurer un délit de consultation de sites terroristes, il devra être plus précis et prendre en compte les critiques exposées par le Conseil constitutionnel en retenant comme élément constitutif de l'infraction l'intention terroriste. Cependant, compte tenu de la richesse de l'arsenal répressif en matière de terroriste, une telle démarche ne semble pas nécessaire.

Les actes commis sur Internet peuvent également porter atteintes aux personnes. Tel est le cas pour la diffusion de contenus offensifs[643] ,l'incitation à la haine raciale, la diffusion de

[642] Cour de cassation, chambre criminelle, 4 octobre 2017, n°17-90017.
[643] Virus, pornographie dure, scènes de violence…

propagande à caractère raciste ou xénophobe, la diffusion, l'intimidation, le chantage, le harcèlement, pour la mise à mal des données à caractère personnel, de la vie privée et de l'intimité, pour l'usurpation d'identité, etc. Ainsi, Internet a accentué la vulnérabilité de la société de manière générale, mais aussi des enfants. Outre les dangers exposés préalablement - virus informatique, accès à la drogue, terroriste - il existe un fléau qui a profité de l'essor des technologies et notamment du Darknet, il s'agit de la pédophilie. En effet, cette dernière est un phénomène criminel très ancien qui est entré dans une nouvelle dimension avec l'apparition d'Internet et encore plus avec le Darknet. Le contenu pédopornographique s'échangeait déjà dans les années soixante mais les apparitions d'Internet et du Darknet vont accentuer le la chose dans les années quatre-vingt-dix puis vers 2010. En effet, protégés par l'anonymat que le Darknet procure, les pédophiles ont su exploiter les nouvelles technologies de l'information et de télécommunication. Ainsi, le rôle incontestable du Darknet a permis à la pédophilie de devenir une forme de criminalité organisée qu'il faut combattre avec acharnement (§ 2)

§2) La lutte contre la pédophilie sur le Darknet

L'omniprésence du numérique a fragilisé les mineurs qui sont très actifs sur les réseaux pour consulter des sites web, regarder des films, écouter de la musique, faire des recherches scolaires, échanger via les réseaux sociaux ou se déplacer. Internet est accessible autrement que par un ordinateur puisqu'il s'applique aux tablettes tactiles mais aussi aux smartphones grâce à la 4G[644]. Internet conserve énormément d'informations, comme la géolocalisation, qui peuvent être utilisées par des personnes malintentionnées. Ces dernières utilisent les réseaux sociaux pour atteindre les victimes mineures ou utilisent des applications *peer-to-peer* afin d'échanger du contenu. En effet, les mineurs sont confrontés à énormément de contenu qui ne devrait pas leur être destiné puisque la diffusion de contenus pornographiques est illicite lorsqu'elle est destinée à un mineur ou susceptible d'être visionnée par lui. La moralité du mineur est aujourd'hui protégée.

« *La loi pénale française impose de ce fait le principe d'une certaine moralisation du réseau Internet*[645] ». En effet, le code pénal français est très protecteur des mineurs et a prévu une

[644] « En télécommunications, la 4G est la quatrième génération des standards pour la téléphonie mobile ». Disponible à cette adresse : https://fr.wikipedia.org/wiki/4G.
[645] JABBER A., *Les infractions commises sur Internet*, l'Harmattan, page 285.

section nommée « *de la mise en péril des mineurs*[646] ». Au sein de cette section, une infraction protège le mineur qui peut être destinataire de contenus pornographiques, elle est prévue à l'article 227-24 du Code pénal qui dispose que « *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 (…) 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, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur* ». Il n'y a pas de précision quant au support utilisable puisque le législateur a envisagé une approche ouverte prenant en compte l'évolution et donc le Darknet. Ce dernier est également visé par l'expression « *quelque moyen que ce soit* ».

L'idée est d'envisager un élément matériel suffisamment large[647] pour protéger les mineurs sur Internet, « *initialement conçue pour moraliser le Minitel, cette disposition permet donc de réprimer la diffusion via Internet de contenus pornographiques susceptibles d'être perçus par un enfant*[648] ». Il suffit que le contenu soit susceptible d'être vu ou perçu pour que l'infraction soit envisagée[649]. Cette précision est importante puisqu'Internet n'est pas régulé contrairement à la télévision ou au cinéma. Ainsi, ce texte pénal semble inadapté au réseau Internet et aux réseaux Darknet qui assurent un partage infini de données. Il est impossible de prendre en compte l'ensemble des échanges publics et privés d'Internet et du Darknet alors que pour certains l'article 227-24 du code pénal ne prend en compte que la diffusion publique. Néanmoins, le texte ne précise pas ce qu'il faut faire pour empêcher l'accès du contenu pornographique aux mineurs, sachant qu'il est possible qu'un mineur utilise les numéros de carte bancaire ou la pièce d'identité de ses parents pour s'inscrire sur un site pornographique payant.

[646] Partie législative, Livre II, Titre II, Chapitre VII, section 5.
[647] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 134.
[648] JABBER A., *Les infractions commises sur Internet, l'Harmattan,* page 294.
[649] Cour d'appel de Paris, 13ème chambre, 2 avril 2002 : « *il appartient à celui qui décide à des fins commerciales de diffuser des images pornographiques sur le réseau Internet dont les particulières facilités d'accès sont connues, de prendre les précautions qui s'imposent pour rendre impossible l'accès des mineurs à ces messages* ». Par ailleurs, « *les mises en garde et informations sur les logiciels de restriction d'accès présentes dans les pages d'accueil (…) ne sauraient être considérées comme des précautions utiles puisqu'elles interviennent alors que le mineur est déjà entré dans le site et n'empêchent nullement la vision des textes et photos de présentation qu'elles peuvent au contraire avoir pour effet de rendre attractives* », http://archive.dgmic.culture.gouv.fr/article.php3?id_article=443.

Mais, l'une des préoccupations majeures des États reste l'exploitation sexuelle des mineurs. En effet, le développement de la cybercriminalité implique celui de la pédopornographie qui a naturellement migrée vers le Darknet. Les actes pédophiles sont nombreux et peuvent prendre différentes formes. Les pédophiles exploitent les caractéristiques du réseau sombre afin d'agir dans l'obscurité la plus totale grâce à l'anonymat et au chiffrement des échanges. Informaticiens en herbe ou réels experts, les pédophiles se sont adaptés au Darknet si bien que des réseaux de pédophiles se sont rapidement formés, à tel point que le phénomène a pris une nouvelle dimension.

La pédophilie, activité criminelle ou délictuelle qui compromet l'intégrité morale et physique des mineurs, s'est développée avec l'essor d'Internet et du Darknet. Il s'agit du lieu de prédilection de beaucoup de pédophiles qui échangent ou créent du contenu. Les réseaux de pédophiles sont très actifs et représentent un réel fléau pour la société. Selon Thierry Boulouque, l'ancien patron de la BPM[650], pendant « *longtemps, ces prédateurs ont tourné autour des écoles. Aujourd'hui, grâce à internet, ils ont le monde entier à leur disposition*[651] ». Il faut préciser que le visionnage d'images ou de vidéos de pornographie infantile en ligne augmente les chances de passages à l'acte pédophile[652] : il s'agit d'un réel fléau.

Même s'il est impossible de connaître l'ensemble du volume du contenu pédopornographiques, différentes sources permettent d'établir des approximations et une tendance. En France, l'étude des statistiques du casier judiciaire et les différentes enquêtes policières permettent d'assurer qu'il s'agit d'une réelle menace non négligeable. En ce sens, le procureur adjoint au TGI de Créteil, Myriam Quéméner, affirme que « *la cyber-pédopornographie est en train de devenir un contentieux de masse* ». La loi n° 2007-293 du 5 mars 2007 reformant la protection de l'enfance et aggravant entre autres les peines de certains délits commis par le biais d'Internet n'a pas découragé les pédophiles. Il est alors opportun de se demander dans quelles mesures la législation française permet de lutter contre la pédopornographie. La singularité de cette forme de criminalité complique la tâche du législateur qui doit tenir compte de nombreuses contraintes

[650] Brigade de protection des mineurs.
[651] LOGEART A., *Comment les enquêteurs traquent les pédophiles sur Internet,* 30 mars 2014. Disponible à cette adresse : https://www.nouvelobs.com/l-enquete-de-l-obs/20130329.OBS6181/comment-les-enqueteurs-traquent-les-pedophiles-sur-internet.html, [consulté le 18 novembre 2016].
[652] https://www.fondation-enfance.org/2017/06/13/6674/.

telles que son caractère international.

Les espaces publics du Darknet comme les forums de discussions sont un moyen dynamique et interactif de communication sur des sujets relatifs à la pédophilie et les sites du Darkweb proposent même du contenu à caractère pédopornographique. Ces sites peuvent être personnels, commerciaux et idéologique c'est-à-dire prônant les relations sexuelles entre adultes et enfants. Tout au long de ce paragraphe, il s'agira de mettre en évidence les spécificités de la répression de la pédopornographie en étudiant l'arsenal législatif (A) et les services d'enquête (B).

A) L'arsenal législatif en matière de pédopornographie

Le sens étymologique du terme « *pédophilie* » conduit à « *l'amitié pour les enfants* », il est composé des radicaux grecs « *païs* » qui signifie « *enfant* » et « *philia* » qui signifie « *amitié* ». L'utilisation du terme « *pédérastie* » aurait été plus appropriée au sens actuel du terme « *pédophilie* » dans la mesure où il est composé des radicaux grecs « *païs* » et « *érôs* » qui signifient respectivement « *enfant* » et « *amour sexuel* ». Aujourd'hui, le terme « *pédophile* » a une connotation négative en étant souvent assimilé aux violeurs d'enfant. Mais, il peut en outre désigner la pédopornographie et l'utilisation de celle-ci. Les auteurs utilisent parfois le terme plus large de « *pédocriminalité* » pour viser les délits et crimes relevant à la fois d'abus sexuels sur mineur[653] et de pornographie mettant en scène des enfants.

Le réseau Darknet est devenu le lieu de prédilection de personnes ayant des pratiques répréhensibles portant atteinte à l'intégrité physique et morale des mineurs. Les pédophiles l'utilisent de plus en plus afin d'échanger du contenu pornographique impliquant des victimes mineures. Le fléau n'est pas négligeable et suppose une lutte efficace. En effet, des réseaux actifs de pédophiles se sont organisés et regroupés afin de proposer ou d'obtenir le plus de contenus pédopornographiques en évitant la répression des autorités. De vrais réseaux criminels pédophiles se sont mis en place. Toutefois, contrairement à Internet qui permet également aux pédophiles d'établir le contact avec des victimes mineures, le Darknet ne se cantonne pas qu'au simple échange de contenu pédopornographique. Il permet en effet de mettre en contact des

[653] Ministère de l'éducation nationale, 18 mai 2005. Disponible à cette adresse : http://www.education.gouv.fr/cid694/un-plan-de-lutte-contre-la-cyber-pedocriminalite.html, [consulté le 2 mai 2015].

pédophiles ou des trafiquants d'êtres humains[654] qui souhaiteraient créer eux-mêmes le contenu pédopornographiques en mettant en scène des mineurs. La vulnérabilité des enfants est accrue et le potentiel des réseaux pédophiles immense.

En droit et notamment en matière de lutte contre la pédophilie, la Convention des Nations Unies de 1989 relative aux droit de l'enfant[655] constitue une base répressive solide. Elle contraint les pays contractants à protéger les enfants contre toute forme d'exploitation sexuelle en prenant les mesures appropriées afin notamment « *que des enfants ne soient (pas) exploités aux fins de la production de spectacles ou de matériel de caractère pornographique*[656] ». Cette Convention aura des conséquences radicales sur le droit pénal français dans la mesure où elle est à l'origine de l'article 227-23 du Code pénal. Par suite, d'autres incriminations vont être apportées par le législateur. La loi n°98-468 du17 juin 1998 relative à la prévention et à la répression des infractions sexuelles qui va introduire l'alinéa 3 de l'article 227-23 du code pénal afin de créer une circonstance aggravante lorsque les faits d'exploitation pornographique de l'image d'un mineur se font sur un réseau de télécommunication.

En outre, les infractions relatives à la pédopornographie et à l'apologie du terrorisme ont un point commun en ce qu'elles punissent la « *consultation habituelle* » de contenu. La pédopornographie est visée par l'article 227-23 du Code pénal qui dispose notamment 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*[657] *par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende* ». C'est la Commission des affaires culturelles de l'Assemblée nationale qui est à l'origine de cet alinéa relatif à la consultation habituelle de contenu pédopornographique. Elle a souhaité élargir l'incrimination de détention de contenu pédopornographique en punissant également la consultation de ce genre d'images sur des sites visités par des pédophiles par le biais d'Internet et du Darknet. Cette modification est une conséquence de l'évolution d'Internet et de la facilité de connexion qui permettent désormais

[654] Le Conseil de l'Europe, La pornographie enfantine, un marché lucratif sur le réseau Internet, novembre 2001, page 1. Disponible à cette adresse : www.aidh.org.
[655] Elle est adoptée à New York le 20 novembre 1989 et ratifiée par la France le 26 janvier suivant par la loi n°90-548 du 2 juillet 1990 autorisant la ratification de la Convention relative aux droits de l'enfant.
[656] Article 34 de la Convention des Nations Unies relative aux droits de l'enfant.
[657] D'un mineur lorsque cette image ou cette représentation présente un caractère pornographique.

aux pédophiles de consulter le contenu litigieux sans avoir à le télécharger pour l'enregistrer. Il leur suffit de se connecter sur le site en question pour consulter des images ainsi que des vidéos en streaming.

Avant la modification de l'article 227-23 du code pénal, les juges du fond ont tenté d'utiliser le recel du délit de détention de pédopornographie enfantine pour lutter contre la pédopornographie et contrer la rédaction approximative des dispositions. En effet, prévu à l'article 321-1 du Code pénal le recel est « *le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit* ». Néanmoins, la Cour de cassation a correctement appliqué le principe d'interprétation stricte de la loi pénale en refusant de caractériser la détention pour la consultation d'images pédopornographiques sur un site ou dans une base de données.

Il convient alors d'étudier l'article 227-23 du Code pénal en tant qu'instrument répressif principal dans la lutte contre la pédopornographie (1) et en tant qu'incrimination pour la consultation habituelle de contenu pédopornographique (2).

1. L'instrument juridique principal

Très logiquement la Convention internationale des Nations Unies relative aux droits de l'enfant[658] est très préoccupée par la pédopornographie. En effet, son article 34 dispose que « *les Etats parties[659] s'engagent à protéger l'enfant contre toutes les formes d'exploitation sexuelle et de violence sexuelle. A cette fin, les Etats prennent en particulier toutes les mesures appropriées sur les plans national, bilatéral et multilatéral pour empêcher : a) Que des enfants ne soient incités ou contraints à se livrer à une activité sexuelle illégale ; b) que des enfants ne soient exploités à des fins de prostitution ou autres pratiques sexuelles illégales ; c) que des*

[658] Adoptée à New York le 20 novembre 1989 la Convention internationale des droits de l'enfant (CIDE) est un traité international qui a vocation à protéger les droits spécifiques des enfants et qui a été ratifié par la France le 26 janvier 1990 via la loi n°90-548 du 2 juillet 1990.
[659] Parmi les 193 États reconnus par l'ONU, seuls les USA ne sont pas concernés par ce traité qui n'a pas été ratifié par le Sénat américain en raison du fait qu'il interdit la peine de mort pour les crimes commis par les mineurs qui est toujours légale dans la Constitution de certains États américains malgré son abolition par la Cour suprême dans l'arrêt de mars 2005 « Roper v. Simmons »).

enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique ». Cette Convention a eu un impact important sur le droit français puisqu'elle a permis la création de l'article 227-23 du Code pénal relatif à l'exploitation d'image pédopornographique mais pas nécessairement sur Internet.

L'article 227-23 sera ensuite modifié par la loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs[660] afin d'aggraver l'incrimination[661] « *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* ». Cet article dispose alors que « *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 est puni 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* ».

Ainsi, l'élément matériel de l'infraction peut être constitué par plusieurs actions telles que le fait de « *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*[662] », « *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*[663] ». Sont donc punis le trafic, l'enregistrement et la diffusion[664] de contenu pédopornographique. Par ailleurs, l'alinéa 7 de l'article 227-23 du Code pénal dispose que cet article s'applique même si « *le mineur a l'aspect physique d'un majeur, sauf s'il est établi que*

[660] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000556901.
[661] Code pénal art. 227-23 alinéa 3 : « *les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende* ».
[662] Alinéa 1er.
[663] Alinéa 2.
[664] En ce sens la chambre criminelle de la cour de cassation dans un arrêt du 12 septembre 2007, n°06-86.763 a précisé que « *l'envoi d'un message ne contenant que l'adresse d'un site Internet et le lien permettant d'y accéder ne suffit pas à caractériser le délit* ». Dès lors, c'est la diffusion de l'image qui importe et non la diffusion du moyen permettant d'accéder à l'image.

cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image ». Il s'agit donc d'une présomption simple qui peut être renversée si le prévenu prouve que l'intéressé était majeur le jour de l'enregistrement.

Depuis 2013, l'alinéa 3 de l'article 227-23 incrimine également la consultation de contenu pédopornographique : « *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* » (2).

2. La consultation habituelle de contenu pédopornographique

Le manque de précision du texte l'a rendu inapplicable et a contraint le législateur à intervenir. En effet, avant la modification de l'article 227-23 du Code pénal, seule la détention d'images était visée si bien que les pédophiles contournaient la loi en ne faisant que visionner les images sur Internet sans les télécharger.

Les juges du fond ont alors tenté d'utiliser le recel du délit de détention de pédopornographie enfantine pour lutter contre la pédopornographie et contrer la rédaction approximative des dispositions qui ne permettaient pas la poursuite de l'individu qui n'avait pas enregistré les images sur son ordinateur[665]. Mais la chambre criminelle a estimé[666] que la consultation de sites pédopornographiques n'était pas assimilable à de la détention visée par l'article 227-23 du Code pénal et refusé un quelconque détournement de la loi[667].

Dès lors, le législateur est intervenu avec la loi n°2007-297 du 5 mars 2007[668] en incriminant

[665] Le 16 février 1998 le tribunal correctionnel de la ville du Mans a condamné un pédophile pour recel d'images pédopornographiques en se fondant sur l'article 321-1 du Code pénal et en précisant que l'individu avaient visionné des images « *particulièrement repoussantes, que leur nombre impressionnant dénote plus qu'une simple curiosité malsaine, et que par ses paiements, le prévenu a entretenu des réseaux pédophiles* », disponible à cette adresse https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-du-mans-jugement-correctionnel-du-16-fevrier-1998/.
[666] Cour de cassation, chambre criminelle, 5 janvier 2005, n°04-82.524.
[667] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 130.
[668]Réformant la protection de l'enfance, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000823100&categorieLien=id.

la consultation « *habituelle* » de sites pédopornographiques nonobstant le motif. En effet, il semble difficile d'envisager qu'une personne consulte habituellement des sites pédopornographiques pour un autre motif que la satisfaction de ses besoins sexuels si bien qu'une justification basée sur un aspect intellectuel ou un travail de recherche fasse nécessairement défaut. Il s'agit en outre d'assécher un marché pédophile en pleine expansion.

Enfin, 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[669], rajoute à l'alinéa 4 de l'article 227-23 du Code pénal la consultation « *en contrepartie d'un paiement d'un service de communication au public en ligne » d'images pornographiques de mineurs. « Un service de communication au public en ligne* » est défini par la loi LCEN du 21 juin 2004 suscitée comme un service permettant « *toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur* ». Les réseaux darknets répondent parfaitement à cette définition puisqu'ils permettent la transmission de données numériques aux utilisateurs. Dès lors, l'article 227-23 du Code pénal peut s'appliquer à la consultation contre paiement de sites pédopornographiques sur le Darknet. L'absence de précision suppose que la consultation unique est suffisante. Concernant l'élément moral de l'infraction, il s'agit d'un délit intentionnel qui implique que le prévenu ait eu conscience et la volonté de visionner du contenu pédopornographique.

Aux États-Unis la production de pornographie infantile est interdite en raison de la protection des mineurs utilisés pour la réalisation sans égard pour les effets sur les récepteurs[670]. Même chose pour la diffusion et la possession de ce genre de contenu qui favorisent la circulation de l'enregistrement et continuent de porter atteinte à l'enfant. En France, la loi vise ce genre de contenu en prenant en compte le préjudice susceptible d'être infligé au participant mineur mais également le trouble que la pédopornographie cause à l'ordre public. Dès lors, l'article 227-23 peut s'appliquer pour la représentation d'actes pédophiles fictifs et permettre aux enquêteurs d'appréhender un grand nombre de pédophiles, qu'il s'agisse d'une image ou de la

[669]https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027805521&categorieLien=id.
[670] New York v. Ferber, 458 U.S. 747 (1982). Cf. F. Schauer, *Codifying the First Amendment: New York v. Ferber*, Supreme Court Review, volumes 1982, 1983, page 291.

« *représentation d'un mineur* » (B).

B) Les services d'enquête

Dans cette lutte contre cette forme de criminalité spécifique, l'office Européen de Police Europol tend à impliquer les utilisateurs en mettant en place une plateforme permettant de dénoncer les pédophiles. Sur le site « *Stop Child Abuse*[671] » sont postés des objets utilisés par les pédophiles dans leurs vidéos. Il peut s'agir d'une décoration ou d'une tenue vestimentaire permettant d'identifier et signaler les pédophiles.

En France, il existe plusieurs services d'enquêteurs compétents en matière de pédopornographie. L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication dit OCLCTIC est un service spécial de la sous-direction de la Lutte contre la Cybercriminalité qui traite des délits relatifs à la pédopornographie. Le Centre national d'analyse des images pédopornographiques dit CNAIP est un organisme de la gendarmerie nationale[672] qui a pour mission la collecte et l'analyse de l'ensemble du contenu pédopornographique récolté par les enquêteurs. Par ailleurs, le contenu pédopornographique peut être signalé sur la plateforme « *Pharos* » gérée par le ministère de l'Intérieur. Il s'agit d'un site Internet permettant de recueillir le signalement de contenu « *suspect ou illicite* » tel que le contenu pédopornographique. En 2017, sur les 153 586 signalements enregistrés sur la plateforme, 15% concernaient des faits de pornographie infantile[673]. Ces nouvelles méthodes doivent être utilisées afin d'optimiser l'efficacité de la lutte contre les formes de délinquance et criminalité touchant les mineurs.

En tout état de cause, eu égard au caractère international de toutes les infractions précitées, la lutte contre la cybercriminalité dissimulée suppose une coopération entre États (Chapitre 2).

[671] https://www.europol.europa.eu/stopchildabuse.
[672] Les textes pris en application de la loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance ont permis « *la création d'un centre national d'analyse des images de pédopornographie (CNAIP) qui a pour vocation 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* ».
[673] ADAM L., *Cybercriminalité en France : les autorités adaptent leur dispositif, mais la route est longue,* 22 juin 2018. Disponible à cette adresse : https://www.zdnet.fr/actualites/cybercriminalite-en-france-les-autorites-adaptent-leur-dispositif-mais-la-route-est-longue-39870090.htm, [consulté le 7 juillet 2018].

CHAPITRE 2
LA COOPÉRATION ENTRE ÉTATS FACE À LA CYBERCRIMINALITÉ

« *La menace cybercriminelle qui plane au niveau international requiert une coordination sur l'ensemble du territoire national de chaque État, de la détection de la cybercriminalité et la lutte contre ce phénomène*[674] ».

Traditionnellement, la matière répressive est gérée par chaque État qui est souverain sur son territoire. Pourtant, aujourd'hui les traités internationaux sont une véritable source du droit pénal et la portée des règles de droit pénal n'est plus limitée à un seul pays. Ainsi, un traité ratifié de manière régulière a une valeur supérieure à la loi dans la hiérarchie des normes. C'est le cas notamment du Pacte international sur les droits civils ratifié par la France le 4 novembre 1980 après que les Nations Unies l'ont adopté en 1966. Ce texte vise, à titre d'exemple, les traitements inhumains et empêche le législateur d'autoriser la torture. Pour un autre exemple, il est possible de citer le traité de Rome du 17 juillet 1998 qui est le texte à l'origine de la Cour pénale Internationale.

Cette habilitation pour un État à prendre des mesures est fondée sur des obligations conventionnelles qu'ils doivent respecter, notamment en matière d'incrimination. En 1925 déjà la Cour permanente de justice internationale estime qu'un « *État qui a valablement contracté des obligations internationales est tenu d'apporter à sa législation les modifications nécessaires pour assurer l'exécution des engagements pris*[675] ». Ainsi, une obligation morale pèse sur les États engagés.

Par exemple, la CESDH ratifiée par la France le 3 mai 1974 est une source importante en droit pénal. Son respect par les États signataires est garanti par la Cour EDH, et selon la Cour de cassation le juge français peut relever d'office la violation d'une disposition de la convention[676]. De plus, ce texte peut contraindre les États à renforcer leur législation en créant de nouvelles infractions. C'est ainsi que la France a été condamnée en matière d'esclavage domestique[677].

[674] CHAWKI M., *Combattre la cybercriminalité*, Editions de Saint-Amans, 2008, pages 401 et suivantes.
[675] Cour permanente de justice internationale, Assemblée du 21 février 1925 sur l'Echange de populations turques et grecques, série B, n° 10, page 20.
[676] Cour de cassation, chambre criminelle, 5 décembre 1978, n°78-91.826.
[677] CEDH 26 juillet 2005, *Siliadin contre France* ; voir Code pénal art. 225-13 et 225-14.

Pour autant, cette obligation ne porte pas atteinte à la compétence pénale des États exercée au nom de la souveraineté. Chaque État établit sa propre juridiction et ses propres lois. Dès lors, pour les situations essentiellement internes, la compétence territoriale va de soi et le droit international la reconnaît. Cette dernière est en réalité une obligation pour les États qui doivent protéger leur territoire et leurs citoyens.

Ainsi, les droits conventionnels et internationaux prévoient généralement de simples obligations de prendre des mesures internes ou des engagements à destination des États qui doivent établir des mesures dans les domaines couverts par les Conventions. Toutefois, la faculté d'incriminer revient à l'État. Concrètement, il s'agit de guider les États et non de les contraindre. En ce sens, dans les Conventions, il y a beaucoup de références aux législations nationales mais peu concernant la sanction pénale.

De manière générale, le droit national, le droit européen et le droit international reconnaissent comme étant illégales la plupart des atteintes aux personnes, aux organisations et aux États.

Depuis les années 2000, ils reconnaissent également la cybercriminalité comme étant illégale. Selon Mireille Ballestrazzi, directrice centrale de la police judicaire et ancienne présidente du comité exécutif d'Interpol[678] : « *La cybercriminalité est clairement la nouvelle menace du 21ème siècle. Elle force les polices à repenser leurs moyens d'action, à se mettre au niveau techniquement et à développer des outils transnationaux, car l'échelle devient mondiale. Le cybercrime est d'autant plus difficile à appréhender qu'il prend des formes diverses et n'a, par définition, pas de frontières. Il peut s'agir d'apologie du terrorisme, de réseaux de pédopornographie ou de proxénétisme, ou encore d'attaques contre des systèmes de données, comme celle qu'a connue récemment TV5 Monde. Internet donne aussi aux malfaiteurs un nouveau terrain de jeu pour mettre en place des escroqueries comme la fraude à l'e-paiement, le blanchiment d'argent ou le trafic de stupéfiants. Le cyberespace permet l'expression de menaces inédites par l'utilisation des nouvelles technologies, mais il étend aussi le périmètre des crimes classiques. Avec la démocratisation de l'accès à Internet et l'innovation constante*

[678] ROLLAND S., *La cybercriminalité est la nouvelle menace du XXIème siècle*, 26 juillet 2015. Disponible à cette adresse : https://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html.

autour des nouvelles technologies, la cybercriminalité devient un enjeu de société, à la fois pour les gouvernements, les entreprises et les citoyens. Et ce n'est que le début : toutes les études tablent sur une augmentation significative du nombre de crimes liés à Internet dans les années et décennies à venir. Il s'agit d'un vrai défi pour les États et les polices du monde entier ». Ainsi, seul un travail coordonné permettra d'appréhender les cybercriminels.

Mireille Ballestrazzi ajoute qu'une lutte efficace « *contre le crime en général et contre la cybercriminalité en particulier demande la mise en place d'outils globaux. Interpol, dont le siège est à Lyon, remplit déjà cette mission. Il dispose de bases de données massives, sur la pédopornographie par exemple, alimentées par l'ensemble des polices du monde. En revanche, les crimes sur Internet nécessitent une attention particulière. C'est pourquoi les 190 membres d'Interpol ont accepté à une quasi-unanimité l'ouverture de cette nouvelle structure à Singapour. Le Complexe mondial transcende le modèle traditionnel répressif en matière d'application de la loi, en utilisant toutes les possibilités de l'ère numérique… Prenons l'exemple de la pédopornographie, qui prospère sur Internet. Il existe des sites d'une horreur absolue. Grâce à sa base de données, Interpol peut découvrir un réseau. Mais souvent, l'initiative part d'un pays membre, qui identifie un certain nombre d'adresses IP problématiques et ouvre une enquête judiciaire. Internet étant mondial, les adresses IP concernent souvent plusieurs États. Interpol contacte alors le bureau central d'Interpol dans chaque pays concerné pour mettre en place une coopération internationale. Celle-ci permet de partager les informations et de mener des actions simultanées comme l'arrestation, au même moment et dans plusieurs pays, de plusieurs organisateurs d'un réseau pédopornographique. Il arrive très régulièrement que la police française ou la gendarmerie participe à ce genre d'opérations. De même, la police judiciaire est en lien direct avec Singapour via un commissaire de police qui y est détaché. Nous collaborons aussi avec EC3, la plateforme d'Europol vouée à la cybercriminalité. L'objectif de toutes ces structures est d'être plus efficace sur le terrain mais aussi d'éviter les doublons, car lutter contre la cybercriminalité coûte très cher. Pourquoi faire enquêter plusieurs équipes, séparément, dans différents pays, quand on peut avoir une vision d'ensemble ?*[679] ».

[679] ROLLAND S., *La cybercriminalité est la nouvelle menace du XXIème siècle*, 26 juillet 2015. Disponible à cette adresse : https://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html.

À ce titre, depuis 2004, l'Agence européenne chargée de la sécurité des réseaux et de l'information [680] tente d'avoir un rôle dans cette guerre numérique, mais les faiblesses budgétaires lui empêchent d'être efficace face aux menaces. Cela conforte l'idée qu'aucune organisation internationale n'a de réelle autorité en matière de cybercriminalité où la coopération internationale est incarnée par la Convention de Budapest sur la cybercriminalité. Cette dernière vise à travers 48 articles « *à harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité, à fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique, et à mettre en place un régime rapide et efficace de coopération internationale*[681] ». Dans un souci d'harmonisation et de modernisation des règes relatives à la cybercriminalité, cette convention rallie vingt-six membres du Conseil de l'Europe sur quarante-trois ainsi que l'Afrique du Sud, le Canada, le Japon et les États-Unis soit trente pays. D'autres attributions ont été données à INTERPOL, l'Organisation internationale de police criminelle, qui réunit en 2018 cent quatre-vingt-douze pays.

En matière de numérique, le caractère multinational des infractions a contraint les États à coopérer entre eux : « *la transnationalité des infractions cyber et l'absence de frontière de cet espace virtuel oblige les États à s'entendre et à coopérer en Europe (...) la convention de Budapest*[682] *(2001) sur la cybercriminalité a posé les bonnes intentions des membres qui s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale (...) Pour les pays hors Convention de Budapest, d'où peuvent provenir les attaques cyber, les résultats des investigations vont souvent dépendre de l'entente bilatérale entre les États*[683] ».

[680] L'ENISA pour « *European Network and Information Security Agency* » est située à Heraklion en Crète.
[681] Conseil de l'Europe, *Rapport explicatif de la Convention sur la cybercriminalité*, Budapest, 2001, STE N°185, page 4.
[682] Des États hors Europe ont signé cette Convention.
[683] Institut national des hautes études de la sécurité et de la justice, *Enjeux et difficultés de la lutte contre la cybercriminalité*, juillet 2015, page 29.

Il convient de traiter la coopération européenne (section 1) d'une part, et la coopération internationale d'autre part (section 2).

SECTION 1
La coopération européenne

Le droit communautaire[684] est aussi une source importante du droit pénal. Il comprend les règlements et directives directement applicables en France. Dès lors, cette dernière est tenue d'adopter de nouvelles mesures tout en étant libre en ce qui concerne les modalités. Par exemple, le règlement général sur la protection des données, dit « *RGPD* », est un acte juridique de l'Union Européenne obligatoire en France depuis le 25 mai 2018.

L'OCDE[685], une organisation composée de 31 membres aspirant à améliorer le bien-être économique et social des individus, est l'une des premières organisations à s'être souciée de la cybercriminalité. Elle crée en 1982 un groupe de travail dont les recommandations destinées aux législateurs nationaux leur conseillent de mettre en place une politique pénale incluant un certain nombre d'infractions relevant de la matière. Dans ce sens, l'OCDE dresse la liste de cinq comportements illicites[686] : 1) « *l'introduction, l'altération, l'effacement et/ou la surpression de données et/ou de programmes informatiques effectuées volontairement avec l'intention de commettre un transfert illégal de fonds ou d'autres valeurs* » ; 2) « *l'introduction, altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques effectués volontairement avec l'intention de commettre un faux en écriture* » ; 3) « *l'introduction, l'altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques ou autres ingérences dans des systèmes informatiques accomplis volontairement avec l'intention d'entraver le fonctionnement du système informatique et/ou de la télécommunication* » ; 4) « *la violation du droit exclusif du propriétaire d'un programme informatique protégé avec l'intention d'exploiter commercialement ce programme et de le commercialiser sur le marché* » ; 5) « *l'accès à, ou l'interception de fonctions d'un système informatique et/ou de télécommunications, accomplis volontairement et sans l'autorisation de la personne responsable du système, en violation des mesures de sécurité et avec l'intention de nuire, ou d'autres intentions frauduleuses* ».

Elle est rapidement suivie par le Conseil de l'Europe qui émet le 3 septembre 1989 une

[684] Il s'agit du droit de l'Union européenne qu'il ne faut pas confondre avec le Conseil de l'Europe.
[685] L'organisation de coopération et de développement économiques.
[686] OCDE, *La fraude liée à l'informatique : analyse des politiques juridiques*, Paris, 1986, page 72.

recommandation sur « *la criminalité en relation avec l'ordinateur* » ayant le même objectif consistant à inciter les États à prendre en compte la cybercriminalité dans leur arsenal pénal. Sur sa lancée, le Conseil de l'Europe publie également un projet de convention intitulé « *Projet de convention du Conseil de l'Europe sur la criminalité* informatique » et qui est à l'origine de le Convention sur la cybercriminalité de novembre 2001.

Par la suite, dans la lignée de l'OCDE et du Conseil de l'Europe, c'est l'Union européenne qui va intervenir en la matière en communiquant sur les « *questions essentielles du débat, tant procédurales que relatives au droit pénal de fond*[687] » et en insistant sur la nécessité d'une définition des infractions sur Internet en prenant le soin de différencier les infractions liées particulièrement à la criminalité informatique des infractions classiques facilitées grâce aux réseaux. Elle propose également de s'accorder sur les éléments procéduraux du droit de l'Internet et notamment sur « *ce qui touche les interceptions des télécommunications, à la conservation des données relatives au trafic, à l'anonymat de l'accès et de l'utilisation des réseaux, à la coopération et la compétence internationale ainsi qu'à la formation et à l'expertise des autorités policières et judiciaires en charge de cette catégorie particulière de la criminalité*[688] ».

La mise en place de l'espace « *européen de liberté, de sécurité et de justice*[689] » par l'Union Européenne a impliqué une coopération des États membres dans la lutte contre la cybercriminalité. Dès lors, au sein de l'Union Européenne, en matière de coopération policière, Europol, l'agence « *européenne de police criminelle qui facilite l'échange de renseignements entre polices nationales en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédophilie au sein de l'Union européenne*[690] », et en matière de coopération judiciaire, EUROJUST, l'Unité de coopération judiciaire de l'Union européenne[691], se sont vues attribuer

[687] Communication de la Commission.
[688] Disponible à cette adresse : http://ec.europa.eu/transparency/regdoc/rep/1/2001/FR/1-2001-429-FR-F1-1.pdf.
[689] « *L'espace de liberté, de sécurité et de justice (ELSJ) est un objectif inclus dans les traités sur l'Union européenne par le traité d'Amsterdam en 1997 et qui vise à assurer la libre circulation des personnes et à protéger les citoyens, qui remplace partiellement la coopération policière et judiciaire en matière pénale* ». Disponible à cette adresse : https://fr.wikipedia.org/wiki/Espace_de_liberté,_de_sécurité_et_de_justice.
[690] https://fr.wikipedia.org/wiki/Europol.
[691] « *Chargée de renforcer la coopération judiciaire entre les États membres par l'adoption, au niveau européen, de mesures structurelles destinées à promouvoir une coordination optimale des actions d'enquête et de poursuites débordant le cadre d'un seul territoire national, dans le plein respect des libertés et des droits fondamentaux* ». Disponible à cette adresse : https://fr.wikipedia.org/wiki/Eurojust.

de nouvelles attributions en matière de lutte contre la cybercriminalité.

Ainsi, en matière de lutte contre la cybercriminalité, nombreux sont les efforts qui ont été entrepris par les États au niveau de l'Union européenne et du Conseil de l'Europe. Ces efforts ont été entrepris en ce qui concerne la coopération judiciaire (§1) mais également en ce qui concerne la coopération policière (§2).

§1) La coopération judiciaire

Pour les infractions informatiques, l'extradition entre États est possible même si aucun accord n'est prévu. Il faut que l'infraction prévue dans les deux États membres du Conseil de l'Europe soit punie d'au moins un an d'emprisonnement. Cette procédure a été mise en place pour lutter contre la criminalité informatique qui ne se soucie pas des frontières. En outre, pour l'extradition, la voie diplomatique peut être remplacée par une autre autorité compétente, plus rapide et spécialisée en la matière.

Au delà de cette possibilité d'extradition, en matière de coopération au sein de l'Union européenne, plusieurs Conventions de coopération judiciaire pénales ont été entreprises et ont apporté quelques améliorations notables en terme d'entraide et de coopérations judiciaires. Eurojust (A) et la Convention relative à l'entraide judiciaire (B) en sont les parfaits exemple.

A) Eurojust

« *Eurojust a été instituée par la décision du Conseil 2002/187/JHA, amendée par la décision du Conseil 2009/426/JHA du 16 décembre 2008. La mission d'Eurojust consiste à renforcer l'efficacité des autorités nationales chargées des enquêtes et des poursuites dans les dossiers de criminalité transfrontalière grave et de criminalité organisée et de traduire les criminels en justice de façon rapide et efficace. Eurojust a pour ambition de devenir un acteur clé et un centre d'expertise au niveau judiciaire pour lutter efficacement contre la criminalité organisée transfrontalière dans l'Union européenne*[692] ».

Eurojust peut rassembler les enquêteurs de plusieurs États pour une durée déterminée et un but

[692] http://www.eurojust.europa.eu/Pages/languages/fr.aspx.

prédéfini. Cette équipe, mise en place via une JIT[693], effectue des enquêtes pénales sur le territoire des États dont proviennent les enquêteurs. En effet, « *les membres nationaux ont le droit de participer aux équipes communes d'enquête (...) en ce qui concerne leur propre État membre, y compris à la création de ces équipes*[694] ».

Eurojust n'est pas un organe européen supranational mais une agence européenne dont le but est de renforcer la coopération et la coordination entre les autorités judiciaires de ses membres[695]. En effet, il n'a pas de pouvoir juridictionnel si bien qu'il ne peut procéder seul aux enquêtes et aux poursuites et conforte la souveraineté des États. Toutefois, il a vocation à le devenir puisque le 8 juin 2017, vingt États membres de l'Union européenne ont trouvé un accord politique sur la création d'un Parquet européen à partir d'Eurojust. En ce sens, depuis l'entrée en vigueur du Traité de Lisbonne le 1er décembre 2009, l'article 86 du TFUE[696] prévoit que « *pour combattre les infractions portant atteinte aux intérêts financiers de l'Union, le Conseil, statuant par voie de règlements conformément à une procédure législative spéciale, peut instituer un Parquet européen à partir d'Eurojust* ». Ainsi, initialement sa compétence n'était limitée qu'à la fraude et aux intérêts financiers de l'Union européenne. Sa compétence matérielle sera élargie à la poursuite de la criminalité grave à dimension transfrontalière.

Dans une optique de coopération renforcée, la naissance du parquet européen a été inscrite dans les traités de Nice et de Lisbonne en 2001 et 2007. Néanmoins, des pays comme la Suède, la Pologne, les Pays-Bas ou la Hongrie, ont bloqué les discussions relatives à sa création[697]. Il faut attendre le Conseil de l'Union européenne du 3 avril 2017 pour que seize États membres notifient officiellement leur volonté de mettre en place une coopération renforcée en adressant une lettre au Conseil. Dès lors, le 8 juin 2017, c'est lors du Conseil « *Justice* » que vingt États membres parviennent à un consensus concernant la création du Parquet européen. Le Parlement européen donne également son approbation le 5 octobre 2017. En novembre 2017, l'UE adopte le règlement 2017/1939 créant le Parquet européen. La date de commencement des travaux du

693 « *Joint Investigation Team* ».
694 Décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust.
695695 BOOS R. La lutte contre la cybercriminalité au regard de l'action des États, Université de Lorraine, 2016, page 235.
696 « *Traité sur le fonctionnement de l'Union européenne* ». Avec le Traité sur l'Union européenne, il s'agit de l'un des deux traités fondement des institutions politiques de l'UE.
697 Ils ne veulent pas céder une partie de leurs prérogatives à l'Union européenne en la laissant agir directement dans le champ juridique interne.

Parquet européen est prévue pour 2020. Vingt pays[698] se sont affilés à la création du Parquet européen mais d'autres pourront y adhérer par la suite.

En tant que « *première instance européenne indépendante avec des compétences judiciaires propres* »[699], le Parquet européen sera chargé de diriger les enquêtes et les poursuites pénales et exercer l'action publique devant les juridictions des États membres. En l'absence de tribunal européen, il engagera les poursuites au niveau national à un niveau décentralisé, avec des procureurs européens délégués qui agiront dans leurs pays respectifs, et à un niveau centralisé avec l'organisation de chambres permanentes comprenant les procureurs européens[700]. Ces derniers seront choisis par le Conseil européen après que les États membres auront présenté une liste de trois candidats. Ils surveillent les enquêtes et les poursuites gérées par les procureurs européens délégués. Un tel parquet sera un outil utile permettant d'améliorer la coopération judiciaire entre États.

Les cybercriminels profitent encore des différences législatives et judiciaires qu'il y a entre les États. Le Parquet européen sera en mesure de poursuivre les délinquants à un niveau européen sans égard pour les frontières. Les infractions transfrontalières comme le terrorisme, la criminalité informatique ou la pédopornographie pourront être mieux gérées. Une Convention relative à la coopération judiciaire mérite également d'être étudiée (B).

B) La Convention relative à l'entraide judiciaire

Concernant la coopération, la Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne[701] elle aspire à faciliter l'entraide entre les autorités des différents pays membres[702]. Cette entraide concerne la matière pénale,

[698] La Slovénie, l'Espagne, la Slovaquie, la Roumanie, le Portugal, le Luxembourg, la Lituanie, la Lettonie, l'Italie, la Grèce, l'Allemagne, la France, la Finlande, l'Estonie, la République tchèque, Chypre, la Croatie, la Bulgarie, la Belgique et l'Autriche.
[699] Disponible à cette adresse : http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2013/0534/COM_COM(2013)0534_FR.pdf.
[700] Chaque État disposera d'un procureur général.
[701] Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'UE, la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne. Disponible à cette adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:C:2000:197:TOC.
[702] Il faut attendre le 1er mai 2009 pour qu'elle soit ratifiée dans quasiment tous les États membres. En France, il faut attendre la loi n°2005-287 du 30 mars 2005 autorisant l'approbation de la Convention.

c'est-à-dire la justice, la police et les douanes. Elle comble la Convention sur l'entraide judiciaire en matière pénale établie par le Conseil de l'Europe en 1959[703]. La portée territoriale de la Convention est élargie le 8 novembre 2001 avec le deuxième protocole de la Convention d'entraide du Conseil de l'Europe qui reprend presque toutes ses dispositions. La coopération s'étend alors puisque le Conseil de l'Europe rassemble quarante sept États membres tandis que l'Union Européenne vingt-huit.

Dans la continuité des autres Conventions d'entraide qu'elle complète, la Convention du 29 mai 2000 apporte quelques améliorations importantes. Elle favorise l'entraide avec des avancées relatives au contact direct entre États, en réduisant les conflits territoriaux de loi et en adaptant la procédure d'entraide aux nouvelles technologies.

La Convention a diversifié le nombre de procédures d'entraide. Les demandes d'entraide sont généralement effectuées par écrit, transmises et mises en exécution par les autorités territorialement compétentes. Toutefois, certaines procédures[704] telles que les demandes de transit de détenus ou les transmissions d'avis de condamnation, passent par les autorités centrales des États membres. S'il y a urgence, la demande est alors transmise par le biais d'Interpol ou d'une organisation compétente selon le traité sur l'UE.

La Convention permet également la mise à disposition d'objets volés[705], l'audition de témoins ou d'experts par vidéoconférence[706], les livraisons surveillées[707], les équipes communes

[703] Et son protocole de 1978.
[704] Les pièces de procédure quelconques sont envoyées directement par courrier aux enquêteurs se trouvant sur le territoire d'un autre pays membre.
[705] « *Les objets volés retrouvés dans un autre État membre sont mis à la disposition de l'État requérant en vue de leur restitution à leur propriétaire* ». Disponible à cette adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33108.
[706] « *Un témoin ou un expert peut être entendu par les autorités judiciaires d'un autre État membre par vidéoconférence si cela n'est pas contraire aux principes fondamentaux de l'État requis et si toutes les parties impliquées sont d'accord ».* Disponible à cette adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33108.
[707] « *Les livraisons surveillées sont autorisées sur le territoire d'un autre État membre dans le cadre d'enquêtes pénales relatives à des infractions susceptibles de donner lieu à extradition. Elles se déroulent sous la direction et le contrôle de l'État membre requis* ». Disponible à cette adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33108.

d'enquête[708], les enquêtes discrètes[709] et l'interception des télécommunications[710].

Même si les pratiques offertes par la Convention sont nombreuses, deux reproches peuvent lui être adressés. Premièrement, toutes les possibilités offertes ne peuvent pas encore être exploitées par tous ses membres car certains ne disposent pas des moyens techniques requis. Secondement, à l'instar des autres conventions, les particularités relatives aux réseaux anonymes tels que le Darknet sont mises de côtés, ce qui contribue au côté sombre de l'Internet dissimulé.

Il existe d'autres organismes européens qui ont été mis en place en vue de renforcer la sécurité de l'Europe. Il est possible de citer Europol et l'ENISA, qui constituent les fondements de la coopération policière européenne (§2).

§2) La coopération policière

Dans la lutte contre la cybercriminalité il existe également des organismes rattachés aux institutions de l'Union européenne. Existe notamment depuis janvier 2004[711] le Contrôleur européen de la protection des données[712] qui est une autorité de contrôle indépendante ayant vocation à garantir le respect du droit à la vie privée et la protection des données par les institutions et organes européens. Précisément, les principaux organismes européens sont

[708] « *Deux ou plusieurs États membres peuvent mettre sur pied une équipe commune d'enquête, dont la composition est définie par un accord commun des États membres concernés. L'équipe commune est créée dans un but déterminé et pour une durée limitée. Un fonctionnaire de l'État membre sur le territoire duquel l'équipe intervient assure la direction de l'équipe et dirige les activités sur le territoire de cet État membre* ». Disponible à cette adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33108.
[709] « *Des enquêtes discrètes peuvent également être menées, par des agents intervenant sous une identité secrète ou fictive, à condition que la législation et les procédures de l'État membre sur le territoire duquel elles se déroulent soient respectées* ». Disponible à cette adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33108.
[710] « *L'interception des télécommunications peut être effectuée, sur demande de l'autorité compétente d'un autre État membre, par une autorité judiciaire ou une autorité administrative désignée par l'État membre concerné. Une télécommunication peut être soit interceptée et transmise directement à l'État membre requérant, soit enregistrée et transmise ultérieurement* ». Disponible à cette adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33108.
[711] La base légale de cette autorité est l'article 286 du traité instituant la communauté européenne et le règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. Elle a été créée par la directive 2001/45.
[712] Page d'accueil du Protecteur européen de la protection des données : https://edps.europa.eu/edps-homepage_fr.

l'Europol (A) et l'ENISA (B).

A) Europol

Créé en 1992, Europol est une agence européenne[713] de police criminelle dont l'objectif est de faciliter les échanges de renseignements entre les services de police des États membres en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédophilie. L'agence a donc vocation à travailler sur le Darknet.

En ce sens, récemment, l'Agence européenne des drogues et Europol ont publié un rapport sur les drogues et le Darknet[714]. Ils mettent en avant la dangerosité des marchés darknets ou « *cryptomarkets* » qui fournissent des plateformes de commerce illicite anonymes. Ils estiment que la vente de drogue représente deux tiers de l'activité du marché du Darknet[715]. Ainsi, avec un peu de retard, ils présentent des contre-mesures potentielles pour les acteurs politiques et les professionnels de l'application de la loi qui seraient susceptibles de lutter contre la cybercriminalité dissimulée. Leur point de départ a été une analyse de la menace à laquelle est confrontée la communauté internationale. Cela leur a permis d'identifier des domaines prioritaires d'actions ciblées afin de fixer une stratégie permettant de réduire les opportunités malveillantes dans l'écosystème Darknet.

À cet égard, Dimitris Avramopoulos, commissaire européen chargé de la migration, des affaires intérieures et de la citoyenneté, a déclaré : « *au cours de la dernière décennie, les marchés en ligne illégaux ont changé la façon dont les médicaments sont achetés et vendus. L'activité criminelle sur le Darknet est devenue plus innovante et plus difficile à prévoir. Nous ne devrions pas faire de rattrapage avec les criminels : nous devrions être en avance sur eux. C'est pourquoi nous redoublons d'efforts pour lutter contre les drogues illicites et renforcer la cybersécurité. Le cyberespace n'a pas de frontières et nous devrions tous travailler ensemble,*

[713] Il s'agit d'une agence de l'Union européenne depuis une décision du Conseil européen Justice et Affaires intérieures du 6 avril 2009 (Décision du Conseil 2009/371.J1I du 6 avril 2009 portant création de l'Office européen de police). Auparavant, il s'agissait d'un simple bureau.
[714] EUROPOL, *Drugs and the Darknet. Perspectives for enforcement research and policy*. Disponible à cette adresse : file:///Users/Nad/Downloads/drugs_and_the_darknet_-_td0417834enn.pdf.
[715] « *Drugs are estimated to account for around two thirds of darknet market activity* ». Disponible à cette adresse : https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy.

la Commission, les États membres, l'OEDT[716]*, Europol et nos partenaires internationaux. Notre objectif est de mettre un terme aux énormes profits de la drogue dans les poches des groupes criminels organisés en Europe et au-delà, mais surtout de protéger la santé de nos citoyens et en particulier des jeunes*[717] ».

Rob Wainwright, le directeur exécutif d'Europol, ajoute que « *la lutte contre la cybercriminalité et l'utilisation de plates-formes informatiques à des fins criminelles est devenue une priorité importante dans le maintien de l'ordre dans l'UE. La récente décision prise en juillet 2017 contre Alphabay et Hansa*[718]*, deux des plus grands marchés opérant sur le marché noir, illustre bien l'intervention des forces de l'ordre pour perturber cet environnement. Malgré ces résultats positifs, les personnes impliquées dans le trafic de drogue en ligne semblent résister à de telles perturbations et sont en mesure de se réorganiser rapidement. La coopération au niveau européen et le partage des renseignements, ainsi que le ciblage des fournisseurs à fort impact, seront essentiels pour contrer cette menace*[719] ».

D'après le rapport, des équipes d'enquête Darknet seront mises en place et formées par Europol. La collaboration avec les industries clés comme les médias sociaux, les services de paiement ou les technologies de l'information, devient une priorité afin d'identifier les nouvelles menaces du Darknet. Alexis Goosdeel, le directeur de l'OEDT, connaît bien la nature dynamique des marchés en ligne et leur capacité à contrer les menaces ennemies, et à évoluer pour trouver d'autres opportunités : « *En quelques clics seulement, les acheteurs peuvent acheter presque*

[716] L'Observatoire européen des drogues et des toxicomanies.
[717] Texte original : « *Over the last decade, illegal online markets have changed how drugs are bought and sold. Criminal activity on the darknet has become more innovative and more difficult to predict. We shouldn't be playing catch-up with criminals : we should be one step ahead of them. That is why we are boosting our efforts to fight illegal drugs and step up cybersecurity. Cyberspace has no borders and we should all work together, the Commission, Member States the EMCDDA, Europol and our international partners. Our aim is to stop huge profits from drugs ending up in the pockets of organised crime groups in Europe and beyond, but most importantly to protect the health of our citizens and in particular of young people* ». Disponible à cette adresse : https://www.europol.europa.eu/newsroom/news/drugs-and-darknet-growing-threat-to-health-and-security.
[718] Le FBI et Europol ont annoncé la fermeture de ces deux sites du Darknet le jeudi 20 juillet 2017.
[719] Texte original : « *Addressing cybercrime and the use of information technology platforms for criminal purposes has become an important policing priority across the EU. The recent takedown in July 2017 of Alphabay and Hansa, two of the largest darknet markets, is an example of how law enforcement can intervene to disrupt this environment. Despite this positive achievement, those involved in the online drug trade appear to be resilient to such disruption and able to re-organise rapidly. European-level cooperation and intelligence sharing, along with the targeting of high-impact vendors, will be critical in countering this threat* », op. cit.

tous les types de drogues sur le réseau, qu'il s'agisse de drogues synthétiques, de cannabis, de cocaïne, d'héroïne ou d'une série de nouvelles substances psychoactives, y compris des fentanyls[720] *très puissants. Cela constitue une menace croissante pour la santé et la sécurité des citoyens et des communautés à travers l'UE. Les nouvelles informations fournies par cette analyse conjointe apportent une contribution importante à l'information et à la préparation de la réponse de l'Europe à cette menace*[721] ».

Pour faire face au Darknet, les enquêteurs doivent mettre en place une surveillance accrue que le rapport semble enfin envisager. Le commerce en ligne de biens illicites sur le web visible et le web invisible est désormais reconnu par Europol comme un moteur essentiel du crime organisé et une menace importante pour la sécurité des citoyens européens. Il est également traité dans le cycle politique de l'Union européenne pour la lutte contre la criminalité internationale organisée entre 2018 et 2021. Une autre agence de l'Union européenne mérite d'être traitée, il s'agit de l'ENISA (B).

B) L'ENISA

Créée le 10 mars 2004, l'ENISA[722] est une agence de l'Union européenne qui est en charge de la sécurité des réseaux et de l'information. En tant que centre d'expertise en cybersécurité, l'agence est chargée d'aider les États membres de l'Union européenne afin qu'ils mettent en place des politiques et des stratégies efficaces en matière de cybersécurité[723].

En juillet 2018[724], les législateurs européens ont voté en faveur d'un renforcement de ses pouvoirs et d'une augmentation de son budget. Le rapport arpente trois domaines. Le premier domaine concerne la politique destinée à faciliter les discussions européennes pour la lutte contre la cybercriminalité dissimulée. Le deuxième domaine concerne l'analyse de

[720] Le fentanyl est un analgésique opioïde très puissant assimilé aux stupéfiants dans la plupart des États.
[721] Texte original : « *In just a few clicks, buyers can purchase almost any type of drug on the darknet whether synthetic drugs, cannabis, cocaine, heroin, or a range of new psychoactive substances, including highly potent fentanils. This poses a growing threat to the health and security of citizens and communities across the EU. The new insights provided by this joint analysis make an important contribution to informing and preparing Europe's response to this threat* », op. cit.
[722] *European Union Agency for Network and Information Security.*
[723] BOOS R. La lutte contre la cybercriminalité au regard de l'action des États, Université de Lorraine, 2016, page 245.
[724] TANNAM E., *How does ENISA help EU member states with their cybersecurity strategies ?* 9 août 2018. Disponible à cette adresse : https://www.siliconrepublic.com/enterprise/steve-purser-enisa-cybersecurity.

l'approvisionnement en stupéfiant sur le Darknet. Le troisième concerne l'application de la loi pénale sur le Darknet et les recommandations dans les domaines de la surveillance et des politiques.

Selon Steve Purser, le responsable des opérations de l'ENISA, cette nouvelle politique était nécessaire pour établir un modèle de sécurité avec des bases solides. Son expertise passe par l'envoi de recommandations politiques et de liaisons avec les acteurs politiques et industriels de chaque État membre. Il précise que la gestion des risques est importante et qu'il faut comprendre quels sont les futurs risques : « *il est préférable de faire des pas de bébé. Identifier les lacunes et n'oubliez pas de mettre en place un plan pour s'attaquer réellement à ces lacunes*[725] ».

L'ENISA sait que les criminels deviennent de plus en plus sophistiqués. Selon Steve Purser, l'ingénierie sociale est un outil très utilisé par les cybercriminels et c'est la raison pour laquelle ils travaillent énormément sur le Darknet et la cryptographie[726]. Depuis quelques années des pays hors Europe ont manifesté un grand intérêt pour la cybersécurité en mettant en place des dispositifs importants pour lutter contre la cybercriminalité. Tous les États sont concernés par le phénomène qui s'affranchit des frontières. Dès lors, une coopération mondiale a été nécessaire (Section 2).

[725] Texte original : « *It is best to go at baby steps. Identify the shortcomings and don't forget to put in a plan to actually tackle these shortcomings* ».
[726] ENISA REPORT, *the 2017 cyber threat landscape*, 15 janvier 2018. Disponible à cette adresse : https://www.enisa.europa.eu/news/enisa-news/enisa-report-the-2017-cyber-threat-landscape.

SECTION 2 :
La coopération internationale

Le droit pénal révèle un nouvel espace qu'il convient d'organiser et de maîtriser. La cybercriminalité se développe souvent dans un espace transnational ou international[727]. En effet, la nature immatérielle du cyberespace permet aux criminels d'agir à distance, loin du lieu où ils se trouvent, de se délocaliser et de déplacer leurs activités. Ainsi, il y a des particularités de commission qui vont permettre à la cybercriminalité de se jouer des frontières. Cette espèce d'éclatement spatial de la cybercriminalité permet de tenir les autorités à distance des criminels et des lieux où l'infraction produit ses effets. Les criminels choisissent des États qui sont peu regardants sur l'Internet et qui sont peu sévères dans le domaine de la répression pénale. Cet espace sans frontière a été utilisé à dessein d'éloigner les autorités des conséquences de l'infraction.

Par conséquent, les autorités vont être contraintes de recourir aux mécanismes de coopération sauf si l'infraction est purement nationale. Ce panorama transnational est difficile en terme de répression dans la mesure où il s'agit d'une criminalité par nature multinationale. Le plus important n'est pas le lieu de commission de l'infraction mais le lieu où elle produit ses effets. En effet, les critères de localisation des infractions sont appelés à être différents des critères classiques, c'est la destination beaucoup plus que l'action qui compte. La collaboration est obligatoire car les autorités ne peuvent pas agir directement sur un territoire étranger, mais là où le cyberespace ne connaît pas les frontières, l'action des autorités s'y heurte. Les mécanismes de coopération sont donc nécessaires pour faire cesser les effets des cybercriminels et les faire punir.

Ce phénomène de criminalité transnationale n'est pas propre à la cybercriminalité, il existe déjà pour la criminalité terrestre, aérienne ou maritime et c'est la raison pour laquelle les mécanismes juridiques sont anciens. Ces mécanismes sont établis par des textes généraux qui ont vocation à s'appliquer à la cybercriminalité. Par exemple, la Convention des Nations unies contre la criminalité transnationale organisée ou Convention de Palerme adoptée le 15 novembre 2000 a mis en place un cadre international en matière de coopérations policière et

[727] Dans le cadre de ces recherches, ces deux termes seront utilisés comme synonymes. Concrètement l'adjectif transnational signifie à travers un pays, l'adjectif transnationaux à travers plusieurs pays et l'adjectif international entre plusieurs pays.

judiciaire afin de lutter contre la criminalité organisée qui se retrouve sur Internet et sur le Darknet. La Convention de Vienne contre le trafic de stupéfiants entrée en vigueur le 11 novembre 1990, définit des moyens légaux permettant de lutter contre le trafic de stupéfiants international qui se trouve également sur Internet et le Darknet. La Convention de Berne de 1886 est relative à la protection des œuvres et des droits des auteurs sur leurs œuvres. C'est également le cas pour la procédure d'extradition[728] et le mandat européen[729].

Toutefois, ces dispositifs anciens sont marqués par une criminalité fondamentalement terrestre si bien qu'ils sont parfois difficiles à adapter à la cybercriminalité. Par exemple, les mécanismes généraux ne sont pas adaptés à la collecte de preuves et aux perquisitions numériques. De plus, dans le cyberespace il peut y avoir des considérations d'urgence qui nécessitent la récupération rapide des données d'un site, ou son blocage puisque les cybercriminels sont en mesure de fermer rapidement un site pour en ouvrir un autre ailleurs. Lorsque c'est trop tard, il est presque impossible de retrouver leur trace. Pour ces raisons, la coopération internationale se heurte à des difficultés qui subsistent encore aujourd'hui.

Dès lors, les États ont commencé à compléter ces mécanismes généraux par des instruments spéciaux adaptés à la cybercriminalité. On voit apparaître des instruments de coopération spécifiques à la cybercriminalité prenant en compte les difficultés qu'il peut y avoir à saisir cette criminalité avec les mécanismes classiques de coopération. Un certain nombre d'États a mis en place des instruments particuliers comme la Convention du Conseil de l'Europe[730] de Budapest spécifique à la cybercriminalité, qui est le seul instrument international contraignant en la matière, il s'agit de l'instrument de référence. Elle se déclare comme étant complémentaire des instruments existants et ne s'y substitue pas. Elle est divisée en trois ensembles. Le premier définit un certain nombre d'infractions essentiellement numériques que les États doivent adopter. Cette harmonisation permet d'uniformiser ces incriminations pour éviter l'obstacle de la double incrimination. Le deuxième porte sur les règles procédurales internes en matière de cybercriminalité, comme la perquisition numérique qui doit être adoptée dans les États

[728] Il s'agit d'une procédure qui permet à un État de livrer à un autre État qui le réclame, l'auteur d'une infraction afin qu'il y soit jugé ou qu'il y exécute sa peine.
[729] Institué en 2002 au sein de l'Union européenne, il élargit le principe de reconnaissance mutuelle des décisions judiciaires au droit pénal.
[730] Il faut bien préciser Convention du Conseil de l'Europe et non Convention européenne dans la mesure où elle est ouverte à des pays non européens.

membres. Ces règles ne sont pas limitées aux infractions que la Convention définit et s'étendent aux infractions classiques qui peuvent se commettre au moyen d'un système d'information et de communication. Le troisième expose les dispositions en matière de coopération pénale. Cette dernière devient obligatoire dans la mesure où une Convention ayant pour effet de transformer les rapports entre États en obligations a vocation à transformer les rapports entre États en obligations. La Convention de Budapest ne prévoit pas de sanction. Un comité de suivi peut en revanche intervenir.

Pour autant, cette lutte contre la cybercriminalité se heurte à des difficultés liées à cette nature immatérielle. On peut se demander à quel point les notions de frontières et de territorialité sont adaptées au cyberespace. Concernant la compétence normative, le critère pertinent n'est pas celui du lieu d'action de source mais celui de production des effets, il faut penser les infractions de cette manière, chose qui a été prise en compte en droit pénal international.

La deuxième difficulté en matière de coopération concerne les échanges de données, de fonctionnements des systèmes sur les stratégies et les États peuvent avoir des réticences à ce niveau car ils peuvent indirectement renseigner sur l'organisation du web, sur leur capacité d'action sur Internet. Or, un État ne veut pas renseigner les autres États sur l'avancement de sa propre technologie. Cela suppose un grand degré de confiance.

Une troisième difficulté concerne le cyberespace qui est un lieu de communication. Or, agir dans ce domaine de façon répressive peut porter atteinte aux libertés individuelles. Ce sont ces difficultés inhérentes à ce cyberespace qui vont nécessiter un cadre juridique spécifique.

L'adoption de la Convention de Budapest par des États non européens démontrent l'intérêt porté à la coopération en matière de cybercriminalité (§1). Au niveau international, il existe d'autres organisations multilatérales qui prennent en compte les systèmes d'informations (§ 2).

§1) La Convention de Budapest

« *Il est clair que l'échelle nationale n'est pas suffisante, il faut agir au niveau européen et mondial. Nous souhaitons que la Convention de Budapest, rédigée par le Conseil de l'Europe en 2005, soit transposée au niveau mondial. Il s'agit du premier traité définissant les grands*

principes de la cybercriminalité. Il tente aussi d'harmoniser certaines lois nationales pour améliorer les techniques d'enquêtes en augmentant la coopération entre les nations. C'est un combat de longue haleine, car les pays n'ont pas tous la même vision de ce qu'est la cybercriminalité et comment il faut la traiter. Il est important de s'organiser, car ce n'est que le début. On entre dans un monde connecté[731] ».

Œuvre du Conseil de l'Europe et signée à Budapest en novembre 2001, la Convention sur la cybercriminalité est la première convention pénale destinée à lutter contre le cybercrime. Elle aborde les crimes informatiques afin d'harmoniser certaines lois nationales, d'améliorer les techniques d'enquêtes et d'augmenter la coopération entre les nations. Les infractions commises sur Internet mettent en danger les droits de l'Homme et la démocratie, raison pour laquelle le Conseil de l'Europe est intervenu. Ce traité dépasse le cadre du Conseil de l'Europe dans la mesure où 49 États l'ont ratifié[732]. Par ailleurs, la cybercriminalité étant en constante évolution, le Conseil de l'Europe a décidé de créer à Bucarest un bureau qui soutiendrait les pays dans leur lutte contre la cybercriminalité : le C-PROC[733], et une réunion internationale nommée Octopus a lieu tous les 18 mois et permet de faire le point sur les nouvelles pratiques apparentes. L'objectif est de répondre efficacement aux nombreuses demandes d'assistance.

Elle a vocation à faciliter la lutte contre la cybercriminalité en harmonisant les différentes législations internes. En France, la transposition de cette convention a été faite par la loi n°2005-493 du 19 mai 2005 parue au JO n°116 du 20 mai 2005[734]. Un autre instrument international a été adopté au sein du Conseil de l'Europe, il s'agit du « *Protocole additionnel à la Convention sur la cybercriminalité* » qui est entré en vigueur le 1er mars 2006[735]. Il a vocation à incriminer les actes racistes et xénophobes commis via les systèmes informatiques. Ces deux dispositifs sont les principales armes employées par l'Europe pour lutter contre la

[731] ROLLAND S., *La cybercriminalité est la nouvelle menace du XXIème siècle*, 27 juillet 2015. Disponible à cette adresse : https://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html.
[732] Les États non membres du Conseil de l'Europe l'ayant ratifié sont l'Australie (le 30 novembre 2012), le Canada (le 08 juillet 2015), les États-Unis (le 29 septembre 2006), Israël (le 09 mai 2016), le Japon (le 03 juillet 2012), la République de Maurice (le 15 novembre 2013), le Panama (le 05 mai 2014), la République dominicaine (le 07 février 2013) et le Sri Lanka (le 29 mai 2015).
[733] Bureau de Programme du Conseil de l'Europe à Bucarest.
[734] « *Loi autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* ».
[735] Il a été adopté le 28 janvier 2003 à Strasbourg.

cybercriminalité.

Théoriquement, il s'agit d'une progression importante mais la pratique a démontré l'inefficacité de ces dispositifs et l'absence de prise en compte du Darknet. Concrètement, la Convention définit un cadre juridique minimal qui est nécessaire en matière de cybercriminalité afin d'éviter les zones de non droit (A) et a aussi des conséquences pratiques importantes (B).

A) La mise en place d'un cadre minimal

Dès le début des années 80, le Conseil de l'Europe s'est penché sur l'adoption d'une convention sur la protection des données personnelles à l'égard du traitement automatisé des données. Elle entre en vigueur le 1er octobre 1985. Mais, au delà de la protection des données personnelles, le Conseil de l'Europe s'intéresse aussi aux problèmes de procédure pénale concernant les technologies de l'information, et c'est la raison pour laquelle un comité d'experts chargé de la cybercriminalité est créé, par la décision[736] CDPC/103/211196 du *« Comité européen pour les problèmes criminels »*[737].

[736] « *Les rapides progrès des techniques de l'information ont des répercussions directes sur tous les secteurs de la société moderne. L'intégration des systèmes de télécommunication et d'information, en permettant le stockage et la transmission – quelle que soit la distance – de toutes sortes de données, ouvre un immense champ de possibilités nouvelles. Ces progrès ont été favorisés par l'apparition des réseaux informatiques et des autoroutes de l'information, notamment l'Internet, grâce auxquels toute personne ou presque peut avoir accès à la totalité des services d'information électronique, où qu'elle se trouve sur la planète. En se connectant aux services de communication et d'information, les usagers créent une sorte d'espace commun, dit « cyberespace », qui sert à des fins légitimes, mais peut aussi donner lieu à des abus. Les infractions commises dans ce cyberespace le sont contre l'intégrité, la disponibilité et la confidentialité des systèmes informatiques et des réseaux de télécommunication, à moins qu'elles ne consistent en l'utilisation de ces réseaux ou de leurs services afin de commettre des infractions classiques. Le caractère international des infractions en question – par exemple celles commises au moyen de l'Internet – se heurte à la territorialité des institutions nationales de répression.*
Le droit pénal doit donc suivre le rythme de ces évolutions techniques, qui offrent des moyens extrêmement perfectionnés d'employer à mauvais escient les services du cyber- espace et de porter ainsi atteinte à des intérêts légitimes. Étant donné que les réseaux informatiques ignorent les frontières, un effort international concerté s'impose pour faire face à de tels abus. La Recommandation no. R (89) 9 a certes permis de rapprocher les conceptions nationales touchant certaines formes d'emploi abusif de l'ordinateur, mais seul un instrument international contraignant pourrait avoir l'efficacité nécessaire dans la lutte contre ces nouveaux phénomènes. Un tel instrument devrait non seulement prévoir des mesures de coopération internationale, mais aussi traiter de questions de droit matériel et procédural, ainsi que de facteurs liés à l'emploi des techniques informatiques. »
[737] *Le Comité Européen pour les Problèmes Criminels est instauré en 1958 par le Comité des Ministres afin de superviser et de coordonner les activités du Conseil de l'Europe en matière de prévention et de contrôle du crime. Il se réunit au siège du Conseil de l'Europe à Strasbourg. Lors de ses sessions plénières qui ont lieu deux fois par an sont présents : les délégations nationales des États membres, les représentants de l'Assemblée Parlementaire et du Congrès des Pouvoirs Locaux et Régionaux d'Europe, les représentants de*

Par ailleurs, le comité des ministres crée le « *Comité d'experts sur la criminalité dans le cyberespace* »[738]. Ces comités vont permettre l'élaboration et la présentation au Comité des Ministres de la Convention de Budapest. Le 8 novembre 2001 elle sera adoptée par le comité des ministres du Conseil de l'Europe et signée à Budapest le 23 novembre lors de la Conférence internationale sur la cybercriminalité.

La cybercriminalité relève du droit pénal des nations de sorte qu'il existe autant de définitions que de pays. Dans cette guerre numérique, la convention édicte des infractions relatives à la cybercriminalité afin que les États les adoptent au niveau national, et ce, afin d'harmoniser certaines lois. La section « *droit pénal matériel* » est divisée en cinq titres comprenant douze articles (articles 2 à 13) qui présentent des infractions ayant vocation à être complétées par le droit interne des États membres. Elle s'inspire principalement de la recommandation n° R (89) 9 « *du Comité des ministres aux États membres sur la criminalité en relation avec l'ordinateur* » et des nouvelles pratiques illégales liées à l'évolution des réseaux de télécommunications.

Ainsi, elle ne précise pas explicitement le terme de cybercriminalité mais définit les infractions qui relèvent de celle-ci. Son préambule l'explicite : « *[...] la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ; [...] préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux*[739] *[...]* » ; Le préambule délimite le pourtour de la cybercriminalité en inscrivant sa lutte dans le contexte de la protection des droits fondamentaux qui inclut la protection des données personnelles, la protection des personnes à l'égard du traitement automatisé des données à caractère personnel : « *Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que*

l'Union européenne, et des observateurs. Il réalise des conventions, des recommandations et des rapports en matière de droit et procédure pénales, de criminologie et de pénologie.
[738] *Décision prise le 04 février 1997 lors de la 583ème réunion des délégués des Ministres*.
[739] Conseil de l'Europe – STCE n° 185 – Budapest 23.XI.2001.

garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée [...]».

En outre, la convention suggère une « *coopération entre les États et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information ; [...] une coopération internationale en matière pénale accrue rapide et efficace ; [...] pour faciliter la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international* ».

Composée de quatre chapitres : I) La terminologie ; II) Les mesures à prendre au niveau national ; III) La coopération internationale ; IV) Les clauses finales, elle apporte des définitions communes (1) et fixe un certain nombre d'infraction (2).

1. La détermination de définitions communes

Tout d'abord la convention définit les notions pouvant faire l'objet de plusieurs définitions. Certaines notions techniques fondamentales sont importantes quant à l'application de la Convention, de sorte que des définitions agréées par tous les États ont été établies. À titre d'exemple, le substantif « *informatique* » est devenu un terme polysémique qui vise soit le domaine industriel en rapport avec l'ordinateur, soit la science du traitement des informations par des algorithmes.

En l'occurrence, elle définit l'expression de « *système informatique* » qui désigne « *tout dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données* ». Dès lors, c'est la partie informatique du système d'information qui est visée. Elle est constituée de matériels, logiciels, réseaux et procédures d'utilisation qui permettent le traitement automatique de l'information.

Les « *données informatiques* » désignent quant à elles « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction*[740] ». Il s'agit ici des informations utilisées par les logiciels. Elles peuvent être créées par l'utilisateur ou par un programme.

Ensuite, la Convention prévoit que les fournisseurs de service peuvent désigner d'une part, « *toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique* » et d'autre part, « *toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs* ».

Enfin, les « *données relatives au trafic désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent* ». Ces définitions communes sont utiles à la détermination des infractions (2).

2. La détermination d'infractions

La Convention de Budapest définit un cadre juridique minimal qui est nécessaire en matière de cybercriminalité afin d'éviter les zones de non droit.

Plusieurs types d'infractions sont fixées contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et de leurs données[741]. Il y a « *l'accès illégal*[742] », «*l'interception illégale*[743] », « *l'atteinte à l'intégrité des données*[744] » et « *les abus de dispositif*[745] ».

D'autres infractions dites « *informatiques*[746] » répriment la « *falsification informatique*[747] » et

[740] Article 1.b. de la Convention de Budapest sur la cybercriminalité, STE n°185, page 6.
[741] « Titre I – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ».
[742] Article 2 de la Convention.
[743] Article 3 de la Convention.
[744] Article 5 de la Convention.
[745] Article 6 de la Convention.
[746] « Titre 2- Infractions informatiques ».
[747] Article 7 de la Convention.

la « *fraude informatique*[748] ». Sont donc visés « *l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques* » ainsi que « *toute forme d'atteinte au fonction d'un système informatique dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui* ». Ces incriminations rejoignent la directive du 13 décembre 1999[749] qui crée une équivalence entre l'écrit électronique et l'écrit papier.

Ensuite, la Convention pose un cadre minimal concernant les « *infractions se rapportant au contenu*[750] » en visant celles « *se rapportant à la pornographie enfantine* ». Sont ainsi visées les productions, offres, mises à disposition, diffusions, transmissions, procuration et possession de pornographie enfantine impliquant des mineurs de dix-huit ans[751], voire de seize ans si le droit interne de l'État le prévoit. Ces règles concernant la pédopornographie sont essentiellement symboliques puisqu'en la matière, les États sont presque tous tomber d'accord : la pédophilie est un fléau qu'il est nécessaire d'éradiquer.

Enfin, les « *infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes*[752] » permettent, au sein de chaque État, de viser de tels actes « *commis délibérément, à une échelle commerciale et au moyen d'un système informatique* ». L'article 10 de la convention érige en infraction pénale les atteintes à la propriété intellectuelle, définies par le droit interne de chaque État, conformément aux droits protégés par l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne[753], par l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et par le traité de l'Organisation Mondiale de la Propriété Intellectuelle. En ce sens, en France, la victime de contrefaçon a la possibilité d'opter pour la voie civile ou pour la voie pénale[754], de sorte que la convention n'a pas apporté de changement majeur. En revanche, « *les droits connexes* » de la convention ont imposé quelques modifications. Outre la détermination des infractions liées à la cybercriminalité, la Convention

[748] Article 8 de la Convention.
[749] Directive 1999/93/C.E du 13 décembre 1999 sur un cadre commun pour les signatures électroniques.
[750] Titre 3- Infractions se rapportant au contenu.
[751] Mineur de moins de 18 ans est un pléonasme car « mineur » du latin minor signifie « *moins de* ».
[752] Le titre 4 et l'article 10 sont intitulés de la même manière.
[753] Pour la protection des œuvres littéraires et artistiques.
[754] Voir première partie, titre I, chapitre 1, section 2, §1, A, 2. la guerre du téléchargement en France.

de Budapest emporte des conséquences pratiques (B).

B) Les conséquences pratiques

« *De 2014 à 2015, on observe une forte croissance des méfaits liés à la cybercriminalité (de 62,3% à 67%). L'hacktivisme reste en seconde position des raisons de piratage, avec néanmoins un recul de près de 4 points (de 24,9% à 20,8%). Les attaques pour cyberespionnage demeurent stables aux alentours de 10%. Enfin, les opérations de cyberguerre sont discrètes à 2,5%*[755] ». Pour faire face à ce fléau, la stratégie internationale s'est concrétisée avec une harmonisation des dispositions pénales, une consolidation de la coopération policière (1) et avec des mesures relatives aux données (2). C'est ce qui a été mis en place par la Convention de Budapest.

1. Une meilleure coopération policière

« *Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace*[756] », la Convention de Budapest préconise une coopération entre les États signataires qui pourront être amenés à utiliser des moyens coercitifs sur leur propre territoire, pour les besoins d'un autre État, s'ils concernent une infraction visée dans la Convention.

Elle aspire à une meilleure efficacité pour les enquêtes et procédures pénales d'infractions en lien avec les données et systèmes informatiques en « *tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclu entre les États membres du Conseil de l'Europe et d'autres États* ».

En dehors du préambule, la convention rappelle que la coopération internationale est une priorité puisque l'article 23 précise que « *les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des*

[755] CHEMINAT J., *Cyberattaques : un cru 2015 très actif et plus criminalisé*, 12 février 2016. Disponible à cette adresse : https://www.silicon.fr/cyberattaques-un-cru-2015-tres-actif-et-plus-criminalise-138826.html, [consulté le 4 avril 2017].
[756] Convention sur la cybercriminalité, Préambule, page 1.

arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale ».

Ces demandes d'aide peuvent être opérées par le biais d'Interpol ou d'Europol : « *C'est un centre ultramoderne, doté d'ordinateurs de grande capacité. Le choix s'est porté sur Singapour, car Lyon n'avait pas la place pour l'accueillir. Il dispose d'experts et d'équipements à la pointe du progrès, au service de deux grandes missions. D'abord, la recherche autour du développement des nouvelles technologies par les criminels, de manière à fournir aux services de police des outils de riposte adaptés. Ensuite, le Complexe fournit une aide aux enquêteurs du monde entier, via des formations, des échanges d'informations et un renforcement des capacités d'intervention. Il travaille aussi avec d'autres organismes transnationaux comme Europol, le réseau des polices des pays de l'UE. Actuellement, le centre compte 95 personnes, mais l'effectif va monter en puissance pour atteindre 160 employés d'ici à 2018-2019*[757] ».

En outre, l'article 35 de la Convention de Budapest prévoit la mise en place d'un « *point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin* d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme electronique d'une infraction pénale. Les échanges d'informations entre représentants des différentes polices ont ainsi été développés par Interpol tandis qu'Europol traite les différentes bases d'informations pour assurer une meilleure coordination des actions policières.

En France, ce point de contact joignable en permanence est l'Office central de lutte contre la criminalité liée aux techniques de l'information et de la communication créé le 15 mai 2000. Il est chargé d'apporter des conseils techniques, de conserver des données, de recueillir des preuves, d'apporter des informations à caractère juridique et de localiser les suspects. Il permet une assistance immédiate pour les enquêtes pénales liées à un système et aux données informatiques (2).

[757] ROLLAND S., La cybercriminalité est la nouvelle menace du XXIe siècle, 26 juillet 2015. Disponible à cette adresse : https://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html.

2. Les mesures relatives aux données

La Convention de Budapest prévoit de nouvelles procédures concernant la conservation rapide des données, leur injonction, leur perquisition, leur saisie ainsi que la collecte en temps réel des données de trafic et l'interception de celles relatives au contenu. Les autorités de chaque État doivent être en mesure de perquisitionner et saisir les informations concernant les infractions informatiques.

En France, dans les articles 56 et 97 du Code de procédure pénale ont respectivement été ajoutés aux termes « *documents* » et « *pièces* » les termes « *données informatiques* » et « *informations* » afin de saisir tout type d'information numérique dans le cadre d'une enquête.

De plus, l'autorité judiciaire a la possibilité d'obtenir les copies des données informatiques et d'obtenir une version accessible des données cryptées. Elle peut même réquisitionner les opérateurs téléphoniques afin d'obtenir les données de connexions et le contenu des communications conformément à ce que prévoit la loi en matière d'écoute téléphonique[758] et conformément au Code des postes et des communications électroniques[759] : « *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. Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire* » de données de leurs utilisateurs pour un délai maximal d'un an.

Les opérateurs privés sont tenus de conserver les données utiles aux enquêtes, comme des

[758] Code de procédure pénale art. 100 et suivants.
[759] Article L34-1.

preuves de connexions. Ces mesures sont encadrées par l'article 17 de la Convention[760] qui renvoie aux articles 14 et 15 dont l'application prévoit qu'elles soient soumises à certains principes[761]. Il s'agit de trouver un équilibre entre la sécurité des citoyens et les atteintes aux libertés individuelles.

La « *perquisition et la saisie des données informatiques stockées* » prévue à l'article 19 de la convention définit le formalisme et les conditions de la perquisition. La preuve numérique est donc reconnue par la convention qui ne pose que les conditions de la perquisition physique sans égard pour la perquisition à distance, très utile en la matière. La protection des libertés individuelles est certainement un élément permettant de justifier cet oubli.

La « *collecte en temps réel de données informatiques* » prévue dans le Titre 5 a trait aux interceptions de données sur les différents réseaux. Ces interceptions sont effectuées en temps réelles pour des données de natures différentes, les données relatives au trafic[762] définies par l'article 1 comme « *toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent* », et des données relatives au contenu[763], non

[760] « *Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15* ».

[761] Chaque Partie veille à ce que l'instauration, la mise en oeuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

[762] Chapitre II, Section II, Titre 5, article 20 de la Convention : « *1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes : a) à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et b) à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes : i/ à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou iii/ à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique* ».

[763] Chapitre II, Section II, Titre 5, article 21 de la Convention : « *1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne : a) à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et b) à obliger un fournisseur de services, dans le cadre de ses capacités techniques: i/ à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou ii/ à prêter aux autorités compétentes son concours et son assistance pour collecter ou*

définies par la convention. Concrètement les données relatives au contenu sont celles qui concernent le fond du message ou de l'information transmise. La distinction entre les deux types de données est importante dans la mesure où l'atteinte à la vie privée de l'utilisateur diffère puisque l'interception d'une donnée relative au contenu peut aller à l'encontre de la liberté de communication.

Pour que cette harmonisation soit la plus efficace possible, les États membres devront respecter ce cadre minimal mais aussi faciliter l'entraide judiciaire entre les différents services. D'autres organisations internationales tentent de lutter contre la cybercriminalité (§2).

§2) Les autres organisations

L'évolution du numérique a changé Internet qui est passé d'un espace de liberté à un outil de surveillance grâce aux facilités de stockage et de traitement qu'il offre. Pour faire face à une collecte grandissante de données personnelles, par les géants du Net et les services de renseignement[764], le Darknet est de plus en plus utilisé avec ses côtés positifs et négatifs. Les cybermenaces se sont multipliées et ont contraint les États à envisager une coopération totale entre eux. A titre d'exemple, les 9 et 10 décembre 1997, les membre du G8[765] ont programmé une rencontre entre les ministres de l'Intérieur et de la Justice de l'organisation afin d'examiner les cybermenaces et les dangers de la sécurité des informations numériques. D'autres organisations luttent contre la cybercriminalité. Ainsi, il est possible de citer l'OTAN ou l'ONU. L'Organisation du traité de l'Atlantique Nord s'est également dotée de deux centres dédiés à la recherche sur cyberdéfense afin de former des agents chargés de combattre les infractions commises sur la Toile. L'ONU sera étudiée dans la sous-partie suivante (A). Toutefois, une réelle coopération internationale est freinée par les disparités des droits internes et l'absence de volonté politique de gérer ensemble une situation très claire (B).

enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique ».

[764] Voir l'affaire Snowden.

[765] Créé en 1975, le G8 était composé de la France, les États-Unis, l'Italie, le Japon, le Royaume-Uni et l'Allemagne. Le Canada a été inclus en 1976 et la Russie progressivement à partir de 1998. Par conséquent, la Russie n'était pas présente à cette rencontre.

A) L'exemple de l'ONU

Pour les Etats-Unis, la lutte contre la criminalité informatique est essentielle et c'est la raison pour laquelle c'est le premier pays à avoir pris en compte le Darknet. Mais face aux atteintes occasionnées par la cybercriminalité, les autres États se sont très rapidement intéressés à ce phénomène qui n'épargne personne. Dès lors, compte tenu du caractère transfrontalier de la cybercriminalité, une lutte groupée a été nécessaire.

Par exemple, l'unité « cybercrime » de l'ONU lutte contre la cybercriminalité et surtout contre l'exploitation sexuelle des mineurs sur Internet puisqu'elle traque fermement les pédophiles qui agissent sur les réseaux : « *Les auteurs de cybercriminalité et leurs victimes sont souvent situés dans des régions différentes et leurs effets se répercutent dans les sociétés du monde entier. Cela souligne la nécessité de mettre en place une réponse urgente, dynamique et internationale*[766] ».

Financé par quelques pays[767], le programme mondial sur la cybercriminalité a vocation à assister les États membres de l'ONU dans la lutte contre la cybercriminalité en application de plusieurs résolutions[768]. Avant même le lancement de ce programme mondial, l'ONU a tenté d'apporter des réponses en matière de cybercriminalité. En 2011, une réunion a été organisée sur les normes internes, les pratiques, l'assistance technique et la coopération[769].

L'ONU apporte une précision concernant les crimes commis sur Internet. Généralement, les cyber infractions concernent *« i) infractions à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes informatiques ; ii) les infractions informatiques ; iii) les infractions liées au contenu ; iv) infractions liées aux atteintes au droit d'auteur et aux droits connexes*[770] ».

[766] Site web de l'ONU, *Programme mondial sur la cybercriminalité*. Disponible à cette adresse : https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.
[767] Le programme mondial sur la cybercriminalité est entièrement financé par les Gouvernements américain, britannique, norvégien, japonais, canadien et australien.
[768] De la résolution 65/230 de l'Assemblée générale et des résolutions 22/7 et 22/8 de la Commission pour la prévention du crime et la justice pénale.
[769] *Open-ended intergovernmental expert group meeting on cybercrime*. Disponible à cette adresse : https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html.
[770] *« i) offences against the confidentiality, integrity and availability of computer data and systems ; ii) computer-related offences ; iii) content-related offences ; iv) offences related to infringements of copyright and related rights* ».

Aussi, l'ONU agit aussi bien sur le web visible que sur le Web invisible en différenciant le *Deep Web* du Darknet : « *Ce que la plupart des gens voient en ligne, ce n'est qu'une petite partie des données disponibles sur le web visible. La plupart des moteurs de recherche, par exemple, indexent seulement 4% d'Internet. Le Deep Web, défini comme une partie du World Wide Web qui n'est pas détectable par les moteurs de recherche, comprend des informations protégées par un mot de passe, des réseaux sociaux aux serveurs de messagerie. Le Darknet est un ensemble de milliers de sites Web qui utilisent des outils d'anonymat tels que TOR pour chiffrer leur trafic et masquer leurs adresses IP. Le niveau élevé d'anonymat dans l'espace numérique permet aux criminels d'agir sans être facilement détectés*[771] ».

Toujours concernant le Darknet, il est intéressant de constater que les Nations Unies définissent également les bons côtés du réseau sombre : « *Le Darknet est surtout connu pour ses ventes d'armes au marché noir, ses ventes de médicaments et la diffusion d'enfants maltraités. Le darknet est également utilisé pour le bien, notamment en permettant aux militants des droits de l'homme et aux journalistes de s'exprimer librement*[772] ». Toutefois, malgré cette prise en compte, la coopération reste lacunaire (B).

B) Une coopération lacunaire

Les États ont mis en place des instruments juridiques concrets pour lutter contre les infractions liées à l'informatique. Néanmoins, le résultat n'est pas à la hauteur des espérances puisque les statistiques prouvent que la cybercriminalité n'a pas été ralentie. Les coopérations judiciaires de l'Union européenne et du Conseil de l'Europe ont montré leurs limites.

D'aucuns[773] estiment que l'harmonisation du droit pénal n'est pas efficace en raison de la

[771] Texte original : « *What most people see online is only a small portion of the data that's out there on the clearnet. Most search engines, for example, only index 4% of the internet. The Deep Web, which is defined as a part of the World Wide Web that is not discoverable by search engines, includes password-protected information - from social networks through to email servers. The Darknet is a collection of thousands of websites that use anonymity tools like TOR to encrypt their traffic and hide their IP addresses. The high level of anonymity in the digital space enables criminals to act without being easily detected* »
[772] Texte original : « *The darknet is most known for black-market weapon sales, drug sales and child abuse streaming. The darknet is also, however, used for good - including enabling free speech by human rights activists and journalists* ».
[773] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016.

grande marge de manœuvre qui est laissée aux États membres qui ne sont pas tout le temps contraints de modifier leurs dispositions. En effet, les États ne sont pas coopératifs. Certains pays comme l'Allemagne, les Pays-Bas ou l'Espagne, ne sont pas très emballés quand il s'agit de transposer une directive européenne. Ainsi, même s'ils ont adhéré à la Convention sur la cybercriminalité, certains pays ne sont pas forcément inspirés lorsqu'il s'agit d'harmoniser les lois ou de coopérer avec d'autres pays.

La coopération judiciaire passe nécessairement par une approche législative consistant à harmoniser les systèmes pénaux internes. Ainsi, certaines infractions ont fait l'objet d'une définition et de sanctions communes. Toutefois, la procédure pénale a été négligée. Or, la matière procédurale est nécessaire à l'application des mécanismes de coopération. L'effectivité des réseaux judiciaires internationaux passent par un rapprochement des droits pénaux matériels mais aussi des droits procéduraux des États membres. A défaut, la diversité des droits pénaux et procéduraux pourra être exploitée par les cybercriminels, qui pourront en profiter directement ou indirectement dans la mesure où des disparités pourraient gêner les enquêtes judiciaires et les internautes qui ne peuvent pas connaître tous les droits pénaux et procéduraux des États du monde.

Toutefois, la collaboration entre États trouve sa limite dans la territorialité puisque chaque État est compétent pour fixer les règles pénales sur son territoire. Il en résulte des systèmes répressifs différents aux niveaux national et international posant problème lorsqu'une infraction présente un élément d'extranéité. En effet, la souveraineté des États leur assure une liberté dans l'organisation de leurs systèmes pénaux créant ainsi à l'échelle mondiale la juxtaposition de plusieurs règles appropriées à chaque État.

CONCLUSION TITRE I
L'ARSENAL REPRESSIF EN MATIÈRE DE CYBERCRIMINALITÉ DISSIMULÉE

En droit pénal, il existe des responsabilités spécifiques aux communications électroniques et aux outils numériques dont fait partie le Darknet. Il est alors possible de différencier deux types de cybercriminalité.

La première cybercriminalité définie comme la « *criminalité de la communication* » concerne les atteintes aux réseaux Internet et Darknet. Elle concerne des infractions qui n'existaient pas avant leur apparition. Des phénomènes comme l'intrusion et le sabotage informatiques ou le détournement de données protégées se sont démocratisés. Ce faisant, le législateur français a riposté et s'est doté d'un arsenal répressif efficace qui a permis d'établir une jurisprudence abondante.

La seconde cybercriminalité définie comme la « *criminalité par la communication* » concerne des infractions classiques qui sont facilités par l'utilisation d'Internet et du Darknet. Sur ce dernier la puissance des criminels s'est amplifiée et la vulnérabilité des victimes accentuée. Des infractions relatives aux stupéfiants, aux terroristes et à la pédophilie sont devenues les fléaux du Darknet. À l'instar de la criminalité informatique, le législateur dispose d'un arsenal répressif complet permettant de lutter contre ces infractions.

Toutefois, ces dispositions relatives aux technologies numériques existent de manière éparpillée et nécessiteraient une harmonisation. En ce sens elles pourraient être réunies dans un même chapitre afin de garantir une meilleure application et une meilleure compréhension.

En outre, la pratique a révélé de nouveaux défis puisqu'une infraction peut impliquer plusieurs États. Or, les différents systèmes juridiques ne se sont pas adaptés de la même manière à ce nouveau phénomène. Par conséquent, une coopération a été nécessaire afin d'agir de manière concertés contre le cyberespace qui n'a aucune frontière. Des initiatives de coopération à l'échelle européenne ou internationale se sont mises en place pour lutter contre la cybercriminalité. La Convention de Budapest sur la cybercriminalité en est le parfait exemple.

Cependant, il y a énormément de lacunes quant à la compétente territoriale française qui ne s'est pas du tout adaptée à cette cybercriminalité internationale qui a migré vers le Darknet. À cet endroit l'anonymat et le chiffrement des données restent foncièrement présents et compliquent la tâche des enquêteurs qui doivent respecter les règles de procédure pénale (Titre II).

TITRE II
UN SYSTÈME JUDICIAIRE INADAPTÉ A LA CYBERCRIMINALITÉ DISSIMULÉE

Les cybercriminels ont su s'adapter au Darknet afin d'exploiter ses particularités pour y commettre des infractions. Sous couvert d'un anonymat renforcé, ils ont su porter atteintes aux biens et personnes sans égard pour les frontières. Le caractère international de la cybercriminalité dissimulée fait en sorte que la lutte doit être envisagée par l'ensemble des pays pour que le cyberespace ne devienne pas une zone de non droit. Ce territoire sans limite qu'est le Darknet offre aux cybercriminels la possibilité d'agir dans des pays où la législation est différente, pas encore au point ou moins sévère, tout en étant basés dans un autre pays afin d'atteindre des victimes qui ne soient pas en mesure de s'en rendre compte immédiatement. C'est cet élément d'extranéité qui complique la tâche des enquêteurs qui sont ainsi confrontés à plusieurs difficultés relatives à la fois au fond et à la forme. En effet, il est très difficile d'identifier les auteurs et les victimes d'infractions, mais il y a également des obstacles quant à la recherche des preuves puisque certains pays autorisent la provocation à l'infraction alors qu'elle n'est pas admise en France.

Les cadres normatifs européen et international sont-ils suffisamment efficaces pour poursuivre les infractions relevant de la cybercriminalité dissimulée ? En dépit de la volonté coopérative, les États ont été confrontés à des problèmes relatifs à la compétence juridictionnelle à la suite de la découverte d'une infraction. En effet, la convention de Budapest se heurte à des procédures très lourdes qui contraignent les États à remplir des formulaires avec des délais de traduction pouvant être un frein. On peut alors légitimement se demander si une infraction commise sur le Darknet et liée à plusieurs Etats peut être poursuivie devant différentes juridictions pénales. Pourquoi un Etat serait-il plus légitime qu'un autre pour poursuivre ? De plus, les mécanismes juridiques varient fortement d'un pays à un autre et compte tenu de son caractère international l'espace numérique nécessite un cadre législatif serein et adapté. La poursuite des infractions se fait plus efficacement dans certains pays mais de manière générale il y a de réelles déficiences législatives dans la répression de cette nouvelle forme de cybercriminalité dissimulée.

L'exécution d'une infraction peut se faire sous différentes formes, il peut s'agir d'un acte positif, ou d'une abstention, d'un acte unique ou de plusieurs actes, d'un acte instantané ou d'une action qui se prolonge dans le temps. La simple pensée coupable ne suffit pas à appliquer une sanction pénale à individu. Un pédophile qui s'imagine en train de violer un enfant ne peut pas être poursuivi. Ainsi, sauf exception[774], le droit français ne punira pas un individu *ante delictum*, c'est-à-dire avant qu'il ne soit passé à l'acte. Cet acte peut avoir différentes formes. De plus, dans certains cas, l'individu sera poursuivi sur le terrain de la tentative, alors même qu'il n'a pas atteint le résultat recherché.

L'étude de l'élément matériel de l'infraction permet d'examiner les différents moyens d'atteindre le résultat interdit par la loi, en les classant en fonction de leur nature, de leur durée ou de la nécessité de l'atteinte d'un résultat ou non. Une première distinction peut être envisagée entre les infractions par commission qui supposent la réalisation d'un acte positif et celles par omission qui résultent d'une simple abstention. L'individu fait ce que la loi interdit, il atteint le résultat illicite en accomplissant de manière concrète ce que la loi vise de manière abstraite. Le résultat est la conséquence de l'acte interdit. À titre d'exemple, le code pénal interdit la pédopornographie en prévoyant que cette dernière est « *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*[775] ». Dès lors, un individu qui diffuse les images pornographiques d'un mineur se rend coupable de ce délit : son action positive recouvre la définition prévue par la Code pénal. À l'instar du droit de la responsabilité civile délictuelle, l'infraction de commission suppose, elle aussi, une faute qui peut prendre plusieurs formes, en l'occurrence celle que la loi prévoit, un résultat et un lien de causalité entre les deux. Dans son sens le plus logique le résultat est la conséquence de l'acte interdit. Toutefois, la doctrine distingue le résultat sociologique, le résultat matériel et le résultat juridique. Le premier concerne le type d'atteinte à l'ordre social. Ainsi, le vol, l'escroquerie et l'abus de confiance entraînent une atteinte à la propriété. Le deuxième est la conséquence immédiate du comportement incriminé : la conséquence du vol est un déplacement de la propriété. Le troisième type de résultat est celui qui conduit à une atteinte effective à la valeur

[774] Loi n°2008-174, JO 26 février 2008, page 3266, partie relative à la rétention de sûreté qui permet de maintenir en détention une personne qui a accompli sa peine et qui n'a pas encore commis de nouvelle infraction.
[775] Code pénal art. 227-23.

sociale protégée par le droit pénal[776]. Dès lors, l'importance de la sanction pénale ne dépend pas de l'importance du résultat : « *qui vole un œuf, vole un bœuf* ». L'autre moyen de parvenir à un résultat illicite résulte de l'abstention. Le délinquant va obtenir le résultat illicite en se gardant d'agir. Ces actes d'omission ne sont réprimés que s'ils sont expressément incriminés par un texte qui impose une certaine obligation et sanctionne ceux qui ne l'accomplissent pas. Même si ce type d'infraction a augmenté, il reste moins courant que les interdictions dans la mesure où notre société est basée sur des principes de liberté individuelle. Il existe deux sortes d'omission. En effet, la doctrine distingue l'omission dite « *pure et simple* » de l'infraction de commission par omission. La première ne soulève pas de difficultés particulières puisque l'individu ne fait pas ce que la loi impose : le fait de ne pas attacher sa ceinture de sécurité dans un véhicule est une infraction d'omission pure et simple prévue par le code de la route. La seconde est proche de la commission puisque le résultat est identique mais également proche de l'omission car l'agent n'a pas agi positivement. Ainsi, il est possible de tuer une personne en l'exécutant ou en la laissant mourir. Néanmoins, en vertu du principe de la légalité criminelle et de l'interprétation stricte de la loi, le juge ne pourra condamner, celui qui laisse mourir, que pour le délit de non assistance à personne en péril prévu à l'article 223-6 du Code pénal[777]. Les infractions commises sur le Web dissimulé tels que le terrorisme, la prostitution, la pédocriminalité, l'escroquerie, le trafic d'armes, le trafic de drogues et les cyberattaques, sont toutes des infractions de commission. Mais la non-révélation d'infractions en rapport avec des actes de terrorisme peut par exemple constituée une infraction par omission[778].

Une autre distinction concerne les infractions simples, complexes ou d'habitude. Tout d'abord les infractions simples sont celles qui se consomment par l'accomplissement d'un acte matériel unique. Tel est le cas du vol qui est consommé par la seule soustraction frauduleuse de la chose d'autrui. Ensuite, les infractions complexes supposent quant à elles une pluralité d'actes matériels pour être consommées. Lorsque ces actes sont de nature différente, alors il s'agit d'une infraction complexe « *pure et simple* ». Dès lors, l'escroquerie[779] suppose d'une part, l'utilisation de moyens frauduleux et, d'autre part, la remise d'un bien. En revanche, lorsqu'il s'agit de la réalisation de plusieurs actes similaires, qui pris isolément, ne constituent pas une

[776] CONTE P., MAISTRE DU CHAMBON P., *Droit pénal général*, 4e éd. Armand Colin, 2004.
[777] Voir l'affaire dite « *de la séquestrée de* Poitiers » : Poitiers, 20 novembre 1901.
[778] Code pénal Art. 434-1.
[779] Code pénal Art. 313-1.

infraction, alors il s'agit d'une infraction d'habitude. C'est le cas notamment de l'exercice illégal de la médecine. Cette distinction trouve son importance lorsqu'une procédure est enclenchée. En effet, tous les tribunaux dans le ressort desquels ont été accomplis un des actes matériels de l'infraction complexe ou d'habitude sont compétents. Ainsi, la loi pénale française est applicable dès lors qu'un des actes matériels a été commis en France, même si les autres ont été accomplis à l'étrangers[780]. De plus, pour une infraction simple, le point de départ de la prescription de l'action publique est le jour de la réalisation de cet acte unique, alors que pour une infraction complexe, il est nécessaire que tous les éléments matériels soient réalisés. Par exemple, pour l'escroquerie le délai ne court qu'au moment du dernier versement.

Ensuite, une distinction fondée sur la durée existe puisque les infractions instantanées sont traditionnellement opposées par la doctrine ou la jurisprudence aux infractions continues. Les premières se consomment en un trait de temps, comme le meurtre qui se consomment par le décès de la victime[781]. À l'inverse, la commission des secondes suppose une certaine durée, comme la séquestration qui ne peut se réaliser en quelques secondes. En outre, l'infraction peut être permanente lorsque l'acte matériel s'exécute en un trait de temps, mais avec des effets qui se prolongent dans le temps, comme le délit de construction d'un immeuble sans permis de construire. Cette distinction a de nombreuses conséquences. Ainsi, la prescription d'une infraction continue ne court que lorsque le délit est fini, alors que celle d'une infraction instantanée ou permanente, court le jour de la commission de l'acte incriminé même si les effets se prolongent après cette date. Elle a aussi un impact sur l'application de la loi pénale dans le temps.

En France, l'arsenal législatif utilisé pour la lutte contre la cybercriminalité existe déjà mais doit être amélioré afin que les acteurs de cette lutte aient le sentiment de combattre à armes égales. En effet, la loi est trop souvent en retard par rapport à l'évolution constante du monde numérique. Pour plus d'efficacité, il faut que chaque réforme prenne en compte le travail de tous ceux qui combattent l'insaisissable cybercriminalité : les enquêteurs, les magistrats du siège et du parquet, les pouvoirs publics et les dirigeants. La formation de tous ces acteurs ainsi que les moyens techniques et financiers ne peuvent pas être négligés pour faire face à l'ampleur

[780] Voir le thème sur l'applicabilité de la loi pénale.
[781] Un meurtre peut durer plusieurs heures, mais l'infraction ne se consommera instantanément qu'au moment du décès.

du phénomène. Par ailleurs, la vision française de cette réalité n'est pas suffisante. La Convention de Budapest du 23 novembre 2001 l'illustre parfaitement. Elle permet en théorie de combattre le fléau grâce à une meilleure collecte des preuves. Pourtant, dans un domaine par essence régalien, une telle convention a du mal à trouver sa place au sein de chaque Etat et son efficacité n'est pas à la hauteur des attentes. Dans la lutte contre la cybercriminalité dissimulée l'attention doit être portée sur la procédure pénale et notamment sur l'interception et la captation de données, sur la géolocalisation, sur le chiffrement et sur l'accès de la preuve. En ce sens, au niveau européen, la Commission européenne[782] présente régulièrement ses travaux sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective en matière de cybercriminalité. Le 26 juillet 2017, elle a travaillé sur l'amélioration de l'accès à la preuve numérique et s'est consacrée à une enquête auprès de la société civile : « *afin de recueillir les avis des parties intéressées (États membres, institutions et agences européennes, représentants du secteur privé, associations, ...) sur ces travaux. Les questions posées visent à recueillir des informations sur les pratiques actuelles en matière d'obtention de preuves électroniques transfrontalières dans les États membres ainsi que sur les problèmes pratiques et juridiques rencontrés* ». Le même sujet a été abordé au niveau international avec un protocole additionnel à la Convention de Budapest qui aurait pour but d'améliorer l'accès à la preuve numérique entre les Etats-Unis et l'Europe notamment.

La poursuite des infractions sur Internet est limitée par tous ces obstacles liés à la territorialité et à la souveraineté des Etats. Par exemple, en matière de lutte contre la cybercriminalité, nombreuses sont les problématiques qui affectent la collecte des preuves numériques. Or, la preuve de l'infraction de manière certaine et non équivoque est nécessaire pour qu'elle ait des conséquences juridiques. En cas d'impossibilité, le droit pénal n'a pas vocation à s'appliquer (Chapitre 1) dans la mesure où tout individu qui se voit reprocher un délit ou un crime, est réputé innocent tant que sa culpabilité n'a pas été démontrée de manière légale (Chapitre 2).

[782] Il s'agit de l'une des principales institutions de l'Union Européenne siégeant à Bruxelles.

CHAPITRE 1
DES DIFFICULTÉS LIÉES A L'APPLICATION DE LA LOI PÉNALE

Internet est à la fois un bienfait et un danger pour la démocratie. Concernant ses bienfaits, il favorise son développement en permettant une meilleure communication à moindre coût. C'est ainsi qu'il est devenu un lieu de débats où s'échangent des informations et se confrontent des points de vue par le biais des réseaux sociaux, des courriers électroniques, du Web et des forums. Ensuite, il permet une meilleure diffusion de l'information aux citoyens et garantie une meilleure interaction entre gouvernants et gouvernés. Les échanges par courriers électroniques permettent aux administrés de transmettre leurs attentes et réactions aux élus. Certains imaginent même Internet comme un outil qui permettrait de faire participer les citoyens au processus législatif via des forums ouverts à l'Assemblé Nationale et au Sénat ou grâce à l'envoi de propositions d'amendements aux élus. Un forum ouvert avait été envisagé lors de l'élaboration du projet de constitution européenne[783]. Des organisations de la société civile ont eu la possibilité de verser leurs contributions aux débats. Enfin, Internet permet de favoriser les actions collectives en mobilisant des individus isolés avec les mêmes idées.

Toutefois, Internet présente également des dangers pour la démocratie. Tout d'abord, seule une minorité de la population mondiale est concernée par son utilisation, seule une certaine élite peut s'y connecter de manière régulière, on parle de « *fracture numérique* ». De plus, Internet fragilise fortement la protection de la vie privée avec les cookies et la collecte des données personnelles à but commercial par les GAFA. Internet est également le support d'idée contredisant les fondements de la démocratie puisque nombreux sont les sites diffusant des idées racistes ou négationnistes. Le Darknet présente également cette double facette en étant à la fois un danger et un vecteur de liberté. Pour cette raison, les Etats ne souhaitent pas qu'il soit comme son cousin, un média sans contrôle démocratique : « *Internet, en s'affranchissant des frontières, pose le problème du contrôle des serveurs et des sites. Les juridictions nationales peinent à imposer leur verdict et les législateurs à suivre le rythme des évolutions technologiques*[784] ».

[783] Février 2002-juillet 2003.
[784] http://www.vie-publique.fr/decouverte-institutions/citoyen/enjeux/media-democratie/internet-bienfait-ou-danger-pour-democratie.html.

Pourtant, contrairement à Internet, le Darknet a su s'émanciper et échapper aux contrôles Étatiques. Mais, ce qui inquiète le plus, c'est la possibilité de commettre des infractions en toute impunité, et l'appréhension du droit pénal à l'endroit de cette cybercriminalité dissimulée. La nature transnationale de ces réseaux complique l'application du droit et implique une surabondance des systèmes juridiques si bien que pour des mêmes faits, plusieurs droits peuvent se faire concurrence.

En effet, le principe de légalité s'applique également en droit pénal international si bien qu'une infraction suppose un texte préétabli. Cela nécessite une intervention des États qui ont le monopole sur le droit pénal et déterminent les comportements antisociaux, c'est-à-dire les infractions : « *En droit pénal international, le juge n'applique jamais que sa propre loi et il l'applique toujours comme loi normalement applicable au rapport de droit. Le juge d'un Etat quelconque ne sera jamais saisi de la répression du fait incriminé que si ce fait constitue un délit au regard de l'Etat au nom duquel il punit, et au regard de la loi qu'il a pour mission d'appliquer : dans ces conditions, il ne frappera jamais son auteur que des peines que cette loi y attache*[785] ».

Toutefois, le principe de territorialité de la loi pénale et notamment l'universalité, se concilient mal avec le concept d'Etat souverain. Cela se confirme lorsque les lois pénales de différents Etats se font concurrence pour une même infraction liée à la cybercriminalité internationale. Dès lors, une même cyber infraction peut faire l'objet de plusieurs poursuites et même de plusieurs condamnations dans différents pays. La nécessité d'une harmonisation homogène se fait ressentir au niveau international pour les infractions commises sur Internet et sur le Darknet. Cela est justifié par le fait que les systèmes pénaux nationaux peuvent se contredire et créer une insécurité juridique. En somme, la cybercriminalité a créé des problèmes en matière d'applicabilité de la loi pénale dans l'espace (section 1), et en ce qui concerne le travail des juges (section 2).

[785] BARTIN E., *Etude de droit international*, Université Paris Descartes, 2016, page 214.

SECTION 1
L'applicabilité de la loi pénale dans l'espace

Chaque technologie offre un nouveau potentiel criminel permettant de réaliser des activités illicites. Ainsi avec le Darknet, les criminels peuvent utiliser des actions illégales, avec une relative impunité puisque les conditions leurs sont réellement favorables. Dorénavant le risque est minime au regard du profit qu'ils peuvent tirer d'un champ d'action mondialisé**.** Les criminels s'organisent autour de l'échange d'information grâce à l'informatique et aux télécommunications. Dès lors, le Darknet n'a pas de frontières géographiques puisque qu'il s'agit de plusieurs réseaux interconnectés entre eux. Sa couverture géographique est transfrontalière. Le criminel tire parti de cette « *aterritorialité* » d'Internet, de l'inexistence dans certains États de lois réprimant le crime informatique et des juridictions multiples dont relève le réseau des réseaux. À l'instar des paradis fiscaux, il existe des paradis numériques où un malfaiteur peut agir ou héberger des serveurs et des contenus illicites en toute impunité. La poursuite d'un crime informatique dépend des systèmes nationaux de justice et de police. Des investigations sur un cybercrime, dont les traces, les effets, les acteurs, peuvent être localisés dans différents pays, nécessitent une coopération internationale très performante. Ce qui pose de nombreux problèmes législatifs, juridiques et procéduraux mais aussi d'organisation, de réactivité et d'efficacité de la justice.

Le droit pénal international est défini comme « *la branche du droit qui règle l'ensemble des problèmes pénaux qui se posent au plan international*[786] ». Cette branche du droit permet ainsi de déterminer lorsque les tribunaux répressifs français compétents ont compétence pour juger les infractions commises dans un autre Etat. Ce problème se pose toutes les fois où une infraction présente un caractère d'extranéité c'est-à-dire un élément qui fait que l'infraction est en lien avec un ordre juridique étranger, on parle alors d'infraction transfrontalière. Tel est le cas lorsque l'auteur ou la victime de l'infraction est de nationalité étrangère, ou lorsque l'infraction est commise sur différents Etats. Ces infractions se sont multipliées du fait de l'essor des réseaux de communication et des échanges commerciaux entre Etats. De nombreux trafics liés au terrorisme, à la drogue ou aux enfants ont profité de ce développement d'Internet et du Darknet pour minimiser les chances d'arrestation. Le problème se pose également

[786] Cours disponible à cette adresse : http://www.cours-de-droit.net/cours-de-droit-penal-international-c27647244.

lorsqu'une norme supranationale prime sur une norme nationale conformément à l'article 55 de la Constitution. Dès lors, le droit pénal est international par son objet, si l'infraction présente un caractère d'extranéité, ou par sa source, s'il existe une norme supranationale.

Précurseur en la matière le Conseil d'Etat estime en 1997 que *« ce qui est nouveau, c'est d'une part, la plus grande facilité avec laquelle ces infractions peuvent être commises et diffusées dans le monde du fait de la structure du réseau et de son mode de fonctionnement et, d'autre part, les difficultés rencontrées dans l'application des textes du fait de la fugacité extrême des contenus et de la dimension internationale d'Internet. L'objectif est donc de proposer des solutions concrètes pour que la règle de droit soit respectée, et que l'espace nouveau d'expression humaine que constitue Internet et les réseaux ne soit pas symbole de transgression facile et non sanctionnée. Il importe dès lors de préciser le champ d'application de la loi pénale et civile et la compétence du juge français, de clarifier les responsabilités des acteurs et d'accroître l'efficacité de l'intervention de la police et du juge. Cependant, la lutte contre l'illégalité sur Internet ne saurait se résumer à une action répressive : ce monde est trop décentralisé, trop international pour que la réponse législative ou réglementaire de sanction a posteriori soit la seule ; il convient de la combiner avec l'autorégulation des acteurs, c'est-à-dire la participation active et préventive de ceux-ci au respect de l'État de droit sur les réseaux*[787] ».

Pour le Conseil d'Etat « *il paraît donc très largement préférable de s'en tenir à la solution vers laquelle s'oriente la jurisprudence actuellement, c'est-à-dire la loi et le tribunal du (ou des) pays de réception, pour la part du préjudice subi dans chacun d'entre eux. La victime conserve naturellement la faculté, si elle a une chance de succès, de saisir également le tribunal du lieu d'émission. Il est toutefois important d'essayer de remédier aux inconvénients de cette solution qui ont été décrits plus haut, en facilitant l'exequatur, et en évitant d'obliger la victime à multiplier les procédures dans les différents pays de réception. Il faudrait ainsi donner au titulaire de droits lésé la faculté de saisir un tribunal, autre que celui du lieu d'émission, qui serait reconnu compétent pour réparer l'intégralité du préjudice subi au plan mondial. Ce tribunal devrait être celui qui présente le lien le plus étroit avec le préjudice. On pourrait*

[787] THERY J-F et FALQUE PIERROTIN I., *Internet et les réseaux numériques*, collection Etudes du Conseil d'Etat, 1998, page 116. Disponible à cette adresse : http://www.ladocumentationfrancaise.fr/rapports-publics/984001519/index.shtml, [consulté le 14 février 2016].

présumer qu'il s'agit de celui dans lequel la victime a sa résidence habituelle (s'il s'agit d'une personne physique) ou son principal établissement (s'il s'agit d'une personne morale). Il ne s'agirait que d'une présomption simple, qui pourrait s'effacer si les circonstances particulières de l'affaire ou le choix des parties désignaient un autre tribunal comme étant celui qui présente le lien le plus étroit avec le préjudice (par exemple si l'essentiel du préjudice était subi dans un seul pays)[788] ».

« *Avec un revenu net théorique de plus de 1000 milliards de dollars par an, les différentes activités criminelles sont un des secteurs les plus lucratifs de l'économie mondiale. Si le chiffre est forcément basé sur une approximation, ce montant qui dépasse, et de loin, le budget de fonctionnement de la plupart des États, permet aux groupes qui contrôlent ces fonds de s'acheter toutes les complicités et de gangrener des sociétés entières. Les activités criminelles semblent avoir accompagné l'histoire des sociétés humaines. Liées aux différences sociales, à la pression fiscale, et à la recherche d'un profit quelconque ces actions intègrent les actions violentes contre les personnes, simples particuliers ou représentants de l'autorité, des atteintes aux biens, qu'ils soient individuels ou collectifs, matériels ou immatériels. Dès la création des États, les groupes criminels organisés d'une certaine envergure ont vite su tirer parti des limites des frontières, des différences de législation ou de règlementation, d'autant plus aisément que les frontières intérieures restaient fortes*[789] ».

Internet a accentué cette exploitation des frontières en multipliant les infractions transfrontalières, avec des atteintes aux biens informatiques mais aussi avec des infractions classiques qui existaient bien avant son apparition. Avec Internet et la mondialisation, les règles classiques du droit pénal relatives à la territorialité ont été bouleversées et la souveraineté des Etats mise à mal.

En France, lorsqu'une infraction présente un élément d'extranéité, quatre systèmes sont envisageables pour donner compétence aux juges pour les infractions commises sur le territoire

[788] THERY J-F et FALQUE PIERROTIN I., *Internet et les réseaux numériques*, collection Etudes du Conseil d'Etat, 1998, page 102. Disponible à cette adresse : http://www.ladocumentationfrancaise.fr/rapports-publics/984001519/index.shtml, [consulté le 14 février 2016].
[789] MODICA B., *Mondialisation et criminalité*, Présentation du n°40 de la revue Questions internationales, décembre 2009. Disponible à cette adresse : https://www.diploweb.com/Mondialisation-et-criminalite.html, [consulté le 15 avril 2015].

et en dehors. Dans certains cas, ils auront la possibilité d'instruire et juger une affaire alors même que les investigations étaient transfrontalières. Mais dans quelles mesures sont-ils compétents pour se prononcer sur une affaire transnationale en lien avec Internet ou le Darknet.

Une internationalisation des systèmes juridiques a été nécessaire mais le droit pénal ne dispose toujours pas des moyens efficaces à la lutte contre les infractions à l'aspect international. Malgré les tentatives de collaboration entre Etats, le droit pénal international relève de la compétence de chaque État qui est souverain sur son propre territoire. Dès lors, les règles classiques d'applicabilité de la loi pénale s'applique en matière de cybercriminalité. Tel est le cas en France lorsqu'une infraction cybercriminelle est opérée sur le territoire de la République française (§1). Toutefois, une difficulté surgit lorsque l'infraction est commise sur le web dissimulé mais à partir d'un pays étranger ; ce sont les enjeux de l'application de la loi pénale dans l'espace à l'endroit de la cybercriminalité dissimulée. En effet, un Etat et un législateur ne sont souverain et légitime que sur leur propre territoire, puisqu'ils peuvent intervenir pour une infraction commise à l'étranger (§2).

§1) Les infractions commises en France

« *Le cyberespace étend et modifie les frontières temporelles et géographiques. Cela bouleverse nos habitudes, impose de nouveaux modes de fonctionnement et de nouvelles valeurs de société, tout en créant des changements sans précédent et en instaurant un nouvel ordre numérique. L'ampleur des bouleversements induits par l'urbanisation numérique relève de la révolution informationnelle. La dématérialisation des transactions et des services autorise des formes d'organisation d'échanges et d'activités économiques innovantes*[790] ». Ce paragraphe a encore plus d'impact avec le Darknet et montre à quel point les règles régissant la territorialité sont importantes.

En France, lorsqu'une infraction présente un élément d'extranéité, quatre systèmes sont envisageables pour donner compétence aux juges pour les infractions commises sur le territoire et en dehors. Dans certains cas, ils auront la possibilité d'instruire et juger une affaire alors même que les investigations étaient transfrontalières. Mais dans quelles mesures sont-ils

[790] GHERNAOUTI-HÉLIE S., *La cybercriminalité, le visible et l'invisible*, presses polytechniques et universitaires romandes, page 13.

compétents pour se prononcer sur une affaire transnationale en lien avec Internet ou le Darknet.

Logiquement, c'est la territorialité qui prime pour la répression en France. Si une infraction est commise en France, c'est l'ordre public français qui est perturbé, et c'est la loi française qui aura vocation à s'appliquer pour que les juges français puissent réparer cette perturbation. Il suffit alors qu'un élément constitutif de l'infraction ait eu lieu sur le territoire français.

Plus précisément, lorsqu'une infraction est commise sur le territoire français par un individu de nationalité française et à l'encontre d'une victime de nationalité française, c'est nécessairement la loi française et les tribunaux français qui sont compétents. En effet, contrairement au droit international privé[791], le système répressif français est gouverné par un principe de solidarité des compétences législatives et juridictionnelles[792] qui prévoit que si la loi française est applicable alors ce sont les juridictions françaises qui seront compétentes et inversement. En effet, il résulte de l'article 689 du Code de procédure pénale que l'auteur et le complice d'une infraction commise à l'étranger peuvent être poursuivis en France et jugés par une juridiction française si, conformément aux dispositions du code pénal, la loi pénale française s'applique ou si une convention internationale donne compétence à la juridiction française. C'est le trouble causé à l'ordre public qui justifie l'application de la loi pénale française[793]. Les magistrats français n'appliquent que la loi pénale française si bien qu'ils ne sont compétents que s'il y a violation de celle-ci. Mais parfois, cette violation peut aller au delà du principe de territorialité qui est envisagé de manière très large (A) afin qu'un plus grand nombre d'infractions soit rattaché au territoire de la République (B).

A) La notion de territoire de la République

Tout d'abord le champ d'application de la loi française est déterminé par le principe de territorialité qui préconise une application de la loi pénale française lorsqu'une infraction est commise sur le territoire de la République nonobstant la nationalité de l'auteur de l'infraction

[791] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 150.
[792] DONNEDIEU DE VABRES H., *Les principes modernes du droit pénal international, LGDJ, 2004*.
[793] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 33 : « *Le dogme de la territorialité est le fer de lance de la répression en France. Dès lors qu'une infraction a été commise sur notre sol, notre ordre public est troublé et les juridictions pénales françaises se doivent de réparer ce trouble* ».

et de la victime. En effet, l'alinéa premier de l'article 3 du Code civil dispose que « *les lois de police et de sûreté obligent tous ceux qui habitent le territoire* » et l'article 113-2 du Code pénal dispose que « *la loi pénale française est applicable aux infractions commises sur le territoire de la République* ». Ce principe est justifié par le principe de souveraineté Etatique qui permet à chaque pays de maintenir l'ordre à l'intérieur de ses frontières en jouissant des pouvoirs régaliens. Il permet donc une application large de la loi pénale française à tous les individus ayant commise une infraction sur le territoire de la République peu importe leur nationalité.

Au delà des limites définies par les frontières, il existe des territoires où la loi pénale française a vocation à s'appliquer. En effet, e territoire de la République correspond à l'espace « *où s'exerce la souveraineté de l'Etat* »[794]. Conformément aux articles 113-1 à 113-4 du Code pénal il comprend le territoire terrestre, les espaces maritimes et aériens, ainsi que les territoires assimilés tels que les navires battant pavillon français ou les aéronefs immatriculés en France.

Le territoire terrestre correspond à la France métropolitaine, aux DOM-ROM, aux COM,[795] mais aussi aux ambassades comme le prévoit l'article 113-10 du Code pénal in fine : « *les locaux diplomatiques ou consulaires français* ». Quant à l'espace maritime il comprend la mer territoriale française s'étendant sur une bande imaginaire de douze mille marins[796] à partir de la côte terrestre. Au delà, la loi française n'est applicable que si « *les conventions internationales et la loi le prévoient* »[797]. Enfin l'espace aérien, comprend toute la zone qui recouvre le territoire terrestre et l'espace aérien. Par conséquent, toute infraction commise dans ces espaces à bord ou à l'encontre d'un navire ou d'un aéronef, même étranger, sera poursuivie devant les juridictions françaises. Par ailleurs, la souveraineté de la République française s'exerce pour une infraction commise hors de l'espace aérien française, et à bord d'un aéronef étranger dans les hypothèses prévues à l'articles 113-11 du Code pénal : « *1°) lorsque l'auteur ou la victime de l'infraction est de nationalité française ; 2° lorsque l'appareil atterrit en France, après commission de l'infraction hors de l'espace aérien français ; 3°) lorsque l'aéronef a été donné en location, sans équipage, à une personne physique ou morale ayant son établissement principal en France* ».

[794] Cour de cassation, chambre criminelle, 28 février 1884, Bulletin criminel n°52.
[795] Depuis la loi constitutionnelle du 28 mars 2003 relative à l'organisation décentralisée de la République, ce sont les départements et régions d'outre-mer et les collectivités d'outre-mer.
[796] Soit 22,25 kilomètres.
[797] Code pénal Art. 113-12 in fine.

Internet et le Darknet permettent à des individus mal intentionnés de commettre des infractions à distance sans que leur présence physique ne soit nécessaire. Des pirates informatiques pourraient alors s'attaquer à un navire ou à un aéronef battant pavillon français sans être sur le territoire français. Conformément à l'article 113-3 du Code pénal, si cette hypothèse se présente, c'est la loi française qui a vocation à s'appliquer peu importe l'endroit du navire ou de l'aéronef et même si la loi étrangère n'incrimine pas les faits. L'article 113-3 du Code pénal dispose en effet que « *la loi pénale française est applicable aux infractions commises à bord des navires battant un pavillon français, ou à l'encontre de tels navires ou des personnes se trouvant à bord, en quelque lieu qu'ils se trouvent. Elle est seule applicable aux infractions commises à bord des navires de la marine nationale, ou à l'encontre de tels navires ou des personnes se trouvant à bord, en quelque lieu qu'ils se trouvent* ».

Cette compétence des juridictions françaises est exclusive d'une éventuelle décision étrangère en raison du principe « *non bis in idem*[798] ». En effet, selon ce principe, un même fait ne peut donner lieu, contre la même personne, à deux actions pénales distinctes. Une personne peut dès lors invoquer l'exception de chose jugée et le principe de l'autorité de la chose jugée au criminel sur le criminel. Lorsque la décision a été prononcée par une juridiction étrangère, l'autorité de la chose jugée n'a d'effet que si les faits sont commis en dehors du territoire de la République française[799]. Encore faut-il que la personne poursuivie devant les juridictions françaises puisse justifier avoir été définitivement jugé à l'étranger pour les mêmes faits, ce qui n'est pas le cas lorsque la décision invoquée par le prévenu comme obstacle aux poursuites est une décision de classement sans suite puisque l'action publique n'a alors pas été engagée[800]. Cependant, la Cour de cassation estime que l'exception de chose jugée ne saurait faire obstacle à l'exercice des poursuites exercées sur le fondement de la compétence territoriale française[801] lorsqu'un critère de rattachement justifie les poursuites (B).

B) Les critères de rattachement au territoire de la République

[798] Il s'agit d'une locution latine désignant le principe juridique selon lequel un individu ne peut pas être jugé et poursuivi deux fois pour les mêmes faits.
[799] Cour de cassation, chambre criminelle, 3 décembre 1998, Bulletin criminel n°331.
[800] Cour de cassation, chambre criminelle, 12 mai 2009, Bulletin criminel n°89 ; Cour de cassation, chambre criminelle, 20 juin 2012, Bulletin criminelle n°156.
[801] Cour de cassation, chambre criminelle, 8 juin 2005, Bulletin criminel n°174 ; Cour de cassation, chambre criminelle, 26 septembre 2007, Bulletin criminel n°224.

« *Sauf si la personne poursuivie bénéficie d'une immunité de juridiction, les tribunaux répressifs français sont compétents pour connaître de toute infraction commise sur le territoire français, quelle que soit la nationalité de son auteur ou de sa victime*[802] ». Dans cette affaire, le consul général de Turquie est poursuivi en France pour le délit de « *négationnisme sur Internet* » à l'égard du génocide arménien. Relaxé en première instance, le jugement est confirmé par la Cour d'appel de Paris puisque « *l'intéressé n'a pas agi à titre personnel, mais en sa qualité de consul général de Turquie (qui) n'a fait que diffuser la position officielle du gouvernement turc sur la question du génocide arménien*[803] ».

Pour que la répression de la cybercriminalité ou de la cyberdélinquance soit envisagée en France, il faut obligatoirement que l'infraction soit rattachée à la loi française « *l'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire* »[804] de sorte que le fait que l'activité délictueuse se soit partiellement déroulée en France, suffise à ce que les juridictions françaises soient compétentes (1). En outre, les juridictions françaises sont compétentes en ce qui concerne les actes de complicités (2).

1. La conception extensive d'élément constitutif de l'infraction

S'agissant des infractions commises par le biais d'internet ou du Darknet, les juridictions françaises se reconnaissent facilement compétentes sur le fondement de la territorialité[805], mais il y a eu quelques exceptions comme le prouvent deux arrêts du 8 décembre 2009.[806] Pour ces infractions, la difficulté réside dans le fait qu'il faille prendre en compte les aspects transnationaux et virtuels de ces réseaux.

Par exemple, un site internet hébergé aux Etats-Unis propose un lien vers un site de vente

[802] Cour d'Appel de Paris, 8 nov. 2006.
Disponible à cette adresse : http://www.collectifvan.org/article.php?r=4&id=5457.
[803] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 156.
[804] Code pénal Art. 113-2 al. 2.
[805] TGI Paris, 13 novembre 1998 : Gaz. Pal. 2000. 1. Doctrine 697, observation MANSEUR-RIVET : « *en application de l'art. 113-2, al. 2, C. pén., le fait de diffuser sur internet, depuis un site étranger, des propos révisionnistes constitue un délit relevant de la compétence des tribunaux français* ».
[806] « Le lieu de commission de l'infraction est celui où les menaces ont été proférées et non pas les pays où elles ont ensuite été rapportées par la voie télévisée ou de presse écrite ou électronique et par lesquelles l'intéressé a pu en prendre connaissance »

d'objets nazis. La publicité de ce site ayant été faite en France, le délit d'apologie de crime de guerre y a été réalisé, ce qui donne compétence au juge pénal français[807]. Théoriquement, les « *faits constitutifs de l'infraction* » font directement référence à la notion d'éléments constitutifs de l'infraction et donc à tout élément matériel ou intentionnel commis sur le territoire français. L'escroquerie qui suppose l'accomplissement de plusieurs actes matériels, sera poursuivie en France si l'un de ces actes y a été accompli[808]. Cependant, la jurisprudence française a une conception extensive de cette notion de faits constitutifs. Ainsi, la Cour de cassation étend la compétence des juridictions françaises aux actes préparatoires[809] et aux conditions préalables lorsqu'ils se sont réalisés en France et forment un « *tout indivisible* » avec l'infraction[810]. Sur le Darknet, l'application de la loi pénale n'est pas chose simple.

Avant que soit prise en compte la théorie de l'ubiquité, plusieurs théories se sont opposées[811]. La première est la théorie de l'action selon laquelle la loi pénale d'un pays s'appliquait lorsque l'infraction été commise sur le territoire de ce pays via Internet. A titre d'exemple, si un individu commettait une escroquerie au moyen d'Internet en étant en Chine, avec une victime au Japon, c'est la loi chinoise qui avait vocation à s'appliquer. La seconde est la théorie du résultat selon laquelle la compétence des tribunaux et des lois est donnée au pays sur le territoire duquel les effets de l'infraction se sont produits. Par cette théorie, pour l'exemple relatif à l'escroquerie, c'est la loi japonaise qui aurait eu vocation à s'appliquer[812]. Le mélange de ces deux théories a donné naissance à la théorie de l'ubiquité qui rend compétent les tribunaux des Etats où l'infraction s'est réalisée et où le résultat s'est produit. La seule condition est que l'élément matériel de l'infraction se soit accompli sur le territoire de l'Etat.

En France, c'est ainsi que la jurisprudence[813] effectue ce que la doctrine nomme, une extension

[807] Paris, 17 mars 2004, Juris-Data n° 2004-252 592.
[808] Cour de cassation, chambre criminelle, 28 novembre 1996 : Bulletin criminel n°437.
[809] Cour de cassation, chambre criminelle, 11 avr. 1988 : Bulletin criminel n° 144.
[810] Cour de cassation, chambre criminelle, 13 octobre 1981 : Bulletin criminel n° 271 : « *encourt la cassation l'arrêt qui, pour déclarer l'incompétence de la juridiction d'instruction saisie, ne s'explique pas sur la question de savoir si un acte caractérisant un des éléments constitutifs de l'infraction poursuivie, compte tenu des données de la procédure, n'a pas été accompli en France, auquel cas l'infraction doit être réputée commise en France* ».
[811] HUET A., KOERING-JOLIN R., *Compétence des tribunaux répressifs français et de la loi pénale française*, fascicule 30, 11 mars 2013, page 20.
[812] Cette même théorie a été utilisée pour l'extradition vers les Etats-Unis du trafiquant de drogue mexicain Joaquín Guzman Loera dit « *El Chapo* ». Les effets de la drogue qu'il fabriquait en Colombie se produisaient aux Etats-Unis.
[813] Voir l'affaire Yahoo, TGI de Paris, 17ème chambre, 26 février 2002.

par indivisibilité de la territorialité[814]. Elle applique donc la théorie de l'ubiquité.

« On sait qu'en France, comme ailleurs à l'étranger, la tendance jurisprudentielle dominante va dans le sens d'une extension de ce critère de compétence territoriale, au point que ses excès et son caractère impérialiste sont fréquemment dénoncés[815] ». Ce système peut entrainer un conflit de lois entre plusieurs Etats qui souhaiteraient poursuivre les mêmes faits. Dès lors, un individu risquerait d'être jugé et sanctionné deux fois pour une même infraction. En matière de cybercriminalité cette possibilité est très fréquente.

Par exemple, quels sont les pays compétents pour poursuivre un individu ayant vendu de la drogue sur le Darknet à des individus se trouvant partout dans le monde et alors même que son propre pays ne punit pas ces faits ? Normalement le principe « *non bis in idem* » empêche la double poursuite d'une personne pour les mêmes faits. Pourtant, les éléments d'extranéité d'une infraction commise sur Internet, vont permettre à plusieurs Etats de se déclarer compétents pour la poursuite de cette infraction. Et dans certains cas, les Etats ne prendront pas en compte la chose jugée par un autre Etat[816] si bien qu'il y aura une double poursuite. Par ailleurs, le Code pénal prévoit également la répression des actes de complicité (2).

2. La localisation des actes de complicité

Concernant la localisation des actes de complicité, l'article 113-5 du Code pénal, prévoit que « *la loi pénale française est applicable à quiconque s'est rendu coupable sur le territoire de la République, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi française et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère* ».

Ainsi, deux situations sont possibles. Soit l'acte de complicité accompli à l'étranger se rattache

[814] Cour de cassation, chambre criminelle, 23 avril 1981 : Bulletin criminel n°116 : « *la juridiction française est compétente pour connaître des faits commis à l'étranger par un étranger dès lors que ces faits apparaissent comme formant un tout indivisible avec les infractions également imputées en France à cet étranger et dont elle est légalement saisie* ».
[815] FRANCILLON J., *Le droit pénal face à la cyberdélinquance et à la cybercriminalité*, Revue Lamy droit de l'immatériel (n°81), 2012, page 143.
[816] BRACH-THIEL D., *Conflits positifs et conflits négatifs en droit pénal international*, Université de Lorraine, 2000, page 128.

à un acte principal commis en France, et dans ce cas la complicité sera localisée de manière fictive là où a été commise l'infraction principale de sorte que les juridictions pénales françaises seront compétentes : c'est la théorie de l'emprunt de criminalité. Soit, à l'inverse, l'acte de complicité a été commis sur le territoire français et l'infraction principale à l'étranger et dans cette hypothèse, la théorie de l'emprunt de criminalité devrait écarter la compétence des juridictions françaises. Néanmoins, cette solution poserait problème dans le cas où le complice serait de nationalité française dans la mesure où la France refuse généralement d'extrader ses nationaux[817]. C'est ainsi que l'article 113-5 du Code pénal trouve application lorsque deux conditions sont formellement établies par le juge: 1°) que « *le crime ou le délit (soit) puni à la fois par la loi française et par la loi étrangè*re », et 2°) qu' « *il (ait) été constaté par une décision définitive de la juridiction étrangère* »[818].

Cet article ne trouve à s'appliquer que « *lorsque l'auteur du fait principal ne peut être jugé par les juridictions françaises ; tel n'est pas le cas lorsqu'un Français s'est, en France, rendu complice d'un crime commis à l'étranger par un Français* »[819] (§2).

§2) Les cyber-infractions commises à l'étranger

L'ensemble de la matière pénale est concerné par la cybercriminalité dissimulée qui est un réel défi pour les Etats confrontés à ce phénomène transversal. Compte tenu de la nature immatérielle et virtuelle des échanges de données, le lieu de commission de l'infraction n'est pas nécessairement celui du territoire Etatique où se dégagent les conséquences. Les nombreux réseaux Darknet ont permis une multiplication des infractions un peu partout dans le monde et surtout dans les pays où la législation est plus accommandante. Cette universalité des réseaux numériques, leur instantanéité, associées aux nombreuses règles de compétences ont créé un modèle juridique approximatif. Dans les autres pays, les cyberdélinquants et cybercriminels profitent des difficultés liées à territorialité et n'hésitent pas à transgresser les règles souverainement établies par les Etats : « *le caractère international des infractions en question- par exemple celles commises au moyen de l'Internet – se heurte à la territorialité des*

[817] THOUVENIN J-M., *Le principe de non extradition des nationaux*, Extrait de l'ouvrage Droit international et nationalité, Colloque SFDI de Poitiers, 2012, page 3. Disponible à cette adresse : http://pedone.info/sfdi/Poitiers/647-8-Thouvenin.pdf, [consulté le 2 janvier 2015].
[818] Cour de cassation, chambre criminelle, 10 février 1999, Bulletin criminel n°15.
[819] Cour de cassation, 20 février 1990 : Bulletin criminel n°84, note Fournier.

institutions nationales de répression[820] ».

Dans quelles mesures va-t-on étendre ce principe de territorialité ? Dès lors qu'il y aura un fait constitutif comportant un élément d'extranéité qui peut être en rapport avec le lieu de commission de l'infraction, avec la nationalité de l'auteur ou avec la nationalité de la victime. La seule application du principe de territorialité supposerait la compétence exclusive des juridictions répressives étrangères en cas d'infractions commises à l'étranger. Néanmoins, certains délinquants français pourraient échapper à la répression en venant se réfugier sur le territoire français qui n'extrade quasiment pas ses ressortissants. Dès lors, le droit français a adopté plusieurs systèmes permettant d'envisager l'application de la loi pénale française pour des faits commis en dehors du territoire de la République. Il y a un système basé sur la nationalité de la victime ou de l'auteur de l'infraction (A) et des systèmes particuliers (B).

A) Les compétences fondées sur la nationalité

Le système de la compétence personnelle est fondé soit, sur la nationalité de la victime, c'est la personnalité passive (1), soit sur celle de l'auteur de l'infraction c'est la personnalité active (2), quel que soit le territoire où ceux-ci se trouvent. En ce sens, l'article 683 du Code de procédure pénale dispose que « *la juridiction compétente est celle du lieu où réside le prévenu, celle de sa dernière résidence connue, celle du lieu où il est trouvé, celle de la résidence de la victime ou, si l'infraction a été commise à bord ou à l'encontre d'un aéronef, celle du lieu d'atterrissage de celui-ci. Ces dispositions ne sont pas exclusives de l'application éventuelle des règles particulières de compétence prévues par les articles 697-3, 705 et 706-17* ».

1. La personnalité passive

Le système de la personnalité passive, prévu à l'article 113-7 du Code pénal, permet quant à lui de donner compétence aux juridictions pénales françaises pour les infractions commises contre des victimes françaises à l'étranger. Ainsi, « *la loi pénale française est applicable à tout crime, ainsi qu'à tout délit puni d'emprisonnement, commis par un Français, ou par un étranger hors du territoire de la République lorsque la victime est de nationalité française au moment de*

[820] Fouchard I., *Crimes internationaux : Entre internationalisation du droit pénal et pénalisation du droit international, Emile Bruylant,* 2014, page 345.

l'infraction ». La lecture de l'article montre que contrairement à la personnalité active (2), il n'y a aucune exigence de réciprocité[821], réduisant alors la valeur du principe de légalité des délits et des peines et la souveraineté des autres Etats.

2. La personnalité active

Le système de la personnalité active, prévu à l'article 113-6 du Code pénal, permet aux juridictions pénales françaises d'être compétentes pour les infractions commises par un Français à l'étranger sur des victimes étrangères. Ce système donne compétence à la France pour tous les crimes « *commis par un Français hors du territoire de la République* » et pour tous les délits « *commis par des Français hors du territoire de la République si les faits sont punis par la législation du pays où ils ont été commis* » et ce, même si la qualification donnée par la loi étrangère est différente de celle du droit français et même si les peines ne sont pas les mêmes.

Toutefois, pour certains délits, cette exigence de réciprocité d'incrimination n'est pas nécessaire. C'est le cas « *à bord ou à l'encontre des aéronefs non immatriculés en France* » mais « *lorsque l'auteur ou la victime est de nationalité française* »[822]. Il en va ainsi aussi pour les agressions et atteintes sexuelles sur mineurs[823], pour le délit de recours à la prostitution d'un mineur[824] et pour le délit de proxénétisme à l'égard d'un mineur[825].

Par ailleurs, le système de la compétence personnelle, active ou passive, est soumis à deux règles procédurales prévues aux articles 113-8 et 113-9 du Code pénal. D'une part « *la poursuite des délits ne peut être exercée qu'à la requête du ministère public* » à la suite d'une plainte de la victime[826] ou « *d'une dénonciation officielle par l'autorité du pays où le fait a été commis* ». La plainte de la victime peut être déposée en France ou à l'étranger si elle par la suite

[821] Cour de cassation, chambre criminelle, 21 janvier 2009, bulletin criminel n°22 : « *Seule la qualité de victime directe de l'infraction attribue compétence à la juridiction française* ».
[822] Code pénal Art. 113-11, 1°.
[823] Code pénal Art. 222-22 et 227-27-1.
[824] Code pénal Art. 225-12-3.
[825] La loi n°2006-399 du 4 avril 2006 a écarté l'exigence de réciprocité pour ce délit prévu à l'article 225-7 du Code pénal, lorsque les faits sont commis à l'étranger par un Français ou un résidant habituellement sur le territoire français : Code pénal art. 225-11-2.
[826] La plainte de la victime ne suffit pas à mettre en mouvement l'action publique : Cour de cassation, chambre criminelle, 11 juin 2003, Bulletin criminel n°119.

transmise aux autorités judiciaires françaises[827]. Néanmoins, certains délits comme les délits sexuels ou les violences sur mineurs échappent à cette condition. D'autre part, « *aucune poursuite ne peut être exercée contre une personne justifiant qu'elle a été jugée définitivement à l'étranger pour les mêmes faits et, en cas de condamnation, que la peine a été subie et prescrite* », c'est l'application de la règle *non bis in idem*. Cependant, cette règle ne trouve à s'appliquer que lorsque la compétence des juridictions françaises est due à une compétence subsidiaire c'est-à-dire personnelle ou universelle. Ainsi, cette règle ne s'applique pas lorsque la compétence des juridictions françaises est établie à titre principal c'est-à-dire territoriale ou réelle. Par conséquence, pour la compétence réelle, le juge pénal français sera compétent même si l'individu a fait l'objet d'un jugement à l'étranger[828] (B).

B) Les systèmes de compétences particuliers

En vertu de certains systèmes, c'est le tribunal du lieu d'arrestation qui est compétent, sans égard pour le lieu de commission de l'infraction et la nationalité des protagonistes. Tel est le cas pour les systèmes de compétences universelle et réelle (1). En outre, il semble nécessaire de prendre en compte Internet et Darknet comme des lieux singuliers supposant la création d'un système de compétence adéquat (2).

1. Les compétences universelle et réelle

En France, le système de la compétence universelle est prévu par l'article 689-1 et suivants du Code de procédure pénale qui dispose qu'en « *application des conventions internationales visées aux articles suivants, peut être poursuivie et jugée par les juridictions françaises, si elle se trouve en France, toute personne qui s'est rendue coupable hors du territoire de la République de l'une des infractions énumérées par ces articles. Les dispositions du présent article sont applicables à la tentative de ces infractions, chaque fois que celle-ci est punissable* ».

La compétence universelle suppose la présence en France des personnes soupçonnées des infractions. Celle des victimes d'infractions ne suffit pas à la mise en mouvement de l'action

[827] Cour de cassation, 24 novembre 1998, Bulletin criminel n°312.
[828] Cour de cassation, 26 septembre 2007, Bulletin criminel n°224.

publique[829]. La plupart des conventions vise le terrorisme international, mais aussi les crimes contre l'humanité, les génocides ou encore les crimes ou délits de guerres. A titre d'exemple, le Sénat a adopté une proposition de loi visant à modifier l'article 689-11 du Code de procédure pénal afin d'étendre la compétence des juridictions françaises. Ainsi, ces dernières sont compétentes pour juger toute personne se trouvant en France et soupçonnée d'avoir commis un crime contre l'humanité, un génocide ou un crime ou délit de guerre. Le texte a été transmis à l'assemblée nationale le 26 février 2013[830].

Par ailleurs, il existe des hypothèses dans lesquelles les intérêts de la Nation ont été violés, et dans ce cas la loi française sera toujours compétente comme le prévoit l'article 113-10 du Code pénal pour les atteintes aux intérêts fondamentaux de la nation comme la fabrication de fausse monnaie française par exemple.

En outre, la loi dite Perben II du 9 mars 2004 prévoit que la loi française « *s'applique au crime ou délit puni d'au moins 5 ans commis à l'étranger par un étranger dont l'extradition a été refusée par la France soit parce que le fait à raison duquel l'extradition avait été demandée est puni d'une peine ou d'une mesure de sûreté contraire à l'ordre public français, soit parce que la personne réclamée aurait été jugée dans ledit Etat par un tribunal n'assurant pas les garanties fondamentales de procédure et de protection des droits de la défense, soit enfin parce que le fait considéré revêt le caractère d'infraction politique. Dans ce cas la poursuite a lieu à l'initiative du ministère public et doit être précédée d'une dénonciation officielle du pays ayant requis l'extradition*[831] ».

Ainsi, pour ces infractions, seuls les faits de l'infraction sont pris en considération, nonobstant la nationalité de l'auteur et le lieu de l'infraction. Le mélange de tous ces systèmes de compétence pourrait permettre de créer un système de compétence adapté aux réseaux Internet et Darknet (2).

2. La nécessité d'un principe approprié à Internet

[829] Cour de cassation, 26 mars 1996, Bulletin criminel n°132.
[830] ALLAIN V-E., *AJ pénal,* 2013, page 123.
[831] Code pénal Art. 113-9.

Sur Internet, les conséquences des critères relatifs aux compétences territoriales sont très importantes puisqu'elles empêchent le vide juridique que certains avaient envisagé en raison de l'opaque transmission d'information transfrontalière que permet le réseau. En effet, les règles de territorialité limitent les compétences des Etats afin qu'ils ne se déclarent pas tous compétents pour une même affaire. Cela permet d'assurer une meilleure sécurité juridique conformément au principe de légalité criminelle garantissant l'accessibilité et la prévisibilité pour tous de la loi pénale. En ce sens, il n'est pas possible d'envisager que tous les systèmes pénaux du monde puissent s'appliquer pour une même infraction commise sur Internet. En outre, une condamnation pénale étrangère n'est en principe pas exécutoire dans un autre pays en raison de l'absence d'exequatur[832] en droit pénal.

Dans chaque système judiciaire il y existe des lois pour les infractions liées à Internet mais qu'en est-il de leur efficience réelle ? Dans son ouvrage, « *Combattre la cybercriminalité* », Mohamed CHAWKI[833] met en avant les trois procédés utilisés par les Etats afin de faire face à cette inévitable internationalisation : 1) il est possible de promulguer « *des législations spécifiques concernant la cybercriminalité en ne tenant pas compte des incriminations déjà existantes qui auraient pu s'appliquer à certains types d'infractions* » ; 2) certains Etats ont « *procédé à l'analyse de leurs législations et de leurs lois pénales, les ont adaptées aux vues des nouvelles caractéristiques des méthodes de commission de l'infraction et ont établi de nouvelles incriminations pour encadrer ces infractions* » ; 3) d'autres Etats ont réprimé les différentes formes de cybercriminalité « *par des dispositions législatives déjà en vigueur, à savoir les dispositions sur l'accès non autorisé aux données et aux informations* ».

« *Utilisant des procédés nouveaux, les actes cybercriminels se manifestent sous des aspects inhabituels et méconnus qui pourraient impliquer, semble-t-il, la mise en échec de la protection du droit pénale* [834] ». L'aspect imprévisible, la perspective internationale et le caractère ambivalent du Darknet établit une difficulté quant à l'applicabilité de la loi pénale pour incriminer ce nouveau genre de criminalité.

[832] Il s'agit d'une procédure qui permette de rendre exécutoire dans un pays une décision de justice étrangère.
[833] CHAWKI M., *Op. cit.* p.260., page 117.
[834] JABBER A., *Les infractions commises sur Internet*, l'Harmattan, 2009, page 16.

En cas de litispendance internationale [835], la Convention de Budapest sollicite une « *concertation entre les parties revendiquantes* » sans obligations pour les Etats qui tenteront de trouver des critère de rattachement en matière pénale[836]. Pour le cas d'Internet, les juges français ont appliqué deux théories afin de fonder leur compétence. Il s'agit d'adapter la notion de territorialité à la portée universelle des réseaux Internet et Darknet. Une première théorie, celle de l'accessibilité au site a d'abord été envisagée. Cette conception large permettait au juge français d'être compétent dès lors que le site Internet était accessible en France. Finalement, la jurisprudence a opté pour la théorie de la focalisation[837] qui restreint le champ de compétence des juridictions françaises.

Les juges du fond ont d'abord opté pour le critère de l'accessibilité dans une affaire de négationnisme[838] commis par un étranger. Ce dernier a publié sur un site étranger des propos contestant un crime contre l'humanité alors que la loi loi n° 90-615 du 13 juillet 1990 tendant à réprimer tout acte raciste, antisémite ou xénophobe[839] condamne la publication de ce genre de propos. Le 13 novembre dans un jugement rendu en matière correctionnelle, le Tribunal de grande instance de Paris rejette les exceptions liées à l'incompétence territoriale du Tribunal et se déclare compétent en application de l'article 113-2 alinéa 2 du Code pénal[840]. Les juges du fond estiment que l'accessibilité du site sur le territoire français est assimilable à la publication qui est un des éléments constitutifs de l'infraction.

Une autre affaire va permette aux juges du fond d'aller dans le même sens, il s'agit de l'affaire dite « *Yahoo* » qui a confirmé cette approche universalité du contrôle des activités sur Internet[841]. Cette affaire est initiée[842] par des associations de lutte contre l'antisémitisme et le

[835] Il y a litispendance lorsque deux juridictions compétentes de même degré sont saisies pour connaître de l'affaire.
[836] BOOS R. La lutte contre la cybercriminalité au regard de l'action des États, Université de Lorraine, 2016, page 33.
[837] https://www.valhalla.fr/2006/06/24/tribunal-competent-et-cyber-delits-theorie-de-la-focalisation/.
[838] Décision disponible à cette adresse : https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-jugement-correctionnel-du-13-novembre-1998/.
[839] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000532990.
[840] « *L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire* ».
[841] BOOS R. *La lutte contre la cybercriminalité au regard de l'action des États*, Université de Lorraine, 2016, page 33.
[842] Il y a une affaire engagée au pénal conformément à aux règles procédurales de la procédure pénale et une affaire rendue au civil selon ses règles procédurales.

racisme[843] contre la société « *Yahoo Inc.* » et son Président qui sont accusés d'apologie de crimes de guerre contre l'humanité pour avoir permis la vente en ligne d'objets nazis[844]. Il est demandé à la société *Yahoo ! Inc*. « *de faire cesser toute mise à disposition sur le territoire français à partir de son site Yahoo.com de messages, d'images de textes se rapportant aux objets, reliques, insignes et emblèmes nazis ou évoquant le nazisme*[845] ». Le 22 mai 2000, le juge délégué par le premier Président ordonne à la société de rendre inaccessible le site de ventes aux enchères d'objets nazis[846]. Le 20 novembre 2000[847], le Président du Tribunal de grand instance de Paris confirme l'injonction contre la société et l'ordonne de « *prendre toutes les mesures de nature à dissuader et rendre impossible toute consultation sur yahoo.com du service de ventes aux enchère d'objets nazis et de tout autre site ou service qui constituent une apologie du nazisme ou une contestation des crimes nazis* ». Le simple fait que le site soit accessible en France permet la compétence des juridictions françaises : « *il n'en est pas de même des enchères d'objets représentant des symboles de l'idéologie nazie qui peuvent intéresser et sont accessibles à toute personne qui souhaite les suivre, y compris aux Français* ». La chambre criminelle de la Cour de cassation ira dans le même sens dans un arrêt du 15 janvier 2008[848]. Cette approche universaliste et l'absence d'exequatur en matière pénale[849] amènent à des problématiques quant à son application sur le territoire américain là où la liberté d'expression, garantie par le 1er Amendement de la Constitution.

De plus, le simple fait que la diffusion soit possible en France entraîne donc la compétence des juges français ce qui porte atteinte à la sécurité juridique. La majorité des sites web et du Darknet étant consultables en France, une telle conception pourrait donc être appliquée par d'autres pays provoquant une multiplication des conflits de lois. Les difficultés que posent cette approche ont entrainé une évolution de la jurisprudence qui a préféré opter pour une nouvelle

[843] Il y a l'Association Amicale des Déportés d'Auschwitz et des Camps de Haute Silésie et le Mouvement contre le Racisme et pour l'Amitié entre les Peuples. Ensuite, le Consistoire Israélite de France se constituera partie civile.
[844] Il s'agit de la vente de milliers d'objets et insignes à la gloire du 3ème Reich.
[845] Disponible sur https://juriscom.net/wp-content/documents/yahoo20050517.pdf.
[846] TGI de Paris, référé, 22 mai 2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France : Juriscom.net. Disponible à cette adresse : http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm, [consulté le 23 septembre 2015].
[847] TGI de Paris, référé, 20 novembre 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France*. Disponible à cette adresse : http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm.
[848] Cour de cassation, 15 janvier 2008, n°07-86.944., bulletin criminel n°5.
[849] L'injonction a été prononcée contre *Yahoo ! Inc.* qui est une société américaine et non contre Yahoo France.

conception.

La jurisprudence française applique désormais de nouveaux critères limitant la compétence territoriale des juges français. Ces derniers doivent désormais trouver « *un lien suffisant, substantiel ou significatif entre les faits alléguée et le territoire français*[850] ». S'en suit un arrêt du 9 septembre 2008[851] rendu par la chambre criminelle de la Cour de cassation qui ajoutera une condition pour qu'une infraction commise sur Internet depuis l'étranger soit rattachée au territoire français[852]. Désormais, les juges français ne seront compétents que si le contenu est destiné au public français. Cette évolution jurisprudentielle[853] sera confirmée par un arrêt du 14 décembre 2010[854] concernant la contrefaçon d'une chanson française par un site allemand. La Haute juridiction censure l'a Cour d'appel qui avait retenu la compétence des juges français : « *qu'en se déterminant par ces seuls motifs, les juges du fond n'ont pas suffisamment prouvé l'orientation du site vers la France* ». La langue française ne semble pas suffisante dans la mesure où elle est utilisée dans une cinquantaine de pays francophones. Aucune précision n'a été faite quant au critère permettant de rattaché un site étranger au territoire français ce qui laisse une forte marge d'appréciation aux juges du fond et ne facilite pas leur travail (section 2).

[850] Cour d'Appel Paris, *Zidane contre Unibet*, 14 février 2008.
[851] Cour de cassation, chambre criminelle, 9 septembre 2008, n°07-97.281. Disponible à cette adresse : https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000019570259&fastReqId=850465415&fastPos=1, [consulté le 7 janvier 2015].
[852] En l'espèce, un article est mis en ligne sur un site italien sans l'accord de l'auteur français qui poursuit le site pour contrefaçon en estimant que l'un des éléments constitutifs de l'infraction était constitué sur le territoire français. Les juges du fond se fondent sur le critère de l'accessibilité et estime que l'infraction a été commise sur le territoire français. La chambre criminelle censure cette décision en estimant que l'article n'était pas destiné au public français puisqu'il était accessible sur un site italien et en langue italienne.
[853] Il ne s'agit pas d'un revirement de jurisprudence dans la mesure où les arrêts de 2008 et 2O10 n'ont pas été publiés au bulletin. Leur portée est donc moindre.
[854] Cour de cassation, chambre criminelle, 14 décembre 2010, n°10-80.088.

SECTION 2
Des difficultés pour le juge

À l'instar d'Internet, le Darknet profite de la technologie de l'information pour assurer de manière transnational un échange infini de données sans égard pour les frontières. Dès lors, l'applicabilité de la loi pénale est fragilisée par ces nouveaux réseaux qui ont permis un accroissement de la cybercriminalité. La jurisprudence française a un temps puni les auteurs d'infractions commises sur des sites web accessibles en France, puis a ajouté une condition, celle de la volonté de viser le public français. En tout état de cause, le Darknet est un phénomène qui a vocation à modifier la position des juges répressifs.

Pour être garant des libertés individuelles et de la sécurité juridique le principe de légalité des délits et des peines contraint le législateur à définir de manière claire et intelligible les comportements prohibés et les peines qui y sont attachées afin d'éviter l'arbitraire du juge[855]. L'idée est que celui qui commet un acte doit avoir connaissance du caractère délictueux de son acte au moment de sa commission. Cette connaissance effective est garantie par une fiction de connaissance de la loi selon laquelle « *nul n'est censé ignorer la loi* ».

Dès lors, il est nécessaire que la loi soit claire, accessible et prévisible. Cette contrainte a valeur constitutionnel dans la mesure où elle est prévue à l'article 8 de la Déclaration des droits de l'homme de 1789. C'est d'ailleurs sur ce fondement que le Conseil constitutionnel a précisé la portée du principe de légalité dans sa décision Sécurité et Liberté de 1981: « *aux termes de l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789, nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit et légalement appliquée qu'il en résulte la nécessité pour le législateur de définir les infractions en termes suffisamment clairs et précis pour exclure l'arbitraire ». Ainsi, les dispositions législatives qui ne déterminent pas l'auteur de l'infraction de manière certaine ou qui prévoient des infractions avec des éléments constitutifs qui ne sont ni clairs ni précis, seront invalidées*[856].

[855] DEBOVE F., *L'overdose législative*, Droit pénal, LexisNexis, 2004.
[856] Conseil constitutionnel, décision n° 80-127 DC, 19 et 20 janvier 1981 et Conseil constitutionnel, décision n° 2010-604, 25 février 2010. De plus le Conseil constitutionnel a abrogé l'article 222-33 du Code pénal qui ne définissait pas suffisamment les éléments constitutifs du délit de harcèlement sexuel : Conseil constitutionnel, 4 mai 2012, décision n° 2012-240 QPC.

En outre, la Cour EDH contraint elle aussi le législateur à voter des lois suffisamment accessibles et précises afin que le citoyen sache quelles normes juridiques seront applicables à telles situations. Elle l'exige indirectement sur la base de son article 7 : « *Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou international. De même il n'est infligé aucune peine plus forte que celle qui était applicable au moment où l'infraction a été commise* ». Le principe de légalité a des conséquences pour les magistrats qui sont tenus d'appliquer strictement la loi (§1) afin de prononcer une peine adéquate (§2).

§1) L'application stricte de la loi

Les décisions de justice rendues en matière de cybercriminalité démontrent que les magistrats sont confrontés à de réelles difficultés dans la qualification des faits et dans la recherche d'une catégorie d'infraction existante. L'émergence de la cybercriminalité dissimulée n'a pas facilité les choses. Pourtant, il s'agit d'une étape essentielle. La qualification des faits retenue détermine l'infraction applicable et pour qu'elle soit pertinente, il est parfois nécessaire de se baser sur des principes juridiques classiques utilisées depuis des dizaines d'années, bien avant l'arrivée du numérique. Cependant, les concepts juridiques traditionnels peuvent être marginaux voire inappropriés dans certains cas révélés par les nouvelles technologies du numérique.

L'intervention du législateur a donc été fondamentale pour faire face à la multiplication des cyberattaques, à la menace de la cybercriminalité organisée et au fléau qu'est le terrorisme. L'arsenal juridique pénal sera t-il complété pour combattre la cybercriminalité dissimulée ? La question est pertinente et d'actualité mais il faut prendre en compte les conséquences négatives que pourrait engendrer ce type de modification ponctuelle du droit. En effet, ce phénomène d'adaptation a créé une dispersion des dispositions pénales dans différents codes tels que le Code pénal, le Code de la défense, le Code des postes et des communications électroniques, et un risque de désuétude des normes les moins utilisées par les professionnels du droit. Il semble donc opportun d'introduire de nouvelles perspectives d'aménagement du Code pénal en matière de cybercriminalités visible et invisible. L'objectif étant d'apporter une meilleure lecture des textes légaux pour les magistrats en harmonisant les termes ainsi que les définitions, et en supprimant les redondances inutiles.

En ce sens, un rapport présentant les travaux de associations Cyberlex[857] et CECyF[858] a été rendu public le 25 janvier 2017 lors du Forum international sur la cybersécurité. Les réflexions des auteurs du rapport tendent à à faciliter pour tous la lisibilité de la loi en matière de cybercriminalité. Pour ce faire, ils ont relevé les redondances de textes et proposé des modifications afin de faciliter le travail du législateur. De manière générale, une lutte efficace contre la cybercriminalité passerait par une restructuration complète des infractions relatives au phénomène et une modification des règles de procédure pénale. C'est ce qu'a démontré le délit de vol de données qui a nécessité l'intervention du législateur (A). Dans d'autres cas, le juge a la possibilité d'écarter une disposition (B).

A) L'exemple du vol de données

En pratique, le principe de légalité contraint le juge à s'assurer que le fait poursuivi constitue bien une infraction punissable. Pour cela il doit constater l'existence de tous les éléments constitutifs de l'infraction et s'assurer que la peine prononcée, principale ou complémentaire, soit prévue par un texte. Pour chaque infraction appréhendée à l'endroit de la cybercriminalité dissimulée, il faudra discerner parmi les éléments constitutifs de l'infraction, un élément matériel et un élément moral.

« *En matière criminelle, il faut des lois précises, point de jurisprudence* », cette formule proclamée par Portalis lorsqu'il présenta le code pénal de 1810 illustre parfaitement la méfiance de l'époque à l'encontre de l'autorité judiciaire. Ainsi, inspirés par les philosophes, les constituants révolutionnaires décident qu'il appartient aux juges d'appliquer la loi sans l'interpréter. L'article 111-4 du Code pénal dispose que « *la loi pénale est d'interprétation stricte* », ce principe est un corollaire du principe de légalité criminelle Pour le viol, la Cour de cassation précise que l'infraction suppose nécessairement une pénétration, ou une tentative de pénétration, sur la victime et interprète strictement l'article 222-23 du Code pénal[859]. Ainsi, lorsqu'il n'y a pas de pénétration sur la victime, elle condamne sur le terrain des agressions

[857] L'association du Droit et des Nouvelles technologies.
[858] Le Centre Expert contre la Cybercriminalité Français. Il a vocation à réunir les chercheurs de tout horizon afin de contribuer à la formation, à l'éducation et à la recherche contre la cybercriminalité.
[859] Cour de cassation, chambre criminelle, 21 oct. 1998 : Bulletin criminel n°274 ; Cour de cassation, chambre criminelle, 22 août 2001 : Bulletin criminel n° 169.

sexuelles. Mais c'est surtout en matière d'atteinte involontaire au fœtus que l'Assemblée plénière de la Cour de cassation a fait une application rigoureuse du principe d'interprétation stricte de la loi pénale en refusant d'appliquer l'incrimination d'homicide involontaire sur un enfant à naître[860].Il en résulte pour le juge répressif l'interdiction de procéder par extension, analogie ou induction. Les magistrats ne peuvent donc étendre l'incrimination à des situations non prévues par le texte.

Toutefois, la loi étant générale et impersonnelle, elle ne peut pas tout envisager et il a fallu admettre une interprétation de la loi par le juge mais uniquement afin qu'il puisse en combler les éventuelles lacunes. Le juge doit être capable de s'écarter de la lettre de la loi lorsqu'un respect trop pointilleux du texte amènerait à des situations absurdes. Le juge est alors tenu à une interprétation stricte du droit pénal mais a la possibilité d'écarter une disposition contraire à une norme du droit international ou du droit interne si la solution du procès en dépend. Par exemple, l'article 78, 5° du décret du 11 novembre 1917 interdisait aux voyageurs « *de monter et de descendre ailleurs que dans les gares (…) et lorsque le train est complétement arrêté ». Donc, ce texte imposait aux voyageurs de descendre lorsque le train était en marche. Cette situation étant illogique, les juges ont interprété le texte en condamnant un individu qui était descendu alors que le train était en marche, conformément à la volonté du législateur*[861].

La question s'est également posée avec le vol de données informatiques. Prévu par l'article 311-1 du Code pénal, le vol est « *la soustraction frauduleuse de la chose d'autrui* ». Cette incrimination vise notamment le vol d'une clé USB ou d'un disque dur sur lequel se trouverait une donnée puisqu'en étant assimilable à une chose appartenant à autrui, ce support physique répond à la qualification classique du vol. Les enjeux ne concernent pas le vol du support nonobstant son contenu, mais le vol ou la copie de données se trouvant sur un système. En ce sens, l'article 311-1 du Code pénal n'est pas adapté comme il ne l'était pas pour le vol d'énergie, bien immatériel[862]. En effet, une donnée informatique n'est pas une chose mais un composant immatériel séparable de tout support de stockage. De plus, lorsqu'une donnée est extraite d'un système de traitement automatisé de données, sa soustraction n'est pas systématique puisque la

[860] Cour de cassation, Assemblée Plénière, 29 juin 2001 : Bulletin criminel n°165.
[861] Cour de cassation, chambre criminelle, 19 mai 1999 : Bulletin criminel n° 99, 98-80726. Disponible à cette adresse : https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007070823, [consulté le 30 mars 2015].
[862] Une incrimination spécifique a été créée par le législateur à l'article 311-2 du Code pénal.

copie sur un autre support est possible. Or, la reproduction de données n'est pas une soustraction dans la mesure où le vrai propriétaire n'est pas dépossédé.

Pourtant, la jurisprudence a essayé de faire face aux lacunes de la loi en envisageant le vol de données, une première fois en 2008 et une seconde fois en 2015[863] avec l'arrêt « *Bluetouff* ». Le 4 mars 2008, dans un arrêt non publié au bulletin[864], la chambre criminelle de la Cour de cassation porte atteinte au principe d'interprétation stricte de la loi pénale en retenant la qualification de vol pour une copie de données. En l'espèce, les magistrats du Quai de l'horloge ont rejeté le pourvoi formé contre l'arrêt de la Cour d'appel de Rennes qui avait condamné les prévenus pour le vol de données sur le fondement de l'article 311-1 du Code pénal. Le 20 mai 2015, dans un autre arrêt,[865] la chambre criminelle de la Cour de cassation rejette le pourvoi formé contre l'arrêt de la cour d'appel de Paris qui avait retenu le vol de données d'un bloggeur s'étant introduit sur le site de l'ANSES[866].

L'avocat général M. Desportes a conclu en faveur du vol de données et la Cour de cassation l'a suivi : « *tout en respectant le principe d'interprétation stricte de la loi pénale, vous avez toujours su adapter les incriminations aux évolutions technologiques, veillant à ce que soient atteints les objectifs du législateur et donc à ce que la loi soit appliquée conformément à la fois à sa lettre et à son esprit. Cela est particulièrement vrai s'agissant du vol dont la définition a révélé une certaine plasticité*[867] ».

En l'espèce, la Cour d'appel de Paris avait infirmé le jugement du tribunal de Créteil en condamnant le protagoniste pour piratage informatique, mais aussi pour vol de fichiers informatiques. En 2013, le prévenu avait en effet récupéré des données sur le site de l'ANSES en exploitant une faille de sécurité. Pour les juges du fond, l'individu « *avait conscience de son*

[863] Cet arrêt est postérieur à la loi du 13 novembre 2014 mais les faits lui y sont antérieurs.
[864] Cour de cassation, chambre criminelle, 4 mars 2008, n°07-84.002. Disponible à cette adresse : https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000018550314&fastPos=1, [consulté le 30 mars 2015].
[865] Cour de cassation, chambre criminelle, 20 mai 2015, n° 14-81336. Disponible à cette adresse : https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000030635061, [consulté le 21 mai 2015].
[866] Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail
[867] REES M., *Affaire Bluetouff : la Cour de cassation consacre le vol de fichiers informatiques*, 22 mai 2015. Disponible à cette adresse : https://www.nextinpact.com/news/95165-affaire-bluetouff-cour-cassation-consacre-vol-fichiers-informatiques.htm, [consulté le 22 mai 2015].

maintien irrégulier dans le système de traitement automatisé de données visité ». Un pourvoi en cassation est alors formé par le prévenu qui estime notamment qu'il n'y a pas de vol sans dépossession.

Mais la Cour de cassation ne l'entend pas de cette oreille puisqu'elle rejette le pourvoi et estime que la cour d'appel a bien justifié sa décision. Ses motifs sont les suivants : « *(le prévenu s'est) maintenu dans un système de traitement automatisé après avoir découvert que celui-ci était protégé et a soustrait des données qu'il a utilisées sans le consentement de leur propriétaire* ». Avec cet arrêt, la Cour de cassation considère que le téléchargement de données est du vol[868]. Pourtant aux moments des faits, c'est la loi du 5 janvier 1988 relative à la fraude informatique, dite Godfrain, qui trouvent à s'appliquer. Or, les débats parlementaires de cette loi montrent que le législateur n'a pas eu l'intention d'assimiler le téléchargement de contenu à du vol.

La loi du 13 novembre 2014[869] renforçant les dispositions relatives à la lutte contre le terrorisme est venue clarifier la législation en apportant deux modifications non négligeables. Premièrement, l'article 323-3 du Code pénal réprime désormais « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* ». Secondement, le terme « extraction » fait son entrée dans la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. L'utilisation de ce terme et du verbe « *extraire* » à la place de la notion de vol est-elle opportune ? Ces termes sont employés car ils impliquent un transfert et permettent de viser la copie de données qui restent en la possession du maître du système. En outre, le terme « *reproduire* » de l'article 323-3 du Code pénal permet de sanctionner l'acte de copie. Ces décisions *contra legem* ont donc entrainé une intervention du législateur. Dans d'autres cas, le juge a la possibilité d'écarter une disposition (B).

B) La possibilité d'écarter une disposition

Le juge répressif a la possibilité d'écarter d'office ou à la demande d'une partie, une disposition contraire à une norme interne ou internationale dès lors qu'elle conditionne la solution du

[868] Elle ne le précise pas, mais ce postulat ne s'applique pas en matière de propriété intellectuelle et donc pour le téléchargement et le streaming illégaux. En effet, pour ces infractions, c'est la loi dite Hadopi qui s'applique et non la nouvelle loi de novembre 2014. Or, en droit, le spécial déroge au général.
[869]Elle ne s'applique pas en l'espèce car les faits qui sont antérieurs à son entrée en vigueur.

procès qui lui est soumis et ce afin de respecter la hiérarchie des normes.[870]

S'agissant en premier lieu du droit interne, le contrôle de validité des règlements[871] relève en théorie de la compétence des juridictions administratives, par voie d'action au moyen du recours pour excès de pouvoir, et le principe de séparation des autorités administratives et judiciaires[872] devrait contraindre le juge pénal à surseoir à statuer et à inviter les parties à saisir le juge administratif afin qu'il statue sur la validité de l'acte administratif. Néanmoins, la jurisprudence a permis au juge pénal d'apprécier la légalité d'un acte réglementaire invoqué au cours d'un procès pénal[873] et cette compétence des juridictions répressives pour statuer sur l'illégalité d'un acte réglementaire a été consacrée par l'article 111-5 du Code pénal qui dispose que « *les juridictions pénales sont compétentes pour interpréter les actes administratifs, réglementaires ou individuels et pour en apprécier la légalité lorsque, de cet examen, dépend la solution du procès pénal qui leur est soumis* ». Par conséquent, le juge pénal peut refuser d'appliquer un acte administratif[874], fondement de l'incrimination ou moyen de défense, s'il l'estime non conforme à la loi. Cet acte peut avoir une porté réglementaire[875] ou individuelle[876].

S'agissant, en second lieu, du droit international, le juge peut écarter un texte répressif, une loi ou un règlement, qui serait contraire au droit communautaire ou au droit de la CESDH. Ce contrôle a d'abord été effectué par la Cour de cassation[877], avant d'être repris par le Conseil d'Etat qui abandonne sa jurisprudence de 1968[878] pour se rallier à la position de la Cour de cassation[879]. Cette prise de pouvoir peut paraître par nature inquiétante dans cette protection des libertés individuelles contre l'arbitraire mais cela démontre qu'aujourd'hui il n'est plus

[870] Théorisée par Hans Kelsen (1881-1973), elle permet de garantir une cohérence du système juridique en hiérarchisant l'ensemble des normes. Ainsi, le règlement doit respecter la loi, les traités internationaux et la Constitution.
[871] A l'instar du juge civil, le juge pénal n'effectue pas de contrôle de constitutionnalité de la loi mais opère seulement un contrôle du règlement par rapport à la loi, on parle de contrôle de légalité.
[872] Prévu à l'article 13 de la loi sur l'organisation judiciaire des 16 et 24 août 1790, toujours en vigueur, il prévoit que « *les fonctions judiciaires sont distinctes et demeureront toujours séparées des fonctions administratives. Les juges ne pourront, à peine de forfaiture, troubler de quelque manière que ce soit les opérations du corps administratif ni citer devant eux les administrateurs en raison de leurs fonctions* ».
[873] Tribunal des conflits, 5 juillet 1951, *Avranches et Desmarets* ; Cour de cassation, chambre criminelle, 21 décembre 1961, *dame Le Roux*, D. 1962, page 162.
[874] Il ne peut pas en prononcer la nullité, car cela relève de la compétence exclusive du juge administratif.
[875] Décret, ordonnance de l'article 38 de la Constitution avant ratification par le Parlement.
[876] Arrêté, refus de permis de construire, etc.
[877] Cour de cassation, chambre mixte, 24 mai 1975, *Société des Cafés Jacques Vabre*.
[878] Conseil d'Etat, 1er mars 1968, *Syndicat général des fabricants de semoule de France*.
[879] Conseil d'Etat, Assemblée, 20 octobre 1989, *Nicolo*.

possible de considérer le principe de légalité criminelle dans son son strict. Désormais, le terme « *loi* » inclue la loi au sens strict et le règlement.

En France, c'est l'article 111-3 du Code pénal[880] qui définit le partage de compétences entre la loi et le règlement et qui amène par ailleurs certains auteurs à se référer non plus au principe de légalité mais au principe de textualité. Ainsi, théoriquement, seuls le législateur et les autorités réglementaires peuvent ériger un comportement en infraction et fixer les peines applicables à leurs auteurs. Néanmoins, cette souveraineté des Etats membres dans le domaine pénal est remise en cause et les sources sont en réalité plus nombreuses. Lorsqu'elles le permettent le juge a la possibilité de prononcé une peine adéquate (§2).

§2) Le prononcé de la peine

Si après examen des faits, il est établi que l'infraction est constituée dans tous ses éléments juridiques et que l'auteur est pénalement responsable des faits poursuivis, une sanction est prononcée par le juge. Si cette sanction prendra le plus souvent la forme d'une peine, le juge peut également prononcer une mesure de sûreté. La distinction entre « *peine* » et « *mesure de sûreté* » repose sur leur finalité. Alors que la peine est le « *prix* » à payer pour une infraction, la mesure de sûreté peut être définie comme une mesure individuelle imposée à des individus dangereux pour l'ordre social afin de prévenir la commission d'infractions que leur état de dangerosité rend probable. Les mesures de sûreté diffèrent donc des peines en ce qu'elles n'ont pas de buts d'intimidation ; leur objet est exclusivement de prévenir la commission d'infractions futures par une personne réputée dangereuse.

Dans les limites fixées par la loi, le juge dispose du pouvoir d'individualiser la sanction, tant dans sa nature que dans sa mesure, en fonction des circonstances de l'infraction et de la personnalité de son auteur, ainsi que des ressources et des charges de celui-ci s'agissant de la détermination du montant de l'amende. En ce sens, le législateur a créé des peines complémentaires relatives à Internet.

[880] §1 « *Nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi, ou pour une contravention dont les éléments ne sont pas définis par le règlement. » §2 « Nul ne peut être puni d'une peine qui n'est pas prévue par la loi, si l'infraction est un crime ou un délit, ou par le règlement, si l'infraction est une contravention* ».

Souvent, les cybercriminels passent à l'action en utilisant des ressources immatérielles telles que des noms de domaine ou des forums. L'exemple de *Silkroad* semble tout à fait approprié pour illustrer ce propos. Ainsi, il est opportun de se demander si ce genre de contenu immatériel peut être placé sous-main de justice durant le procès c'est-à-dire de l'enquête judiciaire à la phase de jugement, en passant par la phase d'instruction.

A titre d'exemple, en juillet 2014, à la suite du démantèlement d'un trafic de cryptomonnaies via une plateforme illicite d'échange, les gendarmes de Midi-Pyrénées ont arrêté deux individus. Ils ont ensuite été mis en examen et condamnés à la confiscation de leurs bitcoins. Autre exemple, de janvier à décembre 2018 en Islande[881], des cybercriminels ont dérobé des centaines de serveurs utilisés pour du minage de bitcoins pour un préjudice estimé à presque 1,5 millions d'euros en bitcoin. Pour la réalisation de ce genre d'infraction l'outil informatique est primordial si bien qu'il est nécessaire de le neutraliser en cas d'arrestation.

En France, il serait intéressant d'envisager une peine complémentaire pour la confiscation de ce genre de ressources immatérielles comme les portefeuilles de cryptomonnaies, les adresses électroniques ou les noms de domaines, etc. Une telle peine aurait vocation à s'appliquer pour se substituer à l'emprisonnement[882] et s'inscrirait dans la lignée de l'article 706-103 du Code de procédure pénale relatif à la saisie conservatoire et à la confiscation et du travail de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués. Ensuite, il serait opportun d'interdire l'entrée en contact par le biais d'Internet de l'auteur d'une cyber infraction avec sa victime. Cette interdiction trouverait écho dans l'application d'une disposition similaire du Code pénal[883] en matière de peine : « *13° S'abstenir d'entrer en relation avec certaines personnes, dont la victime, ou certaines catégories de personnes, et notamment des mineurs, à l'exception, le cas échéant, de ceux désignés par la juridiction* ». Si certains ont voulu interdire l'accès total à Internet, cette proposition a été écartée par le Conseil constitutionnel qui se prononçait sur la loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet : « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme [...] : en l'état actuel des moyens de communication et eu égard au*

[881] LE MONDE, *Islande : vol de 600 ordinateurs utilisés pour miner du bitcoin*, 7 mars 2018. Disponible à cette adresse : https://www.lemonde.fr/pixels/article/2018/03/07/islande-vol-de-600-ordinateurs-utilises-pour-miner-du-bitcoin_5267171_4408996.html, [consulté le 8 mars 2018].
[882] Code pénal art. 131-6.
[883] Code pénal art. 132-45.

développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services[884] ». Outre cette limite imposée par le Conseil constitutionnel, il y a une difficulté relative à l'application des peines relatives à la cybercriminalité dans la mesure où il est compliqué pour un juge d'application des peines de vérifier l'application de la peine faite par la personne condamnée. En effet, un condamné pourrait utiliser la connexion wifi d'un voisin et se connecter en utilisant un pseudonyme. Par conséquent, pour faire face aux difficultés procédurales, les magistrats devraient être en mesure d'utiliser des moyens d'enquête appropriés se fondant sur des méthodes d'investigations numériques efficaces et discrètes (chapitre 2).

[884] Décision 2009-580 DC du 10 juin 2009.

CHAPITRE 2
DES DIFFICULTÉS LIÉES À LA PROCÉDURE PENALE

« *Avec les États-Unis et l'Allemagne, la France est l'un des pays précurseurs dans la lutte contre la cybercriminalité. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication a été créé en 2001 par le ministère de l'Intérieur. C'est l'une des premières structures au monde. Sa création, qui remonte à avant même le 11 septembre, a fait office de déclic pour mettre en place un vaste réseau international qui garantisse une réponse coordonnée face aux cybermenaces. La France est régulièrement citée en exemple, notamment en Europe, car elle a des enquêteurs d'excellent niveau, spécialisés en criminalité informatique. Ce n'est pas non plus un hasard si le siège d'Interpol se situe à Lyon. À titre de comparaison, la plateforme européenne Europol a vu le jour il y a seulement deux ans (...) L'action est coordonnée par le ministère de l'Intérieur, où travaille un Monsieur cybercriminalité, Jean-Yves Latournerie*[885]*, dont le rôle est de coordonner les différents services. La police et la gendarmerie ont chacune des enquêteurs spécialisés. La police judiciaire dispose aussi d'une division spéciale, la Sous-direction de lutte contre la cybercriminalité*[886]*. Depuis avril 2014, elle remplace et étend l'action de l'Office, créé en 2001. Quatre-vingts policiers et gendarmes de haut niveau y travaillent pour identifier et anticiper les cybermenaces. L'une de leurs missions est de surveiller le Web. C'est un travail extrêmement difficile, moralement, psychologiquement, notamment pour les agents qui effectuent la veille au sujet de la pédopornographie. Globalement, le champ d'action de la SDLC est plus large que celui de l'Office puisqu'elle prend aussi en compte les attaques subies par les entreprises et les particuliers. Auparavant, les PME dont les systèmes informatiques étaient attaqués, par exemple, ne savaient pas vers qui se tourner, car les policiers de base n'ont pas forcément la connaissance suffisante pour traiter ce genre de plainte. La SDLC va alors conseiller les victimes qui se tournent vers elle, mais aussi les policiers, pour leur indiquer les questions qu'ils doivent poser et ce qu'il faut mentionner dans la plainte*[887] ».

La plupart des pays se sont dotés d'offices de lutte contre la cybercriminalité comme la Suisse

[885] Il est Préfet, chargé de la lutte contre les cybermenaces.
[886] SDLC.
[887] ROLLAND S., *La cybercriminalité est la nouvelle menace du XXIème siècle*, 26 juillet 2015. Disponible sur le site Internet suivant : https://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html, [consulté le 16 avril 2017].

avec le Service de Coordination de la lutte contre la Criminalité sur Internet ou en France, l'Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication.

Cependant, nombreuses sont les infractions qui ne sont pas portées à la connaissance de ces services en raison de l'absence de plainte, c'est le chiffre noir de la cybercriminalité. Il y a donc un écart entre la malveillance connue et celle qui est bien réelle, ce qui accentue la méconnaissance de l'ampleur de la cybercriminalité. Selon le club de la Sécurité de l'Information Français[888], en 2009, le nombre de plaintes déposées à l'international ne représenterait que 20% des délits en général. Par ailleurs, les sondages peuvent être biaisés en fonction de l'intérêt des parties prenantes. En effet, certaines victimes ne souhaitent pas communiquer sur un acte cybercriminel car cela prouverait leur vulnérabilité technologique et leur ferait de la mauvaise publicité. D'autres victimes estiment que l'incident n'est pas assez important, ignorent qu'elles ont été victimes d'une malveillance ou préfèrent agir elles-mêmes en piratant à leur tour les systèmes qui les ont attaquées.

Ainsi, la cybercriminalité dissimulée pose de réels problème concernant l'identification des auteurs d'infraction. « *Cette nouvelle délinquance a conduit le législateur à mener une réflexion sur l'utilisation des nouvelles technologies afin d'adapter la réponse pénale. Dans ce contexte, de nombreux textes furent adoptés ces dernières années avec la volonté de créer un arsenal de la cybersécurité*[889] ».

Il est possible de citer la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite « *Loppsi 2* » qui donne désormais « *la possibilité, sur commission rogatoire du juge, de capter à* distance et en temps réel toutes les informations contenues sur les disques durs d'un ordinateur mais aussi celles apparaissant à l'écran, en particulier dans les affaires liées au terrorisme ou à la grande criminalité. Par ailleurs, depuis 2009, les officiers de police judiciaire ont également la possibilité de procéder à des cyber-infiltrations sous pseudonyme. Prévue inégalement dans les affaires de pédopornographie, cette possibilité a été étendue le 5 décembre 2014 aux enquêtes

[888] CLUSIF.
[889] BOUZOU L., *Les perspectives pénales de la loi LOPSI 2 en matière de cybercriminalité*, 2010, page 45.

terroristes[890]. Il y a une volonté claire de vouloir identifier les auteurs d'infractions commises sur Internet.

Dans une affaire judiciaire, les intermédiaires techniques et les témoins peuvent avoir un rôle à jouer dans l'utilisation des techniques d'investigation (Section 2). À titre d'exemple, au sein d'une entreprise, les informaticiens peuvent se préparer à une éventuelle attaque contre les systèmes mettant en place des procédures de sauvegarde régulières, et faciliter l'enquête le cas échéant. Mais chaque protagoniste est tenu de respecter les règles de procédure pénale classiques (Section 1).

[890] Institut national des hautes études de la sécurité et de la justice, *Enjeux et difficultés de la lutte contre la cybercriminalité*, juillet 2015, page 29.

SECTION 1
L'application des règles de procédure pénale classiques

Internet a entrainé une immatérialisation grandissante d'un nombre quasi infini de données sans fournir une protection suffisamment efficace. Les failles offertes aux cybercriminels et aux cyberdélinquants se sont multipliées. Désormais, les internautes sont plus que jamais vulnérables aux attaques d'individus qui tirent profit d'une nouvelle situation en agissant dans l'ombre. Les cybercriminels du Darknet agissent de manière anonyme si bien qu'il est quasiment impossible de retracer leurs mouvements et de collecter des preuves. Les politiques de prévention mises en place sont insuffisantes et inadaptées à la cybercriminalité visible ou invisible.

En France, il existe deux types d'enquêtes permettant de découvrir et de rechercher des cyber-infractions. L'enquête préliminaire déclenchée par un enquêteur, après un dépôt de plainte par exemple, est la forme la plus simple d'enquête judiciaire. En outre, l'enquête de flagrance intervient lorsqu'une infraction vient de se produire et permet aux enquêteurs d'effectuer un certain nombre d'actes dans un temps très court et sans discontinuer. Ses enquêtes consistent à trouver des preuves. Sans ses dernières aucune accusation ne peut faire l'objet de poursuites judiciaires. Toutefois, à l'instar des preuves classiques, les preuves numériques ne sont pas libres. Les autorités qui collaborent à la manifestation de la vérité ne peuvent user que des moyens conférés par la loi (§1). Par ailleurs, la prescription de l'action publique qui est un motif d'irrecevabilité de l'action publique se basant sur le droit à l'oubli et la négligence de la partie poursuivante peut poser des difficultés lorsqu'il s'agit de poursuivre des cyber-infractions dissimulées (§2).

§1) Le droit de la preuve pénale numérique

La principale difficulté liée à la cybercriminalité concerne les modes de preuve. Même si tous les modes de preuve sont admis[891], les preuves sont difficiles à apporter dans le monde du numérique où les enquêtes judiciaires nécessitent des éléments de preuve susceptibles de se

[891] Code de procédure pénale art. 427 : « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui* ».

manifester sous la forme de documents numériques. Une nouvelle discipline criminalistique a vu le jour, celle relative à la preuve numérique. Ainsi, à l'ère du numérique cette dernière n'est plus l'apanage des enquêtes relatives aux crimes informatiques.

Il n'y a pas de définition de la preuve dans le Code de procédure pénale. En France, tout élément d'information recueilli dans le respect de la loi est recevable au procès. Ces éléments d'enquête peuvent être présentés à la juridiction de jugement qui les évalue. Il peut s'agir d'un procès verbal établi par un enquêteur, d'une audition de suspect ou de témoin, de rapports d'expertise[892], d'analyse de documents, ou d'objets[893]. Concrètement, la preuve permet d'établir la réalité d'un fait ou l'existence d'un acte juridique.

Elle peut être définie plus strictement dans d'autres pays dans la mesure où son exercice varie d'un pays à un autre. Une coopération entre Etats et notamment au niveau européen permet son éventuelle reconnaissance par les tribunaux de différents pays. Il est ainsi possible de citer les principes offerts par l'International *Organisation on Computer Evidence*[894] qui est un groupe scientifique créé en 2015 travaillant sur les preuves numériques ainsi que *l'European Network of Forensic Science Institutes*[895] qui fournit les respecter par les laboratoires criminalistiques pour la preuve numérique.

Pour préserver leur authenticité, les preuves doivent être associés à leur environnement initial et à leurs conditions de saisie et de conservation. Il s'agit de garantir la chaîne de la preuve à l'instar de toutes preuves matérielles. Les enquêteurs démontrent alors que le fichier informatique a été protégé de toute modification extérieure entre la saisie et l'analyse par un spécialiste. A défaut, l'avocat du prévenu ou de l'accusé peut légitimement rejeter les conclusions issues de cet objet. Ainsi, nombreuses sont les situations pour lesquelles un traitement de la preuve, et notamment de la preuve numérique, est nécessaire.

La preuve numérique en droit pénal fait l'objet d'un particularisme certain et d'une importance fondamentale en ce qu'elle assure la conciliation de plusieurs intérêts, parfois opposés. Le

[892] On parle d'expertise lorsqu'un examen complet a été effectué par un expert à la demande d'un juge d'instruction.
[893] Fichiers informatiques comme un disque dur, supports de données, cartes à puce…
[894] http://www.ioce.org/G8_proposed_principles_for_forensic_evidence.html.
[895] http://www.enfsi.org/cms.php?cp=fitwg-docs.

caractère coercitif des preuves permet une recherche efficace de la vérité tout en garantissant une protection accrue des libertés individuelles. Il convient de traiter dans un premier sous-paragraphe la charge de la preuve (A), et dans un second la liberté de la preuve (B).

A) La charge de la preuve

Le droit est fortement impacté par la preuve dont la charge incombe au demandeur[896]. La procédure pénale n'échappe pas à cette règle. En effet, l'article 6, §2 de la CESDH prévoit que « *toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie*[897] ». Cette présomption signifie que la personne poursuivie est tenue pour innocente tant que la preuve de sa culpabilité n'a pas été rapportée. Le principe semble tirer sa substance d'une règle de preuve[898], mais il s'agit, également, d'une règle politique[899] et de l'expression d'un vrai droit subjectif qui s'impose au législateur, aux magistrats mais également aux non-professionnels du droit comme les journalistes[900].

Selon l'adage *actori incumbit probatio*[901], « *la charge de la preuve incombe à la partie poursuivante* ». Le Ministère public doit donc apporter une preuve permettant de renverser la présomption d'innocence dont bénéficie le prévenu. A défaut, selon l'aphorisme *« in dubio pro reo*[902] », le magistrat devra renvoyer le prévenu ou l'accusé des fins de la poursuite.

Dans le cas contraire, après avoir trouvé l'élément légal de l'infraction, c'est-à-dire le texte sur

[896] Code civil art. 1353 : « *Celui qui réclame l'exécution d'une obligation doit la prouver* ».
[897] Voir en ce sens l'article 9 de la Déclaration des droits de l'Homme et du citoyen de 1789, l'article 11 de la Déclaration universelle des droits de l'Homme de 1948 et l'article préliminaire §3 du Code de procédure pénale.
[898] La Cour EDH rattache la présomption d'innocence (article 6, § 2) au droit à un procès équitable (article 6, § 1). Voir notamment CEDH, *Affaire Deweer contre Belgique*, 27 février 1980, 6903/75.
[899] Pour le Professeur Conte, « *la présomption d'innocence consacre des solutions libérales, par l'effet d'un parti pris, de nature politique, en faveur de celui qui est mis en cause et menacé d'une sanction* », Cour de procédure pénale 2018, Licence 2, Université Paris 2 Panthéon Assas.
[900] La loi du 29 juillet 1881 sur la liberté de la presse prévoit des incriminations comme l'interdiction « de publier les actes d'accusation et tous autres actes de procédure criminelle ou correctionnelle avant qu'ils aient été lus en audience publique » (article 38), l'interdiction « *de diffuser l'image d'une personne mise en cause à l'occasion d'une procédure pénale mais n'ayant pas fait l'objet d'un jugement de condamnation et faisant apparaître, soit que cette personne porte des menottes ou entres, soit qu'elle est placée en détention provisoire* » (article 35 ter §1), l'interdiction « *de réaliser, de publier ou de commenter un sondage d'opinion, ou tout autre consultation, portant sur la culpabilité d'une personne mise en cause à l'occasion d'une procédure pénale ou sur la peine susceptible d'être prononcée à son encore* » (article 35 ter, §2).
[901] « *Il appartient au demandeur de faire la preuve de son allégation* ».
[902] « *Le doute profite à l'accusé ».*

le fondement duquel les poursuites vont être engagées, il est nécessaire pour le Ministère public d'établir que l'infraction est caractérisée dans tous ses éléments constitutifs, matériel et intentionnel. La preuve de sa culpabilité pèse sur d'autres parties du procès : la partie civile, mais également les magistrats du siège et notamment le juge d'instruction qui instruit « *à charge et à décharge*[903] ». Enfin, en droit pénal tous les modes de preuve, ou presque, sont admis (B).

B) La liberté de la preuve

En droit pénal, l'administration de la preuve est libre si bien qu'en principe tout élément de preuve peut être versé au dossier. Il peut s'agir de constatations effectuées par les officiers de polices judiciaires, les magistrats ou encore les experts, sur les le corps de la victime, les lieux de l'infraction, l'ordinateur des personnes suspectées. Il peut également s'agir de déclarations émanant de la victime auditionnée, du suspect, du témoin assisté ou du mis en examen (1).

Se pose alors la question de savoir jusqu'où les autorités peuvent aller pour appréhender les délinquants. En France, c'est le Code de procédure pénale, aidé par la jurisprudence, qui donne la réponse. En effet, la fin ne saurait justifier les moyens dans la mesure où les autorités qui aspirent à la manifestation de la vérité doivent se conformer à ce qui est prévu par la loi. En effet, la recevabilité des preuves est limitée par le respect de principes fondamentaux tels que les droits de la défense[904], la dignité[905] et la loyauté de la preuve (2).

1. Les différents modes de preuve

« *Il n'y a pas de serrure dont le crime n'ait la clef*[906] », cette citation reflète idéalement les nouvelles formes de criminalité qui font rage sur Internet et le Darknet[907]. Cyberterrorisme, pédopornographie, trafic de stupéfiants, escroqueries, piratages, vols de données, autant de fléaux qui contraignent les enquêtes policières à s'adapter aux nouvelles technologies.

[903] Code de procédure pénale art. 81.
[904] Les droits de la défense prohibent par exemple la saisie des correspondances entre l'avocat et son client (Article 66-5 de la loi du 31 décembre 1971) ;
[905] Les agents d'un Etat ne peuvent pas utiliser de mauvais traitements pour obtenir des aveux de la part d'un suspect ;
[906] BERTRAND A., *recueil de courts poèmes publié à titre posthume,* 1842.
[907] BOOS R. La lutte contre la cybercriminalité au regard de l'action des États, Université de Lorraine, 2016, page 201.

L'anonymat sous lequel il est possible d'agir sur le Darknet, le chiffrement des données, la facilité d'entrer en contact avec des victimes ou clients potentiels, mettent à l'épreuve les questions probatoires des infractions commises sur Internet et le Darknet. Non loin des méthodes utilisées par « *Malotru* », l'agent secret de la DGSE, dans la série le « *Bureau des légendes* », des unités spécialisées opèrent sur la toile afin d'appréhender des criminels de toute espèce. Lors de leurs investigations les enquêteurs de l'IRCGN[908], de la BEFTI[909] ou de l'OCLCTIC[910] peuvent mettre la main sur des indices numériques qui vont permettre d'établir la vérité et de la prouver. À cette fin, les officiers de police judiciaire sont habilités à procéder à des perquisitions numériques en accédant à un système informatique. Ils peuvent également réquisitionner du matériel informatique comme une clé USB, un disque dur, une tablette tactile ou un ordinateur. Ensuite, ils sont autorisés à participer à des forums de discussion, sous pseudonyme, pour essayer d'entrer en contact avec des criminels.

L'article 427 alinéa 1er du code de procédure pénale énonce que « *hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction* ». Ainsi, en droit pénal, tous les modes de preuves, ou presque, sont admis. C'est au juge d'apprécier la valeur probante de chaque élément du procès et de prendre une décision selon son intime conviction. Pour ce faire, il apprécie de manière souveraine les faits et les preuves soumis à son examen. Seuls certains moyens de preuve imparfaits ne peuvent justifier à eux seuls une condamnation. Tel est le cas pour le témoignage anonyme ou les déclarations d'une victime.

Un autre moyen destiné à améliorer la lutte contra la cybercriminalité a été mis en place par un arrêté du 16 juin 2009[911]. Il s'agit de la plateforme « *PHAROS*[912] » qui permet aux internautes ou aux fournisseurs d'accès de dénoncer tout contenu répréhensible d'Internet en le signalant à l'OCLCTIC. Ce dernier effectue des rapprochements entre tous les signalements pour les

[908] L'Institut de recherches criminelles est une unité de la Gendarmerie chargée des aspects scientifiques des investigations. Des enquêteurs spécialisés peuvent épauler des unités de terrain pour des enquêtes complexes relatives à la cybercriminalité, ou pour analyser des preuves numériques.
[909] Brigade d'enquêtes sur les fraudes aux technologies de l'information.
[910] Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.
[911] Arrêté du 16 juin 2009 portant création d'un système dénommé « *PHAROS* », JORF n°0141 du 20 juin 2009.
[912] Plateforme d'harmonisation d'analyse de recoupement et d'orientation des signalements.

transmettre aux services enquêteurs. En outre, les réseaux sociaux sont très utiles pour les enquêteurs. Ce genre d'aide des internautes appelée « *enquête participative sur Internet* » se fait également sur le Darknet notamment en matière de pédophilie.

Une fois les preuves récoltées les enquêteurs ont la lourde tâche de faire correspondre l'heure des faits, les témoignages, les constatations et les données techniques récupérées. Dans le domaine de la preuve numérique, l'interprétation d'une date est essentielle pour évaluer la culpabilité d'un individu. Les objets numériques tels que les téléphones portables, les cartes à puce, les ordinateurs ou les tablettes tactiles possèdent des informations de date que les enquêteurs doivent prendre avec des pincettes. Il peut s'agit des dates et horaires situées dans les en-têtes de mails et qui proviennent des serveurs via lesquels le mail circule. La vérification de ces dates est très simple mais leur fiabilité incertaine dans la mesure où ces serveurs peuvent être situés à l'étranger. Il peut également s'agir de dates liées à des fichiers se trouvant sur des disques durs ou des clés USB et pouvant être modifiées par l'utilisateur. Dès lors, les dates et heures doivent être prises avec précaution et confrontées aux autres constatations techniques, qui pourront être concordantes ou discordantes.

Par conséquent, le riche domaine de la preuve numérique concerne à la fois le technique et juridique. Des enquêteurs formés doivent ainsi maîtriser la procédure et l'informatique afin d'avoir une longueur d'avance sur des auteurs d'infraction en constante évolution.

Toutefois, ces enquêteurs sont limités par le principe de loyauté de la preuve qui interdit aux agents publics d'inciter à l'infraction. Ce faisant, ils ne peuvent pas créer de sites de ventes de drogues sur le Darknet afin de piéger des trafiquants (2).

2. La limite à la liberté de la preuve : l'exigence de loyauté

Tout moyen de preuve qui constituerait une ingérence dans la vie privée doit, conformément à l'article 8 §2 de la CESDH, « *être prévue par la loi* » sous peine d'être déclaré irrecevable au motif de son inconventionnalité[913]. C'est notamment le cas pour les écoutes téléphoniques qui

[913] L'article 55 de la Constitution du 4 octobre 1958 prévoit que « les traités ou accords régulièrement ratifiés ou approuvés ont, dès leur publication, une autorité supérieure à celle des lois, sous réserve, pour chaque accord ou traité, de son application par l'autre partie ». Dès lors, la loi française doit être conforme aux Conventions.

n'étaient pas encadrées par la loi si bien que leur recevabilité a été contestée. Pendant longtemps, la Cour de cassation a admis les écoutes téléphoniques autorisées par le juge d'instruction et refusé le procédé lors d'une enquête[914] en se fondant sur l'article 81 du Code de procédure pénale[915]. Cela supposait l'absence d'artifice ou d'atteinte aux droits à la défense[916].

Toutefois, se fondant sur l'article 8 de la Convention, la Cour EDH a estimé qu'il y avait une lacune juridique en France, en ce qui concerne la mise en œuvre et le contrôle des écoutes[917]. Dès lors, le législateur est intervenu en adoptant la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques[918]. D'autres limites concernant la provocation à l'infraction ont été affirmées (a) et ont créé des difficultés lors des opérations d'infiltration (b).

a) La provocation à l'infraction

L'exigence de loyauté dans l'administration de la preuve n'a pas vocation à s'appliquer aux particuliers. La jurisprudence estime en effet que les juges ne peuvent pas écarter les preuves obtenues de manière illicite ou déloyale lorsque qu'elles sont produites par une partie privée[919], prévenu ou partie civile, ou par un témoin[920]. D'aucuns estiment qu'il est nécessaire de protéger les particuliers qui ne disposent pas des mêmes moyens que les autorités publiques. D'autres estiment qu'il s'agit d'une stricte application de l'article 427 du Code de procédure pénale : « *hors les cas où la loi en dispose autrement (...) »*. En effet, il n'y a pas de texte en matière d'administration de la preuve des particuliers.

En revanche, la loyauté est une règle absolue en matière d'administration de la preuve des

[914] Cour de cassation, chambre criminelle, 13 juin 1989, Bulletin criminel n°254.
[915] « Le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité. Il instruit à charge et à décharge ».
[916] Cour de cassation, chambre criminelle, 8 novembre 2000, n° 00-83570.
[917] CEDH, 24 avril 1990, Kruslin et Huvig contre France.
[918] Disponible à cette adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000173519, [consulté le 16 avril 2015].
[919] Cour de cassation, chambre criminelle, 11 juin 2002, Bulletin criminel n°131.
[920] Cour de cassation, chambre criminelle, 30 mars 1999, Bulletin criminel n°59.

autorités publiques. En ce sens, les arrêts « *Wilson* »[921] et « *Imbert* »[922] sanctionnent les preuves obtenues déloyalement, et d'autres arrêts[923] les preuves obtenues à la suite du détournement d'une règle de procédure pénale. Sont également sanctionnées les provocations à la commission d'une infraction[924], directement par les enquêteurs ou par un tiers agissant pour eux[925], même lorsque la provocation est réalisée à l'étranger par un agent public étranger, ou par son intermédiaire[926].

Toutefois, même si l'amalgame est fréquent, les provocations à la constatation de la preuve d'une infraction sont acceptées[927]. Dès lors, pour être toléré, le procédé doit permettre la mise en valeur de la preuve d'une infraction qui se serait commise même sans l'intervention de l'enquêteur[928]. L'exemple de l'infiltration pose des difficultés concernant la différence entre la provocation à l'infraction et à la preuve (b).

b) Les opération d'infiltration

Le législateur a autorisé les officiers et agents de police judiciaire à mettre en place des opérations d'infiltration pour les infractions relative aux stupéfiants[929] et à la criminalité organisée[930].

Ces infiltrations qui ne doivent, à peine de nullité, inciter « *à commettre une infraction*[931] », peuvent également être numériques (∂). En outre, les enquêteurs peuvent utiliser l'enquête sous pseudonyme (ß).

[921] Cour de cassation Chambres Réunies, 31 janvier 1888 (S. 1889 I 241). En l'espèce, est condamné le fait pour un magistrat instruction d'avoir contacté par téléphone un complice de l'inculpé en imitant sa voix.
[922] Cour de cassation, chambre criminelle, 12 juin 1952, Bulletin criminel n°153. En l'espèce, un OPC est sanctionné après qu'il a organisé une conversation téléphone entre deux personnes et dicté à l'une les questions afin d'enregistrer les réponses de l'autre.
[923] Cour de cassation, Assemblée plénière, 6 mars 2015, Bulletin Assemblée plénière n°2. La Cour de cassation censure au nom du principe de loyauté, les policiers qui sonorisent sur autorisation d'un juge d'instruction deux cellules contigües pour y placer deux individus en garde à vue et faire en sorte que l'un des deux s'auto-incrimine.
[924] Cour de cassation, chambre criminelle, 9 août 2006, Bulletin criminel n°202.
[925] Cour de cassation, chambre criminelle, 11 mai 2006, Bulletin criminel n°132.
[926] Cour de cassation, chambre criminelle, 4 juin 2008, Bulletin criminel n°141.
[927] Cour de cassation, chambre criminelle, 8 juin 2005, Bulletin criminel n°173.
[928] Cour de cassation, chambre criminelle, 30 avril 2014, Bulletin criminel n°119.
[929] Code de procédure pénale Art. 706-32.
[930] Code de procédure pénale art. 706-81 et suivants.
[931] Code de procédure pénale art. 707-81 alinéa 2.

∂) Les infiltrations numériques

La loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance[932] a inséré les articles 706-35-1 et 706-47-3 dans le Code de procédure pénale relatifs à l'infiltration numérique. Le premier concerne les infractions prévues par les articles 225-4-1 à 225-4-9 du Code pénal en matière de traite des être humains, par les articles 225-5 à 225-12 en matière de proxénétisme, et par les articles 225-12-1 à 225-12-4 en matière de prostitution de mineurs ou de personnes vulnérables. Le second a pour objet la constatation des infractions prévues aux articles 227-18 à 227-24 du Code pénal concernant la mise en péril des mineurs et donc la pédopornographie. L'article 34 de la loi du 14 mars 2001 dite « *LOPSSI II* » a étendu le dispositif à l'infraction de provocation ou d'apologie du terrorisme[933] commise via un moyen de télécommunication[934]. Ainsi, lorsque ces infractions sont commises par Internet, les officiers et agents de police judicaires spécialisés et habilités sont autorisés à procéder à certains actes en étant pénalement irresponsables, et à être actifs sous pseudonyme sur des forums de discussions.

Récemment, la Cour de cassation [935] s'est prononcée sur la régularité d'une procédure impliquant un agent infiltré, accusé d'avoir provoqué à l'infraction. En l'espèce, un individu mis en examen estime d'une part que les règles relatives à l'infiltration n'ont pas été respectées, et d'autre part, que la preuve recueillie à la suite de l'infiltration est déloyale en raison d'une provocation à l'infraction. La Cour de cassation estime que la procédure d'infiltration a été respectée et qu'il n'y a pas eu de provocation à l'infraction. Pourtant, en l'espèce, sans l'aide apportée par l'agent infiltré et l'informateur, l'infraction n'aurait pas été possible. Dès lors, il s'agissait bel et bien d'une provocation à l'infraction et non d'une constatation de l'infraction. Une telle décision est en retrait par rapport à la jurisprudence classique en matière de loyauté des preuves et se rapproche des méthodes utilisées ou Pays-Bas ou aux Etats-Unis.

En effet, le principe de la loyauté de la preuve ne s'applique par dans tous les pays du monde

[932] Disponible à cette adresse :
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000615568.
[933] Article 24 alinéa 6 de la loi du 29 juillet 1881.
[934] Code de procédure pénale art. 706-25-2.
[935] Cour de cassation, chambre criminelle, 9 mai 2018, n° 17-86.558. Disponible à cette adresse : https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000036930206&fastReqId=1014469580&fastPos=1, [consulté le 10 mai 2018].

ou alors de manière différente. A titre d'exemple, aux Pays-Bas une ONG a utilisé un procédé assez singulier pour démontrer l'ampleur de la cyberpédocriminalité. En 2013, l'ONG « *Terre des Hommes*[936] » a créé « *Sweetie* », une petite fille virtuelle de dix ans censée résider aux Philippines, afin qu'elle soit très active sur les réseaux sociaux et forums de discussions. Le résultat est alarmant puisque près de vingt-mille prédateurs sexuels ont été attirés par le profils de l'enfant. Ces pédophiles souhaitaient entrer en contact avec l'enfant afin qu'elle réalise à distance des actes sexuels devant se webcam. Selon un cadre de l'ONG, « *ils sont des milliers d'enfants à subir ces actes. Tous souffrent de dépression. Avec la démocratisation de l'Internet, ce type d'exploitation ne va cesser d'augmenter. Pour la contrer, il faut frapper directement la demande*[937] ». Les informations personnelles de mille d'entre eux ont pu être transmises aux autorités des Etats concernés et à Interpol. En effet, sans piratage informatique, mais uniquement en croisant les informations transmises[938] par les prédateurs eux-mêmes, les enquêteurs de l'ONG ont su identifier mille hommes, d'une soixantaine de pays différents, ayant pris contact avec « *Sweetie* ». Six d'entre eux ont été poursuivis pour « *tourisme sexuel par webcam commis à distance* ».

Aux États-Unis les opérations d'infiltration sont nombreuses et permettent d'obtenir des résultats éloquents. En juin 2018, le ministère de la Justice américain a mis en place une action d'infiltration à échelle nationale afin de cibler les trafiquants de produits illicites du Darknet. L'opération qui a nécessité l'implication de cinq agences fédérales[939] a permis de cibler une soixantaine de réseaux impliqués dans une centaine d'affaires différentes et de perquisitionner des stupéfiants, des millions de dollars en espèces et en or, de la cryptomonnaie pour une valeur de plus de vingt millions de dollars et des armes. Selon Inès Straub, « *si cette opération n'est qu'une goutte d'eau dans l'immensité des vendeurs illégaux du darkweb, il s'agit pour le gouvernement américain de montrer que cet espace n'est pas hors d'atteinte* ».

En matière de pédopornographie, le FBI organise également des opérations très efficaces grâce

[936] Cette fédération qui a des antennes dans toute l'Europe est très active en matière de lutte contre la pédopornographie.
[937] LE PARISIEN, *Sweetie piège 20000 prédateurs*, 6 novembre 2013. Disponible à cette adresse : http://www.leparisien.fr/espace-premium/actu/sweetie-piege-20000-predateurs-06-11-2013-3290473.php, [consulté le 7 décembre 2014].
[938] Page Facebook, ville de résidence, âge…
[939] Le ministère de la justice, la DEA, les renseignements de la sécurité intérieure, l'inspection des services postaux et les services secrets américains.

à la technique du « *honeyspot* » qui consiste à attirer les individus sur des sites afin de les neutraliser. En 2016, des agents ont pris le contrôle d'un site du Darknet, pour y laisser des centaines de milliers d'utilisateurs y naviguer librement et télécharger du contenu pédopornographique. Cela leur permet d'identifier des pédophiles qui agissent sur le Darknet. Le FBI met en place ce genre d'opération depuis 2011[940]. À titre d'exemple, du 20 février au 4 mars 2015, le FBI a pris le contrôle du site « *Playpen*[941] », un site pédopornographique du Darknet accessible via Tor créé en 2014. L'agence américaine l'a laissé en ligne avec tout le contenu pédophile afin de pister les individus s'y étant connectés. Pour ce faire, elle a utilisé un malware et infecté les ordinateurs afin d'obtenir les adresses IP des membres s'étant connectés sur le site. En outre, elle a utilisé un autre outil de piratage appelé « *NIT – Network Investigative*[942] » permettant l'identification des 1300 adresses IP obtenues. Cette opération marquante a permis la fermeture du « *plus grand réseau de pornographique juvénile au monde présent sur le dark web*[943] ».

Toutefois, les méthodes utilisées par le FBI ont fait polémique[944]. Pour l'avocat d'un des accusés du site « *Playpen* », le NIT est une « *extraordinaire extension de la surveillance du gouvernement et de l'utilisation de méthodes illégales à échelle massive* ». Selon Christopher Soghoain[945], « *nous ne parlons pas de rechercher un ou deux ordinateurs. Nous parlons du gouvernement qui pirate des centaines d'ordinateurs, à partir d'un seul mandat*[946] ». Pour l'avocat d'un autre accusé, il s'agit de la provocation à l'infraction car c'est comme si le FBI « *inondait d'héroïne un quartier pour espérer ensuite hameçonner quelques utilisateurs de second rang*[947] ». Dès lors, la justice américaine a annulé la procédure pour vice de procédure

[940] En 2011, l'opération « Torpedo » avait permis de récolter les adresses IP de 25 pédophiles qui utilisaient Tor.
[941] Parc de jeu.
[942] Une technique d'investigation réseau.
[943] ELODIE, *Le FBI pirate le Deep Web pour débusquer des pédophiles*, 8 janvier 2016. Disponible à cette adresse : https://www.journaldugeek.com/2016/01/08/fbi-pirate-deep-web-pedophiles, [consulté le 8 janvier 2016].
[944] LAUSSON J., *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*, 22 avril 2016. Disponible à cette adresse : https://www.numerama.com/politique/165488-pedopornographie-quand-un-piratage-par-le-fbi-sur-tor-prive-les-victimes-dune-justice.html, [consulté le 9 mai 2016].
[945] Il est membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux Etats-Unis.
[946] LAUSSON J., Op. cit.
[947] LORRIAUX A., *Le FBI a pris le contrôle d'un site pédopornographique pour arrêter des criminels. Est-ce éthique*, 26 janvier 2016. Disponible sur le site Internet de « *slate »* : http://www.slate.fr/story/113193/fbi-pedopornographie, [consulté le 9 mai 2016].

et non respect du droit du suspect de savoir la méthode utilisée pour l'identifier. Pour le vice de procédure, le magistrat s'est fondé sur un argument juridictionnel. En effet, l'illégalité du mandat utilisé par le FBI est due au non respect de l'article 41 du Code de procédure pénale américain[948] qui limite l'autorité des magistrats lorsqu'ils émettent un mandat au delà de leur compétence territoriale. En l'espèce, le mandat a été émis par un magistrat se trouvant en Virginie alors que l'un des suspects interpellés par le FBI vit dans le Massachusetts. Ni le mandat ni les preuves retenues ne sont valables. En outre, le FBI n'a pas divulgué d'information quant à la méthode utilisée pour obtenir les adresses IP des utilisateurs de « *Playpen* » qui pensaient jouir d'un anonymat total grâce à l'utilisation du Darknet Tor. Cette abstention est contraire aux droits de la défense selon lesquels un accusé doit savoir comment les preuves ont été collectées pour être en mesure de contester la fiabilité du processus. Pour cette raison, les preuves collectées ont été invalidées par la justice américaine.

Enfin, en matière de terrorisme, un rapport sorti en juillet 2014[949] a montré que le FBI pouvait parfois pousser des individus à commettre des actes terrorismes. L'ONG *Human Rights Watch* qui a produit ce rapport estime que « *dans certains cas, le FBI pourrait avoir créé des terrorismes chez des individus respectueux de la loi en leur suggérant l'idée de commettre un acte terroriste*[950] ». D'après l'ONG, dans près de 30% des affaires, l'agent infiltré aurait eu un rôle actif. Ces milliers d'agents infiltrés en activité aux Etats-Unis peuvent désigner des cibles et même fournir des armes. Selon l'ONG, ils visent des jeunes musulmans fragiles facilement manipulables[951].

Les exemples de sites pédopornographique et ceux des terroristes infiltrés par des agents ne sont pas semblables dans la mesure où dans le premier cas, les agents ont un rôle passif. Mais en tout état de cause, rien ne prouve que ces individus auraient commis de telles infractions sans l'action du FBI. Des limites légales doivent être établies pour ces infiltrations qui peuvent se révéler dangereuses. En France, l'enquêtes sous pseudonyme est également possible (ß).

[948] https://www.law.cornell.edu/rules/frcrmp/rule_41.
[949] HRW, *US : Terrorisme Prosecutions Often An Illusion*, 21 juillet 2014. Disponible à cette adresse : https://www.hrw.org/news/2014/07/21/us-terrorism-prosecutions-often-illusion
[950] LORRIAUX A., Le FBI a pris le contrôle d'un site pédopornographique pour arrêter des criminels. Est-ce éthique, 26 janvier 2016. Disponible à cette adresse : http://www.slate.fr/story/113193/fbi-pedopornographie, [consulté le 9 mai 2016].
[951] Tel serait le cas pour Sami Osmakac un jeune homme de 27 ans qui souffrait de schizophrénie et qui a été condamné à 40 ans de prison pour terrorisme.

ß) L'enquête sous pseudonyme

La lutte contre la pédopornographie nécessite un cadre procédural idoine prenant en considération les particularités d'un tel phénomène en constante mutation. Néanmoins, le législateur est tiraillé entre deux intérêts qu'il ne peut pas négliger. D'une part, il y a la garantie des libertés individuelles qui doit être assurée dans le cadre des règles de procédures pénales, d'autre part, la poursuite d'individus très dangereux qu'il faut appréhender pour la sécurité de tous.

La loi n° 2007-293 du 5 mars 2007 reformant la protection de l'enfance[952] a prévu un régime particulier et « *de nouvelles dispositions autorisant des enquêteurs, formés à cette mission et spécialement habilités, à procéder à des investigation sous pseudonyme sur Internet en matière d'atteintes portées aux mineurs, de traite des êtres humaines et de proxénétisme*[953] ».

À l'instar des autres types de criminalité organisée, l'idée est de renforcer et renouveler les moyens d'investigation des enquêteurs pour leur permettre d'appréhender plus facilement les pédophiles surfant sur Internet. Désormais, l'enquête sous pseudonyme, dite « *cyber infiltration* », permet aux enquêteurs habilités, dits « *cyber patrouilles* », de faire usage d'un pseudonyme afin d'échanger électroniquement du contenu pédopornographique avec des suspects. Une telle procédure vise à créer le contact avec des individus soupçonnés d'être des auteurs d'infractions. Le législateur permet aux officiers ou agents de polices judiciaire d'agir comme de réels pédophiles en s'abonnant sur des sites Internet commercialisant du contenu pédophile. Néanmoins, ce dispositif amène à se poser des questions quant à sa mise en œuvre sur le Darknet où l'identification des pédophiles est très compliquée.

Concernant son domaine, le législateur a apporté des restrictions en la limitant aux infractions mentionnées aux articles 225-4-1 à 225-4-1 à 225-4-9, 225-5 à 225-12 et 225-12-1 à 225-12-4

[952] Cette loi « *poursuit trois objectifs : renforcer la prévention, améliorer le dispositif d'alerte et de signalement, diversifier les modes d'intervention auprès des enfants et de leur famille. Plaçant au cœur du dispositif l'intérêt de l'enfant, elle a aussi pour ambition de renouveler les relations avec les familles* ».
[953] Disponible à cette adresse : http://www.textes.justice.gouv.fr/art_pix/JUSD1005244C.pdf, [consulté le 12 septembre 2017].

du Code pénal relative à la traite des êtres humains et aux proxénétisme[954], aux articles 227-18 à 227-24 du Code pénal concernant les atteintes aux mineurs[955] et à certains infractions contre les STAD[956]. Cela est très regrettable puisque sur le Darknet et sur le Web visible, cette technique permettrait d'identifier plus facilement les auteurs d'infractions qui échangent électroniquement sur des plateformes spécialisées. Cette disposition procédurale permettant de lutter contre la cybercriminalité devrait pouvoir s'appliquer à plus d'infractions du Web visible ou invisible. Les actes autorisés sont la participation « *sous un pseudonyme aux échanges électroniques* », la prise de « c*ontact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions* » et « *l'extraction, la transmission en réponse à une demande expresse, l'acquisition ou la conservation du contenu illicite* ».

[954] Code de procédure pénale art. 706-35-1 : « *Dans le but de constater les infractions mentionnées aux articles 225-4-1,225-4-8,225-4-9, 225-5,225-6 et 225-12-1 à 225-12-4 du code pénal et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé et spécialement habilités à cette fin, dans des conditions précisées par arrêté, procéder aux actes suivants sans en être pénalement responsables : 1° Participer sous un pseudonyme aux échanges électroniques ; 2° Etre en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ; 2° bis Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ; 3° Extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites dans des conditions fixées par décret. A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions* ».

[955] Code de procédure pénale art. 706-47-3 : « *Dans le but de constater les infractions mentionnées aux articles 227-18 à 227-24 du code pénal et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé et spécialement habilités à cette fin, dans des conditions précisées par arrêté, procéder aux actes suivants sans en être pénalement responsables : 1° Participer sous un pseudonyme aux échanges électroniques ; 2° Etre en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ; 2° bis Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ; 3° Extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites dans des conditions fixées par décret. A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions* ».

[956] Code de procédure pénale art. 706-87-1 : « *Dans le but de constater les infractions mentionnées aux articles 706-72,706-73 et 706-73-1 et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables : 1° Participer sous un pseudonyme aux échanges électroniques…* ».

Ces investigations sont donc possibles pour la traite des êtres humains[957], le proxénétisme[958], la provocation à l'usage ou au trafic de stupéfiants[959] , la provocation à la consommation habituelle d'alcool[960], la provocation d'un mineur à commettre un crime ou un délit[961], la corruption de mineur[962], l'enregistrement d'images pornographiques de mineurs en vue de leur diffusion[963], la fabrication et diffusion de messages violents ou pornographiques susceptibles d'être vus par des mineurs[964]. Enfin, à peine de nullité, ce dispositif ne peut « *constituer une incitation à commettre ces infractions*[965] » et ne pourra être utilisé que par les agents ou officiers de police judiciaire habilités par le Procureur près de la Cour d'appel de Paris et affectés dans un service spécialisé. Seules la provocation à la preuve de l'infraction et la constatation de l'infraction sont autorisées.

Les services ou unités ayant la possibilité de mettre en place des « *cyber patrouilles* » ont été définis par un arrêté du 30 mars 2009 relatif à la répression de certaines formes de criminalité

[957] Code pénal art. 225-4-1 : « *La traite des êtres humains est le fait, en échange d'une rémunération ou de tout autre avantage ou d'une promesse de rémunération ou d'avantage, de recruter une personne, de la transporter, de la transférer, de l'héberger ou de l'accueillir, pour la mettre à sa disposition ou à la disposition d'un tiers, même non identifié, afin soit de permettre la commission contre cette personne des infractions de proxénétisme, d'agression ou d'atteintes sexuelles, d'exploitation de la mendicité, de conditions de travail ou d'hébergement contraires à sa dignité, soit de contraindre cette personne à commettre tout crime ou délit* ».

[958] Code pénal art. 225-5 : « *Le proxénétisme est le fait, par quiconque, de quelque manière que ce soit : 1° D'aider, d'assister ou de protéger la prostitution d'autrui ; 2° De tirer profit de la prostitution d'autrui, d'en partager les produits ou de recevoir des subsides d'une personne se livrant habituellement à la prostitution ; 3° D'embaucher, d'entraîner ou de détourner une personne en vue de la prostitution ou d'exercer sur elle une pression pour qu'elle se prostitue ou continue à le faire* ».

[959] Code pénal art. 227-18 : « *Le fait de provoquer directement un mineur à faire un usage illicite de stupéfiants est puni de cinq ans d'emprisonnement et de 100 000 euros d'amende* ».

[960] Code pénal art. 227-19 : « *Le fait de provoquer directement un mineur à la consommation excessive d'alcool est puni d'un an d'emprisonnement et de 15 000 € d'amende* ».

[961] Code pénal art. 227-21 : « *Le fait de provoquer directement un mineur à commettre un crime ou un délit est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende* ».

[962] Code pénal art. 227-22 : « *Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni 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 ou que les faits sont commis dans les établissements d'enseignement ou d'éducation ou dans* les *locaux de l'administration, ainsi que, lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux* ».

[963] Code pénal art. 227-23.

[964] Code pénal art. 227-24.

[965] Cour de cassation, chambre criminelle, 11 mai 2006, n° 05-84837 : « *le fait pour un agent de police ou un intermédiaire de se connecter sur Internet en se présentant comme un mineur recherchant des relations sexuelles constitue une provocation au délit de transmission de fichiers pédophiles et constitue également une provocation à l'infraction d'exploitation d'images pédophiles, entraînant ainsi la nullité des poursuites ainsi que de celle des aveux du prévenu* ».

informatique et à la lutte contre la pédopornographie. Sont alors autorisés « *à procéder aux actes définis par les articles 706-35-1 et 706-47-3 du code de procédure pénale, dans les conditions définies par le présent arrêté, les officiers et agents de police judiciaire affectés à l'un des services ou unités suivants : 1° Les offices centraux de police judiciaire ci-après désignés : a) L'office central pour la répression des violences aux personnes ; b) L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ; c) L'office central pour la répression de la traite des êtres humains ; d) L'office central pour la répression du trafic illicite des stupéfiants ; 2° Le service technique de recherches judiciaires et de documentation de la gendarmerie nationale ; 3° Les directions régionales et interrégionales de la police judiciaire ; 4° Les sections de recherches de la gendarmerie nationale* ».

Ces agents et officiers de police judiciaires sont alors tenus de suivre une formation spécifique dont l'organisation dépend des directions générales de la gendarmerie et de la police nationales. Une fois cette formation effectuée, ils sont habilités individuellement par le procureur général près la Cour d'appel de Paris au vu d'un dossier d'habilitation qui comprend la décision d'agrément du cyber patrouilleur et des attestations de formation aux cyber investigations sous pseudonyme. Cette habilitation peut être révoquée à tout moment par un autre procureur général. Enfin, les pseudonymes utilisés doivent faire l'objet d'une déclaration au SIAT[966] de la DCPJ[967] qui garantit une centralisation et renseigne les agents ou officiers de police judiciaire sur l'existence, ou, non d'un éventuel pseudonyme.

Concernant la mise en œuvre de l'enquête sous pseudonyme le CNAIP[968] s'organise au sein du STRJD[969] de la gendarmerie nationale de Rosny-sous-Bois en Seine-Saint-Denis. Composé d'agents et officiers de la police et la gendarmerie nationales ; ses missions sont précisées par l'arrêté du 30 mars 2009, il doit s'occuper : « *1° De centraliser et conserver, dans les conditions définies par l'article D. 47-8 du code de procédure pénale, les copies des contenus illicites mentionnés au 3° de l'article 706-35-1 et de l'article 706-47-3 du même code ; 2° De communiquer ces contenus illicites aux officiers et agents de police judiciaire mentionnés au*

[966] Service interministériel d'assistance technique.
[967] Direction centrale de la police judiciaire.
[968] Centre national d'analyse des images de pédopornographie.
[969] Service technique de recherches judiciaires et de documentation.

premier alinéa des articles 706-35-1 et 706-47-3 du même code, pour les besoins de leurs investigations et dans les conditions définies par l'article D. 47-9 ; 3° D'exploiter ces contenus, d'initiative ou à la demande de magistrats ou d'officiers ou d'agents de police judiciaire pour les besoins de leurs investigations, afin d'identifier par analyse et rapprochement les personnes et les lieux qui y sont représentés ». Les saisines ou transmissions de contenus et d'informations du CNAIP doivent être accompagnées du dossier complet de la procédure judiciaire comprenant le numéro de dossier de procès-verbal, de dossier parquet ou d'instruction en fonction de l'étape du procès. Conformément au Code de procédure pénale, le CNAIP est alimenté par des données qui proviennent des enquêtes judiciaires et qui sont issues de copies du contenu illicite transmise au CNAIP dans les meilleurs délais. Néanmoins un délai maximum de trois mois est prévu pour le contenu découvert lors des opérations d'enquête sous pseudonyme. La copie est réalisée par une personne qualifiée à la suite d'une réquisition judiciaire ou de la demande d'un expert judiciaire nommé par un juge d'instruction. Lorsque l'enquête le permet, les enquêteurs sont tenus de joindre au contenu l'ensemble des données techniques utiles à l'identification de la source. Il peut s'agir d'un darknet, d'un forum, d'un service de communication électronique, d'un *friend-to-friend*, d'un pseudonyme, d'une adresse en *.onion*, d'une adresse du Web visible, d'une adresse de courrier électronique, etc.

Bien évidemment, dans la mesure du possible, il est souhaitable qu'ils transmettent l'identité des auteurs de l'infractions et des victimes représentées dans le contenu litigieux. En effet, la mission première du CNAIP consiste à identifier victimes et auteurs d'infractions grâce à l'exploitation du contenu saisi au cours d'enquêtes judiciaires, mais aussi grâce aux prises de vue réalisées dans le cadre de ces enquêtes sur les lieux présumés de commission d'infractions. Des éléments tels qu'une chambre à coucher une cave, une salle de bain ou un jardin sont pris en compte afin d'effectuer des rapprochements. Dans le dessein d'obtenir le plus d'indices possibles sur les auteurs d'infraction, d'autres éléments techniques comme les séries, marques et modèles des appareils utilisés pour les prises de vue peuvent être transmis au CNAIP. Lors des identifications et rapprochements sont établis, le CNAIP les transmets simultanément à l'office central de police judiciaire compétent et aux magistrats et enquêteurs chargés des investigations.

Lors d'un échange international d'information, c'est l'office central compétent qui gère le contenu conformément à ce qui est prévu par l'article 24 de la loi n°2003-233 du 18 mars sur

la sécurité intérieure. Dès lors, l'office central compétent fait office d'intermédiaire entre l'autorité internationale et le CNAIP qui est en mesure de recevoir des demandes d'échanges de contenu provenant des organismes de coopération policière internationale. En France, lorsqu'il est informé de la commission éventuelle d'une infraction, le Ministère public est libre de poursuivre ou de ne pas poursuivre. Sauf si l'action publique s'est éteinte par l'effet du temps (§2).

§2) La prescription de l'action publique

L'action publique peut être définie comme « *l'activité procédurale exercée au nom de la société par le ministère public, pour faire constater par le juge compétent le fait punissable, établir la culpabilité du délinquant et obtenir le prononcé de la sanction établie par la loi*[970] » et la poursuite comme *« la saisine d'une juridiction d'instruction ou de jugement par l'exercice du droit de l'action publique*[971] ». Par conséquent, la prescription de l'action publique est l'extinction du droit de poursuivre par l'effet de l'écoulement d'un certain délai qui court dès le jour de la commission de l'infraction. Ce motif d'irrecevabilité de l'action publique est fondé sur le droit à l'oubli et la négligence de l'État qui perd son droit à agir pour ne pas avoir respecté les délais fixés par la loi (A). Sur le Darknet la prise en compte du point de départ du délai de prescription de l'action publique est délicate (B).

A) Le délai de la prescription de l'action publique

En principe[972] et depuis février 2017[973], le délai de l'action publique est de vingt ans pour les

[970] MERLE R. et VITU A., *Traité de droit criminel*, tome 2, Procédure pénale, Cujas, 5e éd., 2001, n°25, fascicule 20, Action publique et action civile – Action publique.
[971] GUINCHARD S. et BUISSON J., *Procédure pénale*, 9e éd., LexisNexis, page 983.
[972] Pour les crimes contre l'humanité l'article 213-5 du Code pénal dispose que : « *l'action publique relative aux crimes prévus par le présent sous-titre, ainsi que les peines prononcées, sont imprescriptibles* ».
[973] Avant la loi n°2017-242 du 27 février 2017 portant réforme de la prescription en matière pénale, le délai de la prescription de l'action publique était de dix ans pour les crimes, trois ans pour les délits et un an pour les contraventions.

crimes[974], six ans pour les délits[975] et un an pour les contraventions[976]. Le calcul du délai se fait de quantième à quantième jusqu'au dernier jour à minuit sans que le jour où l'infraction a été commise ne soit pris en compte[977]. Par exception, le législateur a institué des délais spéciaux et prévu des délais plus courts. A titre d'exemple, en matière d'infractions à la législation sur les stupéfiants[978] ou d'atteintes au mineur le délai est allongé[979].

Internet a des effets considérables car, contrairement au support papier, la divulgation de toute information sur ce réseau est sans limite dans l'espace, de manière horizontale mais aussi verticale grâce au Darknet, et dans le temps si une action n'est pas menée rapidement. En matière de presse le délai de prescription est en principe de trois mois[980], mais il peut être porté à un an en fonction de la gravité des faits[981]. L'article 65 de la loi du 29 juillet 1881 sur la liberté de la presse dispose que « *l'action publique et l'action civile résultant des crimes, délits et contraventions prévus par la présente loi se prescriront après trois mois révolus, à compter du jour où ils auront été commis ou du jour du dernier acte d'instruction ou de poursuite s'il en a été fait* ». Le régime d'un délai de prescription de l'action publique de trois mois peut poser des problèmes lorsque les délits de presse sont commis sur Internet. En effet, ce délai très court justifié par la protection de la liberté d'expression peut être préjudiciable aux victimes qui ne consultent pas nécessairement tous les sites Internet. Dès lors, le principe ne facilite pas la répression de ce genre de faits sur Internet et encore moins sur le Darknet où un contenu peut être publié à un moment donné sans que des associations puissent le consulter. C'est notamment le cas en matière de racisme ou de discrimination dans la mesure où il existe énormément de groupe de ce genre qui sévissent sur le Darknet où les contenus ne sont pas indexés. En somme, ce délai est clairement inadapté à l'ère du numérique.

Le législateur est intervenu afin de faire face à cette situation en instaurant la loi dite « *Perben*

[974] Code de procédure pénale art. 7 : « *L'action publique des crimes se prescrit par vingt années révolues à compter du jour où l'infraction a été commise* ».
[975] Code de procédure pénale art. 8 : « *L'action publique des délits se prescrit par six années révolues à compter du jour où l'infraction a été commise* ».
[976] Code de procédure pénale art. 9 : « *L'action publique des contraventions se prescrit par une année révolue à compter du jour où l'infraction a été commise* ».
[977] Cour de cassation, chambre criminelle, 7 juin 2006, Bulletin criminel n°161.
[978] Code de procédure pénale art. 706-31.
[979] Code de procédure pénale art.7 alinéa 3 et art. 8 alinéa 2.
[980] Articles 65 et 65-1 de la loi du 29 juillet 1881.
[981] Article 65-3 de la loi du 29 juillet 1881.

II[982] ». Cette dernière qui a vocation à s'adapter aux évolutions de la criminalité a allongé le délai de prescription de l'action publique pour les infractions dont la circonstance tient au mobile raciste. De plus, en 2008 le Sénat a adopté en première lecture une proposition de loi tendant à allonger le délai de prescription de l'action publique pour les diffamations, injures ou provocations commises par l'intermédiaire d'Internet[983]. L'idée est d'empêcher les abus sur Internet où les individus ont tendance à se lâcher en instaurant un régime plus stricte. Elle est rejetée mais le débat reste ouvert. Pour faire face à cette inadaptation de l'article 65 de la loi de 1881 sur la liberté de la presse, pas moins de quatre propositions ou projets de texte ont été présentés au Parlement, dont deux récemment avec la proposition de loi portant réforme de la prescription en matière pénale[984] et avec le projet de loi « *égalité et citoyenneté* » de 2016 qui n'ont pas abouti. Le 12 janvier 2017, un amendement[985] pour supprimer cette extension a également été déposé, en vain, par le député Patrick Block.

Toutefois, une réforme est toujours envisageable même si les médias ne veulent pas d'une rupture d'égalité entre la presse papier et le numérique. En effet, le Conseil Constitutionnel a précisé que *« la prise en compte de différences dans les conditions d'accessibilité d'un message dans le temps, selon qu'il est publié sur un support papier, ou qu'il est disponible sur un support informatique, n'est pas contraire au principe d'égalité*[986] ». Sans égard pour la durée de la prescription de l'action publique, le point de départ varie en fonction des circonstances de l'infraction (B).

B) Le point de départ de la prescription de l'action publique

Connaître le point de départ du délai de prescription de l'action publique d'une infraction commise sur le Darknet revient à se demander quel est le moment de la manifestation objectif d'une telle infraction. En effet, il est possible de considérer que ce genre d'infraction est une

[982] Loi n°2002-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
[983] https://www.senat.fr/rap/l08-060/l08-0601.html.
[984] L'article 65 de la loi de 1881 prévoyait cela : « *Lorsque les infractions auront été commises par l'intermédiaire d'un service de communication au public en ligne, sauf en cas de reproduction d'un contenu d'une publication diffusée sur support papier, l'action publique et l'action civile se prescriront par une année révolue, selon les mêmes modalités* ».
[985] Un amendement permet la modification d'un projet de loi ou d'une proposition de loi en cours de délibération. Il s'agit de soumettre le texte au vote d'une assemblée afin de le corriger, le compléter ou entièrement ou partiellement. En France, conformément à la Constitution, ce droit est réservé aux membres du gouvernement, de l'Assemblée nationale et du Sénat.
[986] Conseil constitutionnel, 10 juin 2004, n°2004-496 DC, Considérant n°14.

dissimulée ou occulte par nature.

En principe, conformément à l'article 7 alinéa 1er du code de procédure pénale, le délai de prescription de l'action publique démarre le jour de la commission de l'infraction ou de sa tentative lorsqu'elle est punissable. Toutefois, par exception, il se peut qu'il soit retardé. La loi le permet pour certaines infractions commises contre des mineurs et pour lesquelles le délai court à partir de la majorité de la victime[987]. La jurisprudence le permet aussi pour faciliter la répression de certaines infractions dites clandestines. Une infraction peut être clandestine par nature[988] lorsque l'auteur a agi à l'insu de la victime et clandestine par réalisation[989] lorsque l'auteur prend soin de dissimuler les faits en utilisant des artifices. Dès lors, le point de départ de la prescription de l'action publique est fixé au jour où l'infraction apparaît et peut être constatée.

Cette règle jurisprudentielle a été consacrée dans le code de procédure pénale à l'article 9-1 qui dispose que « *par dérogation au premier alinéa des articles 7 et 8 du présent code, le délai de prescription de l'action publique de l'infraction occulte ou dissimulée court à compter du jour où l'infraction est apparue et a pu être constatée dans des conditions permettant la mise en mouvement ou l'exercice de l'action publique, sans toutefois que le délai de prescription puisse excéder douze années révolues pour les délits et trente années révolues pour les crimes à compter du jour où l'infraction a été commise. Est occulte l'infraction qui, en raison de ses éléments constitutifs, ne peut être connue ni de la victime ni de l'autorité judiciaire. Est dissimulée l'infraction dont l'auteur accomplit délibérément toute manœuvre caractérisée tendant à en empêcher la découverte* » (1).

En outre, d'après l'article 9-2 du Code de procédure pénale l'action publique est éteinte si, dans le délai de prescription de l'action publique peut être interrompu par plusieurs actes tels qu'un procès-verbal, un acte d'enquête ou d'instruction ou encore un jugement (2).

[987] Code de procédure pénale art. 7 alinéa 3 et art. 8 alinéa 2.
[988] Cour de cassation, chambre criminelle, 7 mai 2002, Bulletin criminel n°108 à propos d'un abus de confiance ; Cour de cassation, chambre criminelle, 30 septembre 2008, Bulletin criminel n°197, à propos d'une atteinte à la vie privée.
[989] Cour de cassation, chambre criminelle, 16 décembre 2014, pourvoi n°14-82.939 à propos d'une prise illégale d'intérêts.

1. Les infractions dissimulées du Darknet

La procédure pénale a la lourde tâche de recherche continuellement un équilibre parfait entre les libertés individuelles et les nécessités de sécurité publique. La prescription de l'action publique ne déroge pas à la règle puisque même si son existence n'est pas remise en cause, elle peut être synonyme d'impunité.

Le point de départ du délai de prescription de l'action publique des infractions occultes et dissimulées est une thématique suscitant le débat. Avant la réforme de 2017 relative aux délais de prescription en droit pénal[990] c'est la jurisprudence qui en précisait les contours[991] en qualifiant, au gré des litiges, les délits et crimes relevant de ces catégorie. Le point de départ du délai de prescription de ce genre d'infractions[992] avait en effet été modifié par une jurisprudence *contra legem*[993] : il ne démarrait pas le jour de la commission des faits mais le jour de la découverte de l'infraction. Cette jurisprudence constante a été confirmée par l'assemblée plénière de la Cour de cassation dans une affaire d'infanticides[994] : « *Mais attendu que si, selon l'article 7, alinéa 1er, du Code de procédure pénale, l'action publique se prescrit à compter du jour où le crime a été commis, la prescription est suspendue en cas d'obstacle insurmontable à l'exercice des poursuites* ». D'aucuns ont dénoncé l'imprescriptibilité en cas d'obstacle insurmontable, notion qui n'a d'ailleurs pas été définie.

Depuis, le législateur est intervenu[995] afin de combler les lacunes de cette jurisprudence *contra legem* [996] qui s'appuyait sur les notions non définies de dissimulation et d'obstacle insurmontable. Dorénavant, les alinéas 4 et 5 de l'article 9-1 du code de procédure pénale

[990] Loi n° 2017-242 du 27 février 2017 portant réforme de la prescription en matière pénale.
[991] Cour de cassation, chambre criminelle, 7 juillet 2005, n°05-81.119 : « *Si la tromperie est une infraction instantanée, elle n'en constitue pas moins un délit clandestin par nature, en ce qu'il a pour but de laisser le contractant dans l'ignorance des caractéristiques réelles d'un produit et que, dès lors, le délai de prescription commence à courir du jour où le délit apparaît et peut être constaté dans des conditions permettant l'exercice de l'action publique* ».
[992] Cour de cassation, chambre criminelle, 5 septembre 2007, 07-80.263 : « *Le point de départ du délai de prescription du délit d'escroquerie, infraction instantanée, ne peut être retardé à la date à laquelle la partie civile en a eu connaissance* ».
[993] Dès 1935 la chambre criminelle reporte le point de départ de la prescription de l'action publique au jour où l'infraction a pu être constatée alors que les articles 637 et 640 du Code d'instruction criminelles de 1808 prévoit qu'il doit courir à compter du jour où l'infraction a été commise.
[994] Cour de cassation, Assemblée plénière, 7 novembre 2014, n° 14-83.739.
[995] Avec la loi n°2017-242 du 27 février 2017 portant réforme de la prescription de la matière pénale.
[996] Elle contredisait les articles 7 et 8 du Code de procédure pénale.

prévoient qu'est : « *occulte l'infraction qui, en raison de ses éléments constitutifs, ne peut être connue ni de la victime ni de l'autorité judiciaire ; est dissimulée l'infraction dont l'auteur accomplit délibérément toute manœuvre caractérisée tendant à en empêcher la découverte* ». Pour les infractions occultes ou dissimulées le point de départ de la prescription de l'action publique « *court à compter du jour où l'infraction est apparue et a pu être constatée dans des conditions permettant la mise en mouvement ou l'exercice de l'action publique* ». Toutefois, la portée de ce report est limitée puisque l'article prévoit que le délai de prescription ne peut pas « *excéder douze années révolues pour les délits et trente années révolues pour les crimes à compter du jour où l'infraction a été commise* ».

La notion d'infraction occulte par nature suppose une infraction dont l'un des éléments constitutifs présent un caractère clandestin ayant comme conséquence un retard de sa découverte. Celle d'infraction dissimulée suppose que l'auteur de l'infraction ait accompli délibérément des manœuvres pour dissimuler la découverte de celle-ci. Cette notion amène à des interrogations dans la mesure où cela peut s'appliquer à énormément de situations. Dès lors, les infractions dissimulées s'envisagent pour un nombre important d'infractions. Lorsqu'il donne son avis sur la réforme, le Conseil d'Etat[997] a précisé que cette qualification pouvait s'envisager pour toute infraction à la condition que l'auteur ait accompli une manœuvre pour la dissimuler. Toute infraction liée à l'informatique est donc susceptible d'entrer dans cette catégorie. On peut notamment penser à l'utilisation d'un Darknet ou d'un outil de chiffrement pour empêcher la découverte de l'infraction. Tel pourrait être le cas pour un pédophile qui enverrait du contenu pédopornographique chiffré via un Darknet. En outre, la loi définit les actes interruptifs de prescription (2).

2. Les actes interruptifs de prescription

« *Auparavant, à défaut de définition, il incombait au juge de les caractériser. L'élaboration d'un état des lieux avait été rendue nécessaire en raison de la casuistique opérée, laquelle mettait à mal les principes de sécurité juridique et de prévisibilité de la loi*[998] ».

[997] Conseil d'Etat, section intérieur, 1er octobre 2015, n°390335, avis sur la proposition de loi portant réforme de la prescription en matière pénale.
[998] MIHMAN A., Gazette du Palais, 7 mars 2017, n°10, page 14.

En effet, l'article 9-2 du Code de procédure pénale prévoit que « *le délai de prescription de l'action publique est interrompu par : 1° Tout acte, émanant du ministère public ou de la partie civile, tendant à la mise en mouvement de l'action publique, prévu aux articles 80, 82, 87, 88, 388, 531 et 532 du présent code et à l'article 65 de la loi du 29 juillet 1881 sur la liberté de la presse ; 2° Tout acte d'enquête émanant du ministère public, tout procès-verbal dressé par un officier de police judiciaire ou un agent habilité exerçant des pouvoirs de police judiciaire tendant effectivement à la recherche et à la poursuite des auteurs d'une infraction ; 3° Tout acte d'instruction prévu aux articles 79 à 230 du présent code, accompli par un juge d'instruction, une chambre de l'instruction ou des magistrats et officiers de police judiciaire par eux délégués, tendant effectivement à la recherche et à la poursuite des auteurs d'une infraction ; 4° Tout jugement ou arrêt, même non définitif, s'il n'est pas entaché de nullité* ».

Il faut donc un acte « *tendant effectivement à la recherche et à la poursuite des auteurs d'une infraction* » ce qui exclut à l'instar de la jurisprudence antérieure les simples plaintes. Il pourrait s'agir par exemple de la mise en place d'une enquête sous-pseudonyme pour interpeller des pédophiles du Darknet.

Enfin, l'article 9-3 du Code de procédure pénale a consacré légalement la solution qui avait été dégagée le 7 novembre 2014 par l'assemblée plénière de la Cour de cassation : « *tout obstacle de droit, prévu par la loi, ou tout obstacle de fait insurmontable et assimilable à la force majeure, qui rend impossible la mise en mouvement ou l'exercice de l'action publique, suspend la prescription* ». D'aucuns ont critiqué cet article qui aurait tué la prescription[999] en consacrant l'imprescriptibilité. Elle pourrait en effet s'envisager pour toute infraction, même minime, dès lors que serait caractérisé un obstacle de fait insurmontable rendant « *impossible la mise en mouvement ou l'exercice de l'action publique* ». D'aucuns craignent que la jurisprudence abuse de cette possibilité : « *On sait, en effet, comment, par une hostilité légendaire à la prescription, et dans des affaires autrement moins dramatiques, elle sait se montrer plus complaisante*[1000] ». En matière de cybercriminalité, une cyberattaque ne pourrait-elle pas être assimilée à la force majeure puisqu'il s'agit d'un événement irrésistible, extérieur et bien souvent imprévisible[1001] ?

[999] SAENKO L., D. 2014, page 2469.
[1000] MAYAUD Y., *Revue sciences criminelles 2014*, page 777.
[1001] « *La force majeure est un événement à la fois imprévisible, irrésistible (insurmontable) et extérieur aux personnes concernées* ».
Disponible à cette adresse : https://www.service-public.fr/particuliers/vosdroits/F33790.

La réponse semble être positive mais seule la jurisprudence permettra d'apporter des clarifications à ce propos.

Outre les règles de procédure pénales classiques, les enquêteurs sont confrontés à de nouveaux défis liés aux évolutions dans le domaine de la preuve numérique. L'arrestation des criminels et délinquants du Darknet suppose l'utilisation de techniques d'investigations plus ou moins adaptées aux réseaux dissimulés (Section 2).

SECTION 2
Un renforcement des techniques d'investigations

La loi n°2018-607 relative à la programmation militaire[1002] a été promulguée par Emmanuel Macron le 13 juillet 2018. Elle organise la programmation militaire pour les années 2019 à 2025 et révolutionne la lutte contre la cybercriminalité avec un chapitre III relatif à la cyberdéfense. Tout d'abord, l'article 34 de la loi étend la durée de conservation des données par l'ANSSI[1003]. Désormais, les données techniques « *recueillies directement par l'autorité nationale de sécurité des systèmes d'information en application du premier alinéa du présent article ou obtenues en application du deuxième alinéa de l'article L. 2321-3 ne peuvent être conservées plus de dix ans*[1004] ». Pour le député Jean-Jacques Briday[1005], « *une telle durée est suffisamment longue pour renforcer l'efficacité du dispositif, sans être déraisonnable s'agissant de données techniques. En effet, la "mémoire" et l'historique des évènements de sécurité passés sont essentiels à la prévention des cyber-attaques* ». Ainsi, « *plus la "bibliothèque" de données techniques sera fournie et accessible dans le temps, plus la résilience de notre système sera assurée* ». Ensuite, l'article 34 de la loi prévoit le déploiement de marqueurs techniques afin de « *détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés*[1006] ». Le marquage Web consiste à collecter les données et à en tirer des informations utiles pour la vente et la satisfaction du client. L'endrament légal du marquage Web a pour objectif la détection des « *événements susceptibles d'affecter la sécurité des systèmes d'information* ». Concrètement, ce sont les adresses IP d'un site Web piégé ou d'un serveur malveillant. L'adjectif « *susceptible* » permet d'envisager une surveillance en tant réel sans limite temporelle.

Un contrôle absolu des Etats suppose qu'il y ait la possibilité d'identifier tous les numéros de

[1002] https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000037192797.
[1003] L'autorité nationale de sécurité des systèmes d'information.
[1004] Article 34.
[1005] REES M., *La neutralité du Net s'invite dans la lutte contre la cybercriminalité*, 14 mars 2018. Disponible à cette adresse : https://www.nextinpact.com/news/106304-lpm-2019-2025-neutralite-net-sinvite-dans-lutte-contre-cybercriminalite.htm, [consulté le 14 mai 2018].
[1006] L'article L33-14 Code des postes et des communications électroniques est modifié : « *Pour les besoins de la sécurité et de la défense des systèmes d'information, les opérateurs de communications électroniques peuvent recourir, sur les réseaux de communications électroniques qu'ils exploitent, après en avoir informé l'autorité nationale de sécurité des systèmes d'information, à des dispositifs mettant en oeuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés* ».

téléphones et toutes les adresses IP. Le numérique ne permet pas encore cela et bon nombre de numéros de téléphones et d'adresses IP n'ont pas de véritable identité dans la mesure où il n'est pas possible de leur associer un nom ou un visage. Ainsi, la matière numérique pose énormément de difficultés pour l'application du droit pénal qui a dû s'adapter rapidement aux nouveautés générés par ce nouveau domaine. Internet a envahi la société, avec ses bons côtés et avec ses dérives.

Le Parlement et la jurisprudence ont ramé pour que l'arsenal pénal français s'applique au domaine du numérique et notamment à Internet. Mais ils ont bien plus du mal à appliquer les règles pénales au nouvel enjeu technologique que constitue le Darknet. Eu égard à cette procédure pénale inadaptée à l'anonymat et au chiffrement des données, l'identification de l'auteur de l'infraction est une épineuse tâche. En effet, la cybercriminalité qui se protège derrière un anonymat offre une capacité d'échange infinie et assure un sentiment d'impunité aux auteurs d'infractions. Ces derniers peuvent être des débutants en informatique ou alors très habiles techniquement. Dès lors, les enquêteurs doivent être formés pour avoir un niveau informatique au moins semblable, et les règles de procédure doivent adaptées à ces nouvelles pratiques.

Dans la recherche des preuves d'infraction les enquêteurs disposent d'instruments qui ne sont pas toujours adaptés au numérique et encore moins au Darknet qui offre de nombreuses possibilités technologique garantissant un anonymat ainsi que le chiffrement et l'effacement des données. Dès lors, en matière d'établissement de preuve la tâche des officiers et agents de police judiciaire est très ardue. Ces derniers interviennent en premier dans l'enquête judiciaire mais seuls les officiers de police judicaire sont en mesure de prendre sa direction ou d'établir des actes relevant de leurs prérogatives, comme une mise en garde-à-vue.

À titre d'exemple, pour les infractions dont la peine encourue est supérieure à deux ans d'emprisonnement un juge d'instruction peut porter atteinte à la confidentialité des correspondances privées en ordonnant la mise en place d'une interception téléphonique ou sur Internet. Le juge transmet ses directives sous forme de commission rogatoire[1007] aux enquêteurs

[1007] « *La commission rogatoire est une mission confiée par un juge à un autre juge, ou à un officier de police judiciaire, de procéder, en son nom, à des mesures d'instruction dans le cadre d'une enquête* ». Définition

qui effectuent les réquisitions auprès des acteurs techniques concernés[1008] et retranscrivent les échanges et conversations interceptés. Il peut s'agir d'une perquisition qui permet de visiter un domicile lorsqu'un magistrat ou un enquêteur souhaite trouver et préserver un élément matériel relatif à l'enquête. Ensuite, il peut s'agir d'une mesure de garde-à-vue qui permet de maintenir à la disposition des enquêteurs « *une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre un crime ou un délit puni d'une peine d'emprisonnement*[1009] ». Cette mesure de contrainte décidée par un officier de police judiciaire est très strictement codifiée. En principe, elle ne peut pas dépasser les 24 heures ou les 48 heures lorsque le Parquet autorise une prolongation, mais il y a des exceptions. Le temps de la garde-à-vue permet par exemple aux enquêteurs d'interroger un suspect ou d'analyser le contenu des ordinateurs saisis lors de perquisitions.

Le Parquet qui désigne les services dirigés par le Procureur de la République[1010] sous l'autorité du Garde des Sceaux est chargé d'observer l'ensemble des enquêtes judiciaires, de donner des directives particulières aux enquêteurs [1011] et de prendre une décision concernant les poursuites[1012]. Par ailleurs, lorsque l'enquête concerne un crime ou se relève trop compliquée, l'ouverte d'une information est nécessaire, et l'enquête confiée un juge d'instruction[1013]. Une information judiciaire ou une instruction est une procédure qui va permettre au juge d'instruction de rassembler des preuves à propos de la commission d'une infraction et de

disponible à cette adresse : https://droit-finances.commentcamarche.com/faq/4052-commission-rogatoire-definition.

[1008] Un opérateur Internet ou téléphonique.

[1009] Code de procédure pénale art. 62-2.

[1010] Le Parquet général désigne les services dirigés par le Procureur général dans une Cour d'appel ou une Cour de cassation.

[1011] Code de procédure pénale art. 41 alinéas 1 et 2 : « *Le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions à la loi pénale. A cette fin, il dirige l'activité des officiers et agents de la police judiciaire dans le ressort de son tribunal. Il peut, en outre, requérir tout officier de police judiciaire, sur l'ensemble du territoire national, de procéder aux actes d'enquête qu'il estime nécessaires dans les lieux où chacun d'eux est territorialement compétent* ».

[1012] Code de procédure pénale art. 40-1 : « *lorsqu'il estime que les faits qui ont été portés à sa connaissance en application des dispositions de l'article 40 constituent une infraction commise par une personne dont l'identité et le domicile sont connus et pour laquelle aucune disposition légale ne fait obstacle à la mise en mouvement de l'action publique, le procureur de la République territorialement compétent décide s'il est opportun : 1° Soit d'engager des poursuites ; 2° Soit de mettre en oeuvre une procédure alternative aux poursuites en application des dispositions des articles 41-1, 41-1-2 ou 41-2 ; 3° Soit de classer sans suite la procédure dès lors que les circonstances particulières liées à la commission des faits le justifient* ».

[1013] Code de procédure pénale art. 79 : « *L'instruction préparatoire est obligatoire en matière de crime ; sauf dispositions spéciales, elle est facultative en matière de délit ; elle peut également avoir lieu en matière de contravention si le procureur de la République le requiert en application de l'article 44* ».

décider du renvoi ou non du mis en examen devant la juridiction de jugement s'il y a suffisamment de charges. Il est compétent au premier degré d'instruction. Au second degré c'est la chambre de l'instruction qui l'est pour statuer sur les appels qui ont été formés contre les ordonnances du juge d'instruction. En tant que magistrat du Siège, le juge d'instruction est indépendant. Cette indépendance est garantie par l'article 64 de la Constitution qui assure leur inamovibilité. Dès lors, ils ne peuvent pas être révoqués, suspendus, mis à la retraite d'office sans garanties procédurales, et mutés, même avec avancement, sans le consentement[1014].

Ensuite, intervient le siège constitué d'autres magistrats que le juge d'instruction également réputés indépendants et dont la fonction est de juger les infractions. Ils sont alors chargés des juridictions de jugement que sont le Tribunal de police, le Tribunal Correctionnel et la Cour d'Assises. Le premier, situé dans les tribunaux d'instance, est chargé de juger les contraventions[1015], le deuxième situé dans les tribunaux de grande instance, juge les délits[1016] et enfin, la troisième, également placée au sein des tribunaux de grande instance, a vocation à traiter des affaires criminelles[1017] et a pour particularité de combiner des jurés civils et des magistrats professionnels. Lors des enquêtes, à l'instar de l'enquêteur ou du juge d'instruction, le magistrat peut être confronté à des difficultés techniques et faire appel au concours de spécialistes ou d'experts judiciaires, il s'agit de la criminalistique[1018].

L'analyse d'éléments de preuve numérique doit respecter une procédure stricte. Tout d'abord, l'enquêteur sépare en échantillons individuels tout objet placé sous scellé. Il peut ainsi séparer une carte SIM d'un téléphone portable. Il décrit ensuite chaque échantillon et son environnement, vérifie son fonctionnement et effectue une copie image de son contenu[1019]. Enfin, il interprète les données en ayant à l'esprit le contexte juridique des faits pour leur donner

[1014] Sauf en cas de sanction établie par le Conseil supérieur de la magistrature qui statue comme conseil de discipline pour les magistrats.
[1015] Code de procédure pénale art. 521 : « *Le tribunal de police connaît des contraventions de la cinquième classe* ».
[1016] Code de procédure pénale art. 381 : « *Le tribunal correctionnel connaît des délits. Sont des délits les infractions que la loi punit d'une peine d'emprisonnement ou d'une peine d'amende supérieure ou à égale à 3750 euros* ».
[1017] Code de procédure pénale art. 231 : « *La cour d'assises a plénitude de juridiction pour juger, en premier ressort ou en appel, les personnes renvoyées devant elle par la décision de mise en accusation* ».
[1018] « Ensemble des techniques mises en œuvre par la justice et les forces de police et de gendarmerie pour établir la preuve du crime et identifier son auteur », définition disponible sur Larousse.fr.
[1019] Les données peuvent être protégées par un code PIN ou par un composant électronique. Dès lors, l'enquêteur doit utiliser une technique permettant l'accès aux données tout en préservant le support original ne le préservant de toute modification.

un sens concret. Il existe des procédures particulières pour certaines preuves matérielles. Ainsi, l'analyse d'un disque dur suppose plusieurs étapes. Cela implique son démontage, son identification, la détermination de ses caractéristiques, la fabrication et l'analyse de son image[1020] et l'interprétation de son contenu. Une procédure existe également pour la vente de carte à puce contrefaite, un marché existant sur le Darknet. Ces cartes à puce contrefaites[1021] offrent plusieurs possibilités telles que l'accès gratuit à des chaînes cryptées ou la commande illimité d'objets sur des sites de vente. L'enquêteur va alors lire le programme de la carte grâce à un programmateur afin de connaître sa fonctionnalité.

Selon Mireille Ballestrazzi, directrice centrale de la police judicaire et ancienne présidente du comité exécutif d'Interpol[1022], « *nous sommes démunis face au Dark Web. La quasi-totalité de nos actions se concentrent sur le Web ouvert, qui est déjà très large. Le Dark Web est un vrai problème, car les malfaiteurs les plus pointus techniquement l'utilisent de plus en plus pour des actions liées au terrorisme, aux trafics de stupéfiants ou au blanchiment d'argent. Nous sommes démunis, car nous n'avons pas assez d'outils pour l'explorer. Par définition, on ignore ce qui se passe sur le Dark Web, donc il est très difficile de le combattre. Nous échangeons régulièrement avec le FBI pour mesurer la menace du Dark Web et pour mettre au point des outils technologiques qui nous permettront d'identifier les malfaiteurs qui y opèrent* ».

Un premier obstacle concerne la formation des personnels enquêteurs de l'intégralité de la chaîne, qui doivent faire face à un nombre élevé d'éléments matériels comportant des preuves numériques, notamment pour les enquêtes impliquant les réseaux Internet et Darknet. La formation doit concerner tous les agents et officiers de police judiciaire impliqués dans l'enquête, de la brigade de gendarmerie qui reçoit les plaintes et constate l'infraction, aux spécialistes du numériques, en passant par les unités spécialisées dans les enquêtes judiciaires : *« nous avons un budget consacré à la formation initiale. De nos jours, il est indispensable que*

[1020] L'image d'un disque dur est une fiche reprenant l'intégralité des données contenues sur le disque dur.
[1021] Article 79-1 de la loi n°86-1967 du 30 septembre 1986 relative à la liberté de communication : « *Sont punies de deux ans d'emprisonnement et de 30 000 € d'amende la fabrication, l'importation en vue de la vente ou de la location, l'offre à la vente, la détention en vue de la vente, la vente ou l'installation d'un équipement, matériel, dispositif ou instrument conçu, en tout ou partie, pour capter frauduleusement des programmes télédiffusés, lorsque ces programmes sont réservés à un public déterminé qui y accède moyennant une rémunération versée à l'exploitant du service* ».
[1022] ROLLAND S., La cybercriminalité est la nouvelle menace du XXIème siècle, 26 juillet 2015. Disponible à cette adresse : https://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html, [consulté le 16 avril avril 2017].

chaque policier ait un minimum de connaissances sur ce qu'est Internet, comment fonctionnent les réseaux sociaux, qui sont les grands opérateurs, ce qu'est la cybercriminalité... De nombreux adolescents sont victimes d'arnaques ou d'agressions sur les réseaux sociaux, et de plus en plus de personnes subissent des fraudes sur Internet, liées notamment à l'e-commerce. Si tous les policiers maîtrisent le b.a.-ba d'Internet, ils sauront mieux réagir et aiguiller les victimes. Pour l'heure, ce n'est pas suffisant mais cela va venir. Nous n'avons jamais assez de moyens, mais la France fait partie des pays les mieux dotés au monde[1023] ».

Ensuite, un autre écueil est le volume de données informatique qui doivent être interprétés dans un environnement singulier. La durée d'analyse du disque dur d'un suspect a augmenté parallèlement à l'augmentation de la taille des disques de stockage et a fortiori du nombre de fichiers à traiter et interpréter. La pratique suppose des frais et énormément de temps lorsqu'il s'agit de copier les données intéressantes du disque dur d'un ordinateur. Une fois les données d'un disque dur saisi, l'enquête judiciaire nécessite leur interprétation. Même si ce sont les logiciels les plus classiques qui sont les plus utilisés, beaucoup de logiciels utilisent des protocoles différents d'Internet. À titre d'exemple, un logiciel en relation avec l'usage Darknet comme Tor laisse des traces que les enquêteurs peuvent interpréter. L'existence de traces d'utilisation est due aux fonctionnalités du logiciel[1024], aux fichiers temporaires et aux informations de configuration du logiciel. Les enquêteurs sont censés maîtriser le fonctionnement des protocoles Internet et Darknet pour comprendre ces traces et interpréter les résultats de l'action volontaire de l'individu[1025] ou d'une fonctionnalité automatique[1026]. Pour les affaires de piratage, le délinquant ne facilite pas la tâche des enquêteurs puisqu'il va effacer un maximum de trace. S'il est identifié, les experts et enquêteurs tenteront de relier les constations faites sur l'ordinateur de la victime avec les informations retrouvées sur celui du suspect.

Enfin, les enquêteurs sont de plus en plus confrontés au chiffrement des données et à l'anonymat sur Internet et sur le Darknet. L'anonymat possible grâce au Darknet complique les enquêtes judiciaires actuelles. En effet, la conservation des données comme les preuves de connexions,

[1023] ROLLAND S., ibid.
[1024] Il peut s'agir de conservation de mails échangés, de carnet d'adresses, de groupes d'échange.
[1025] Il peut par exemple entrer une adresse *en .onion* pour accéder à une page du Darknet.
[1026] Un *pop-up* publicitaire peut révéler des informations sur l'historique de recherche de l'utilisateur.

les adresses IP est essentielle pour la réussite d'une enquête. Or, sur le Darknet les serveurs ne récoltent pas de données personnelles permettant l'identification des utilisateurs puisque des logiciels suppriment les traces, empêchent l'archivage et chiffrent les messages.

Comme méthodes d'investigations, les enquêteurs du Darknet ont la possibilité d'utiliser la perquisition de systèmes informatiques (§1) ainsi que d'autres méthodes plus adaptées au Darknet (§2).

§1) La perquisition des systèmes informatiques

D'après le site officiel de l'administration française[1027], « *la perquisition est la fouille d'un lieu en vue d'y trouver des preuves d'une infraction. Les preuves peuvent être des documents, des objets ou des fichiers informatiques. La perquisition ne concerne pas que les logements, mais tous les lieux privés. Elle peut se dérouler dans un garage ou dans les locaux d'une entreprise. La perquisition ne concerne pas que la personne officiellement suspectée : le domicile d'un témoin peut être perquisitionné* ».

Elle ne doit pas être confondue avec « la perquisition administrative[1028], décidée dans le cadre de l'état d'urgence[1029], ou la procédure de la visite, prévue par le dispositif de *sortie de l'état d'urgence* ». Il s'agit ainsi d'une mesure d'enquête ayant pour objet la recherche des preuves d'une infraction, au domicile de l'intéressé ou dans tous lieux où il peut être. Elle est prévue de

[1027] Définition disponible à cette adresse : https://www.service-public.fr/particuliers/vosdroits/F32326.
[1028] Conformément à l'article 11 alinéa 3 de la loi du 3 avril 1955, dans sa rédaction issue de la loi n°2017-258 du 28 février 2017, « *il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ». Ainsi, lorsqu'elles sont « *accessibles* » et « *disponibles* » les enquêteurs peuvent accéder aux informations et les copier depuis un appareil. Ils peuvent donc saisir les ordinateurs, les téléphones, les clés USB lors de perquisitions mises en place par la Police sans l'autorisation d'un juge. Les équipements saisis pourront être utilisés pour accéder aux données et aux conversations des suspects.
[1029] La perquisition administrative était donc possible hors du cadre judiciaire prévu par le Code de procédure pénal et décidée par un Préfet lorsqu'il constatait que le comportement était une « *menace pour la sécurité et l'ordre* publics ». Le régime d'état d'urgence, adopté à la suite des attentats du 13 novembre 2015, est resté en vigueur 719 jours jusqu'au 1er novembre 2017. Dans un contexte de lutte contre le terrorisme, il a permis de transférer des pouvoirs réservés à l'autorité judiciaire au ministère de l'intérieur et de transposer dans le droit commun des dispositions spéciales autorisées par ce régime d'exception.

manière générale pour l'instruction à l'article 94 du Code de procédure pénale[1030] et la délinquance organisées aux articles 706-89[1031] et 706-90[1032] du même code pour la criminalité et la délinquance organisées.

D'après la Convention de Budapest, la perquisition numérique permet de faciliter le déroulement de l'enquête dans le monde virtuel en permettant l'accès aux données informatiques, la captation de ces données et la conservation ou le stockage de ces données pour les utiliser comme preuves. Antérieurement à la Convention de Budapest, aucune disposition ne prévoyait la perquisition. Le législateur va insérer trois lois pour se mettre en conformité avec l'article 19 de la Convention qui prévoit donc la saisie, la perquisition et la captation de données[1033].

[1030] « *Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité, ou des biens dont la confiscation est prévue à l'article 131-21 du code pénal* ».
[1031] « *Si les nécessités de l'enquête de flagrance relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser que les perquisitions, visites domiciliaires et saisies de pièces à conviction soient opérées en dehors des heures prévues par l'article 59* ».
[1032] Si les nécessités de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, décider que les perquisitions, visites domiciliaires et saisies de pièces à conviction pourront être effectuées en dehors des heures prévues à l'article 59, lorsque ces opérations ne concernent pas des locaux d'habitation.
[1033] Article 19 - Perquisition et saisie de données informatiques stockées : « *1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire : a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'entendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :*
a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage informatique ; b. réaliser et conserver une copie de ces données informatiques ; c. préserver l'intégrité des données informatiques stockées pertinentes ; et
d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté. 4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2 ».

Ce sont les articles 707-89[1034] et 707-90[1035] du Code de procédure pénale qui la prévoient. En outre, l'article 57-1 du Code de procédure pénale[1036] dispose que « *les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Ils peuvent également, dans les conditions de perquisition prévues au présent code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial. S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code* ».

Cet article permet de perquisitionner les systèmes informatiques tandis que l'article 706-102-1 du Code de procédure pénale[1037] prévoit la mise en place d'un « *dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur*

[1034] « *Si les nécessités de l'enquête de flagrance relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser que les perquisitions, visites domiciliaires et saisies de pièces à conviction soient opérées en dehors des heures prévues par l'article 59* ».
[1035] « *Si les nécessités de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, décider que les perquisitions, visites domiciliaires et saisies de pièces à conviction pourront être effectuées en dehors des heures prévues à l'article 59, lorsque ces opérations ne concernent pas des locaux d'habitation* ».
[1036] Cet article a été institué par la loi n°2003-239 du 18 mars 2003 et modifié par la loi n°2016-731 du 3 juin 2016.
[1037] Créé par la loi dite LOPPSI 2 du 14 mars 2011 et modifié par la loi n°2016-731 du 3 juin 2016.

d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ». Il s'agit de la captation de données informatiques (A) qui se démarque de la perquisition informatique (B).

A) Les différents types de perquisitions informatiques

Concernant les actes d'enquêtes relatifs à l'informatique, le législateur a prévu de nouvelles dispositions précisant les pouvoirs des enquêteurs.

La perquisition « *permet à la police, à la gendarmerie ou à un magistrat de rechercher des preuves et des documents au domicile d'une personne. Cette mesure est encadrée par des règles précises et s'effectue sous le contrôle d'un officier de police judiciaire ou d'un juge*[1038] ».

La perquisition est informatique lorsqu'elle consiste à rechercher les éléments de preuve d'une infraction commise au moyen d'un ordinateur ou d'un objet connecté. Cette recherche peut donc supposer la perquisition de l'outil informatique au moyen duquel l'infraction a été réalisée, c'est la perquisition physique (1). Un autre type de perquisition est réalisable à distance via Internet, c'est la cyberperquisition ou perquisition à distance (2).

1. Les perquisitions et saisies informatiques physiques

L'article 57-1 du Code de procédure pénale dispose à l'alinéa 1er que « *les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ». Il s'agit donc de la perquisition informatique physique qui se fait directement sur le lieu de la perquisition. Elle permet l'accès aux données stockées sur l'ordinateur ou aux données se trouvant en ligne[1039] ou sur un autre ordinateur à la condition qu'elles soient accessibles à

[1038] https://www.service-public.fr/particuliers/vosdroits/F32326.
[1039] Sur un site ou sur un Cloud.

partir de l'ordinateur perquisitionné.

En outre, la loi n°2004-575 du 21 juin 2004 dite LCEN a modifié l'article 56[1040] du Code de procédure pénale qui dispose que (extrait) : « *Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l''officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal ».* Il s'agit donc de la saisie informatique physique qui a lieu directement sur l'ordinateur et qui permet d'y récupérer les *« données informatiques* ». En effet, dans le cadre d'une perquisition, les données informatiques peuvent être saisies. Dès lors, elles sont inventoriées et placées sous scellés. L'accès à distance aux données informatiques a ensuite été instauré par la Loi dite « *LSI* » (2).

2. Les perquisitions informatiques à distance

En France, la perquisition informatique informatique[1041] à distance existe depuis la loi n°2003-239 du 18 mars 2003 pour la sécurité intérieur[1042]. Cette dernière a inséré l'article 57-1 dans le Code de procédure pénale qui prévoit une telle possibilité. Ayant un coût énorme, elle est généralement réservée aux cas les plus graves comme le terrorisme, la pédophilie ou la criminalité organisée (a). Depuis la loi dite « *LOPPSI II* », la captation de données est également possible (b).

a) L'accès à des données distantes contenues sur un système informatique

L'alinéa 2 de cet article dispose qu'il est possible « *dans les conditions de perquisition prévues au présent code, (d') accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial* ». Ainsi, les enquêteurs pourront accéder depuis leurs locaux aux données

[1040] Avant cette modification législative l'article ne faisait pas référence aux données informatiques.
[1041] Le terme n'est pas approprié mais il s'agit de la traduction littérale de la Convention de Budapest.
[1042] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199.

stockées sur l'ordinateur d'un suspect situé n'importe où.

De plus, ces données pourront faire l'objet d'une saisie comme le prévoit le Code de procédure pénale : « *Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code*[1043] ».

La perquisition informatique de données a un réel intérêt depuis le « *Décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* » qui a instauré l'obligation de conservation des données de connexion d'un an pour les fournisseurs d'accès Internet. D'ailleurs, l'article 60-2 du Code de procédure pénale permet, dans le cadre d'une enquête de flagrance, à un officier de police judiciaire de demander les données contenues dans des « *systèmes informatiques ou traitement de données nominatives* » d'organismes tels que des administrations ou des opérateurs de communications électroniques. En outre, il convient d'étudier la captation de données informatiques instaurée en mars 2011 par la loi dite « *LOPPSI II »* (b).

b) La captation de données informatiques

Si l'article 57-1 du Code de procédure pénale autorise la perquisition dans un système informatique, la loi du 14 mars 2011 dite « *LOPPSI II* » prévoit quant à elle que le juge d'instruction peut, et après avis du procureur, autoriser la mise en place « *d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères*[1044] ». Le dispositif matériel utilisé peut être un équipement d'écoute directement installé sur l'ordinateur mais également un logiciel permettant l'accès à distance.

L'enquêteur peut alors fouiller à distance les données présentes sur un ordinateur connecté, lire

[1043] Code de procédure pénale art. 57-1 alinéa 4.
[1044] Code de procédure pénale art. 706-102-1.

les frappes clavier, activer la webcam, le micro et regarder des fichiers. Il pourra voir et enregistrer en temps réel et à distance le contenu informatique qui s'affiche sur un ordinateur même si les données proviennent d'un périphérique extérieur. La captation pourra se faire par l'introduction direct d'un « *mouchard* » sur le système ou par la transmission d'un mouchard à distance via Internet. L'objectif de ce dispositif est de permettre aux enquêteurs d'obtenir des informations à la source avant qu'elles soient chiffrés ou stockés sur un périphérique extérieur. Il s'agit donc d'un mécanisme procédural très intéressant pour lutter contre la cybercriminalité dissimulée.

Ces opérations très coûteuses ont vocation à être utilisées en matière de terrorisme et de criminalité organisée. Elles seront effectuées sous le contrôle et l'autorité d'un juge d'instruction qui devra, sous peine de nullité, préciser l'infraction qui nécessite le recours au dispositif[1045], la localisation précise, la durée de l'opération et le descriptif détaillé du système concerné. Elles pourront être prises pour une durée maximale de quatre mois, prorogeable une fois.

Les différents types de perquisition informatique permettent donc aux enquêteurs de pénétrer, à distance ou non, au sein d'un ordinateur dans le dessein d'y enregistrer, conserver et transmettre du contenu informatique. Ces perquisitions sont autorisées dans les mêmes cas que la perquisition classique et peuvent donc être mises en œuvre dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une instruction (B).

B) Le cadre juridique de la perquisition informatique

La perquisition informatique ne s'apparente pas à de simples constatations mais à une perquisition classique si bien qu'elle doit en respectée les formes (1). En outre, l'article 32 de la Convention de Budapest intitulé « *Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public* » prévoit qu'une « *partie peut, sans l'autorisation d'une autre Partie : a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données*

[1045] Si le dispositif permet de révéler des infractions autres que celles visées par la décision du juge, elles pourront quand même faire l'objet de poursuites.

informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique ». Ces dispositions ont été codifiées dans le code de procédure pénale à l'article 57-1 qui fixe le régime des perquisitions numériques[1046] (2).

1. Les modalités de mise en œuvre de la perquisition informatique

Seuls les officiers de police judiciaire sont habilités à l'effectuer après l'autorisation du du magistrat dirigeant l'enquête ou l'instruction, le procureur pour l'enquête de flagrance ou préliminaire, ou le juge d'instruction pour l'information judiciaire[1047]. Pour cette dernière, le juge d'instruction délivre une autorisation écrite appelée commission rogatoire. Elle est spéciale si elle n'autorise que la perquisition ou générale si elle autorise d'autres actes en rapport avec une affaire précise.

De plus, à l'instar de la perquisition classique, la perquisition informatique connaît des protections qui se manifestent par des limites matérielles et géographiques. Ainsi, en principe elle n'est possible qu'entre 6h et 21h[1048], requiert la présence de la personne concernée ou de son représentant ainsi que « *l'assentiment exprès de la personne chez laquelle l'opération*[1049] ». Elle ne doit permettre que la collecte des preuves relatives à l'infraction dont le juge est saisie et doit respecter les règles particulières pour les locaux des entreprises de presse et de communication[1050].

[1046] Alinéa 1 et 2 : « *Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles* à partir du *système initial ou disponibles pour le système initial. Ils peuvent également, dans les conditions de perquisition prévues au présent code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial* ».
[1047] Il s'agit d'une enquête menée par un juge d'instruction.
[1048] Il y a des exceptions en matière de terrorisme, de trafic de stupéfiants et de proxénétisme.
[1049] Code de procédure pénale art. 76 : « *Les perquisitions, visites domiciliaires et saisies de pièces à conviction ne peuvent être effectuées sans l'assentiment exprès de la personne chez laquelle l'opération a lieu. Toutefois cette article ne s'applique que pour les enquêtes préliminaires. En cas d'enquête de flagrance ou de commission rogatoire, l'assentiment express n'est pas exigé. De plus, pour l'enquête préliminaire, une autorisation de perquisition sans assentiment peut être délivrée par le Juge des libertés et de la détention sous certaines conditions »*
[1050] Code de procédure pénale art. 56-2.

Au-delà du cadre national, d'aucuns se sont demandés s'il fallait mettre en place un dispositif international qui permettrait les perquisitions informatiques transfrontalières pour la saisie de données. Une tel mécanisme semblait indispensable pour récolter rapidement les données informatiques qui sont souvent les seules preuves en matière de cybercriminalité dissimulée (2).

2. L'accès aux systèmes informatiques étrangers

L'alinéa 3 de l'article 57-1 du Code de procédure pénale autorise l'accès aux données stockées dans un système situé à l'étranger conformément à ce qui est prévu en matière de coopération : « *S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur* ».

Les perquisitions transfrontalières sont toujours délicates. En effet, l'accès aux données contenues sur des systèmes informatiques étrangers peut parfois faciliter une enquête mais sans le consentement du pays en question, il est impossible d'effectuer une perquisition. Pour les données non publiques et lorsque le consentement n'est pas donné, le Conseil de l'Europe estime logiquement que les perquisitions transfrontalières vont à l'encontre de la souveraineté des Etats. La France suit le même raisonnement et préserve les droits des accusés qui ne sont pas obligés de s'auto-incriminer. Evidemment, même si une telle situation est en faveur des délinquants qui profitent de « *cyber-paradis* », il s'agit de trouver un équilibre entre la sécurité des individus, et le respect des libertés fondamentales.

Une autre possibilité consisterait à demander en amont l'autorisation d'un magistrat compétent dans le ressort duquel la perquisition doit être effectuée. À l'instar d'une commission rogatoire, cela permettrait de combler l'absence de consentement de la personne qui possède les données.

Les États essaient d'adapter leur procédure pénale à la cybercriminalité qui n'est plus nouvelle et essaient parfois de prendre en compte la cybercriminalité dissimulée. Le caractère volatil des données et l'anonymat que le Darknet garantit nécessitent des méthodes d'intervention

différentes de celle de la criminalité classique et dans une moindre mesure de celles de la cybercriminalité visible (§2).

§2) Une nécessité constante d'adaptation

L'identification de l'auteur d'une infraction est indispensable pour qu'il y ait un procès et une peine. Cette affirmation peut sembler logique mais elle l'est bien moins lorsque les infractions sont commises sur le Darknet et Internet où règnent l'anonymat et l'invisibilité des auteurs. Les enquêteurs ont du mal à mettre un nom et un visage sur les criminels qui agissent sur le Darknet. En effet, concernant l'identification des auteurs d'infraction sur le Darknet, le filtrage effectué par les enquêteurs en ligne ne semble pas efficace dans la mesure où les auteurs d'infraction ont conscience d'être traqués. Dès lors, ils utilisent des techniques de chiffrement et d'anonymisation très difficiles à détecter (A). En somme, la loi donne plus de possibilités aux enquêteurs mais ne simplifie par leur tâche qui est de plus en plus ardue. Une lutte efficace contre la cybercriminalité dissimulée suppose alors quelques améliorations (B).

A) La question du chiffrement

Depuis 1990, la cryptologie a fait l'objet de nombreuses interventions législatives pour la définir, la promouvoir mais surtout l'encadrer. Défini par la loi du 29 décembre 1990[1051] sur la réglementation des télécommunications, le déploiement de la cryptologie concerne « *toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet* » et tout moyen permettant de préserver « *les intérêts de la défense nationale et de la sécurité intérieure ou extérieure à l'Etat* ».

D'autres dispositions ont été votées pour l'application de certaines dispositions de la loi du 29 décembre 1990 comme la loi du 26 juillet 1996[1052], ou pour donner des éléments techniques

[1051] Loi n°90-1170 du 29 décembre 1990 sur la réglementation des communications, JORF, 30 décembre 1990, pages 16 439- 16 446, article 28.
[1052] Loi n°96-659 du 26 juillet 1996, JORF, n°174, 27 juillet 1996, page 11 384.

comme les décret[1053] et arrêté[1054] du 17 mars 1999. Mais c'est la loi LCEN du 21 juin 2004 qui va plus apporter en la matière puisque son article 29 apporte une définition du moyen de cryptologie : *« tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, et permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité* ».

Une guerre entre pro et anti-chiffrement a été déclarée. Il s'agit d'encourager une telle technique en la limitant malgré tout pour en éviter les dérives. En effet, en janvier 2016, François Molins, procureur de la République de Paris, estime que huit smartphones « *n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé*[1055] ». Pourtant, Guillaume Poupard, directeur général de l'ANSSI[1056], n'est pas contre l'interdiction du chiffrement qui est « *une technologie défensive indispensable pou rassurer la sécurité des données personnelles*[1057] ». Son association préconise une solution intermédiaire consistant à utiliser des tiers de confiance. Les utilisateurs pourraient alors utiliser des systèmes de chiffrement très élaborés sous réserve d'un dépôt sous séquestre de leur clé de chiffrement auprès d'une institution certifiée par l'Etat. En cas d'atteinte à la sécurité de l'Etat, ou d'infraction grave, les autorités pourraient alors récupérer la clé de chiffrement pour accéder au contenu. Pour éviter ce genre de désagrément, des enquêteurs américains qui tentaient d'accéder à un iPhone ont demander à *Apple*[1058] de leur autoriser l'accès. Évidemment, le fabriquant a empêché une telle démarche afin de préserver la sécurité de ses appareils. Ainsi, *Apple* s'est opposé au FBI et à la CIA[1059].

[1053] Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable, JORF, n°66, 19 mars 1999, p. 4 051
[1054] Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie, JORF, n°66, 19 mars 1999, page 4052.
[1055] VANCE JR. MOLINS F., LEPPARD A., ZARAGOZA J., *When Phone Encryption Block Justice*, 11 août 2015. Disponible à cette adresse : https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0, [consulté le 23 décembre 2015].
[1056] Association des Réservistes du Chiffre et de la Sécurité de l'information.
[1057] CHEVALIER H., Chiffrement des données : la guerre est lancée, 28 janvier 2016. Disponible à cette adresse : https://www.franceinter.fr/societe/chiffrement-des-donnees-la-guerre-est-lancee, [consulté le 8 juillet 2016].
[1058] *Apple* est une entreprise multinationale américaine qui conçoit et commercialise des produits électroniques grand public, des ordinateurs personnels et des logiciels informatiques.
[1059] Définition disponible à cette adresse : https://fr.wikipedia.org/wiki/Apple#Sécurité_et_vie_privée.

En 2018, la plupart des enquêtes pénales repose, au moins en partie, sur des moyens technologiques comme les réseaux sociaux, les téléphones portables, la géolocalisation les SMS, l'accès aux fichiers d'un ordinateur, etc. Les utilisateurs protègent souvent l'accès à de tels outils et aux données qu'ils contiennent. En effet, le chiffrement permet de rendre illisible des données en cas d'interception. Or, le déchiffrement d'une clé de chiffrement classique n'est pas facile, a un coût très élevé et suppose l'intervention d'enquêteurs spécialisés ou d'experts. Un enquêteur peut également demander à un suspect de lui donner la clé de déchiffrement ou le code d'accès, mais encore faut-il qu'il tombe sur un individu assez coopératif pour donner des informations pouvant le compromettre. C'est la raison pour laquelle le législateur est intervenu en permettant le déchiffrement dans le cadre d'une procédure pénale (1) et en créant une obligation large de collaboration (2).

1. L'outil administratif de déchiffrement dans le cadre d'une procédure pénale

L'utilisation croissante du chiffrement par les particuliers et les entreprises permet d'assurer un niveau élevé de confidentialité et de contribuer à l'augmentation du nombre d'échange sur Internet et sur le Darknet. Les outils de chiffrement tels que des cartes mères permettant de chiffrer et protéger les fichiers sont désormais accessibles au grand public grâce à de nouveaux fournisseurs. Logiquement, cette généralisation du chiffrement handicape fortement les enquêteurs judiciaires. Pour faciliter les investigations judiciaires, le législateur tente de trouver de nouvelles solutions en matière de techniques d'enquête et de formations.

Instauré par la loi du 15 novembre 2001 relative à la sécurité intérieure[1060], l'article 230-1 du Code de procédure pénale dispose que « *sans préjudice des dispositions des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de*

[1060] Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, JORF, n°266, 16 novembre 2001, page 18 215, texte n°1, article 31.

cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire. Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre ». Pour ce faire, il faut que l'affaire ait un lien avec la criminalité organisée ou avec le terrorisme.

Concernant la procédure de mise au claire des données chiffrées qui supposerait des moyens *« couverts par le secret de la défense nationale* », l'article 230-2 du code pénal prévoit que « *la réquisition écrite doit être adressée à un organisme technique soumis au secret de la défense nationale, et désigné par décret, avec le support physique contenant les données à mettre au clair ou une copie de celui-ci* ». Avant le 24 avril 2017, le juge transmettait à l'OCLCTIC les données à déchiffrer. L'office travaillait en lien avec le Centre technique d'assistance[1061] « *pour servir d'intermédiaire avec les services disposant de moyens plus confidentiels*[1062] ».

Désormais, c'est l'Agence nationale des techniques d'enquêtes numériques judiciaires qui met « *en œuvre la plateforme nationale des interceptions judiciaires* » et qui est compétente pour les « *techniques d'enquêtes numériques*[1063] ». Pour éviter une telle procédure ayant un coût très élevé, le législateur a mis en place la pénalisation du suspect qui refuse de remettre la clé de déchiffrement (2).

2. Une obligation large de collaboration

L'article 434-15-2 du Code pénal punit « *de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre*

[1061] Le CTA est créé en 2002 au sein du ministère de l'Intérieur, Décret n°2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n°2001-1062 du 15 novembre 2001 relative à la quotidienne et portant création du Centre technique d'assistance, JORF, n°186, 10 août 2002, page 13 173, texte n°3.
[1062] FREYSSINET (E.), *La cybercriminalité en mouvement*, Lavoisier, Cachan, 2012, page 137.
[1063] Décret n°2017-614 du 24 avril 2017 portant création d'un service à compétence nationale dénommé « *Agence nationale des techniques d'enquêtes numériques judiciaires* » et d'un comité d'orientation des techniques d'enquêtes numériques judiciaires, JORF, n°97, 25 avril 2017, texte n°27, article 2.

un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale. Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende ».

Cette disposition a été instaurée par la loi du 15 novembre 2001 sur la sécurité quotidienne tandis que la loi LCEN du 21 juin 2004[1064] a alourdi les peines[1065] à propos de l'utilisation de la cryptologie pour la commission d'un crime ou un délit. Toutefois, une telle disposition semble aller à l'encontre du droit de ne pas s'auto-incriminer. Ce dernier est inspiré du droit américain, plus précisément du 5ème Amendement de la Constitution[1066]. Il a été consacré par la jurisprudence de la Cour EDH qui à l'instar du droit au silence[1067], l'assimile aux exigences du procès équitable[1068]. Le 6 mars 2015 l'Assemblée plénière de la Cour de cassation a repris le même principe[1069]. Déjà, en 2001, lorsque l'article 434-15-1 du Code pénal a été adopté, la CNIL estimait qu'il s'agissait d'une disposition contraire au droit de ne pas d'auto-incriminer.

Le 10 janvier 2018 la chambre criminelle de la Cour de cassation[1070] a renvoyé au Conseil constitutionnel une QPC concernant cet article[1071] qui a pris une décision le 30 mars 2018[1072] :

[1064] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF, n°143, 22 juin 2004, page 11 168, texte n°37.
[1065] L'article 132-79 du Code pénal issu de la loi LCEN aggrave les peines encourues « *lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été utilisé pour commettre un crime ou un délit ou pour en faciliter la commission* » ;
[1066] « *Not shall be compelled in any criminal case to be a witness against himself* » ; « *nul ne pourra, dans une affaire criminelle, être obligé de témoigner contre lui-même* ».
[1067] L'article 63-1 du Code de procédure pénale accorde au gardé à vue le « *droit, lors des auditions (…) de faire des déclarations, de répondre aux questions posées ou de se taire* ».
[1068] CEDH, Décision « *Funke contre France »* du 25 février 1993.
[1069] Cour de cassation, Assemblée plénière, 6 mars 2015, n° 14-84.339.
[1070] Https://www.courdecassation.fr/jurisprudence_2/qpc_3396/3478_10_38354.html.
[1071] « *Les dispositions de l'article 434-15-2 du code pénal en ce qu'elles ne permettent pas au mis en cause, auquel il est demandé la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit : de faire usage de son droit au silence ; et du droit de ne pas s'auto-incriminer ; sont-elles contraires au principe du droit au procès équitable prévu par l'article 16 de la Déclaration des Droits de l'homme et du Citoyen du 26 août 1789, au principe de la présomption d'innocence, duquel découle droit de ne pas s'auto-incriminer et le droit de se taire, prévu à l'article 9 de la Déclaration des Droits de l'Homme et du Citoyen du 26 août 1789 ?* »
[1072] DERIEUX E., *Déchiffrement forcé d'un moyen de cryptologie*, La revue européenne des médias et du numérique, n°46-47 Printemps – été 2018.

« *Le premier alinéa de l'article 434-15-2 du Code pénal, dans sa rédaction résultant de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, est conforme à la Constitution*[1073] ». Par conséquent, le Conseil constitutionnel a estimé que l'article 434-15-2 du Code pénal était conforme au texte suprême qu'est la Constitution. Dès lors, l'individu qui refuse de remettre aux autorités la convention secrète de déchiffrement d'un moyen de cryptologie commet un délit. Les Sages ne reconnaissent ni l'atteinte à la vie privée, ni l'atteinte aux droits de la défense. Toutefois, la mesure n'est envisageable que si l'individu a connaissance d'une infraction liée à un outil juridique utilisant un moyen de cryptage. Pour le Conseil constitutionnel une telle mesure d'enquête n'a « *pas pour objet d'obtenir des aveux de sa part et n'emportent ni reconnaissance ni présomption de culpabilité mais permettent seulement le déchiffrement des données cryptées. En outre, l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit. Enfin, ces données, déjà fixées sur un support, existent indépendamment de la volonté de la personne suspectée* ».

Toutefois, il semblerait que l'État ait perdu l'avantage qu'il avait en matière de chiffrement et qu'il soit dépassé. Ainsi, le contournement des techniques de chiffrements et la cryptanalyse sont en train de de venir une prédominante de la criminalistique dans le domaine de la preuve numérique (B).

B) Des améliorations nécessaires

En France, la prolifération des textes a apporté énormément de modifications et a compliqué le travail des hommes et femmes de terrain qui luttent contre la cybercriminalité. La surabondance des lois et leur éparpillement handicapent la répression de certaines infractions qui ne sont pas poursuivies. Dès lors, une simplification et un rassemblement des normes semble impératif pour faciliter le travail des enquêteurs et garantir de meilleures poursuites. Toutefois, dans cette lutte contre la cybercriminalité dissimulée certaines procédures sont inefficaces (1) et les moyens insuffisants (2).

[1073] Décision n°2018-696 QPC du 30 mars 2018. Disponible à cette adresse : https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm.

1. Des procédures inefficaces

Les mesures de géolocalisation possibles lors de l'enquête de flagrance ou préliminaire, et lors de l'instruction ne sont pas efficaces sur le Darknet (a), tout comme le déréférencement (b).

a) La géolocalisation

La géolocalisation est possible pour les enquêtes et informations judiciaires portant sur des infractions punies d'au moins cinq ans d'emprisonnement, des infractions prévues au livre II du Code pénal et punies d'aux moins trois ans d'emprisonnement, ou des délits de recel de crime et d'évasion prévus respectivement aux articles 434-6 et 434-27 du code pénal. Elle est également possible pour les enquêtes ou instructions en recherche des causes de la mort et des blessures, d'une personne en fuite et des causes de la disparition.

Pour les nécessités de la procédure, l'article 230-32 du Code de procédure pénale prévoit que la géolocalisation « *d'une personne* » peut être utilisée « *à l'insu de celle-ci* ». Le texte ne vise pas un suspect, mais « *une personne* » sans apporter de préciser si bien qu'une telle mesure est envisageable à l'encontre de toute personne. De plus, le texte prévoit la géolocalisation « *d'un bien ou de tout autre objet* » sans apporter non plus de précision. Dès lors, des objets comme des téléphones portables, des ordinateurs ou des véhicules équipés d'un GPS pourraient être géolocalisés.

L'article 230-33 du code de procédure pénale prévoit des règles différentes en fonction du cadre procédural dans lequel elle est mise en place. Pour les enquêtes et informations judiciaires portant sur des infractions punies d'au moins cinq ans d'emprisonnement, les infractions prévues au livre II du code pénal et punies d'aux moins trois ans d'emprisonnement, ou les délits de recel de crime et d'évasion prévus respectivement aux articles 434-6 et 434-27 du code pénal, le procureur de la République peut autoriser une mesure de géolocalisation pour un maximum de quinze jours consécutifs. Au delà c'est le juge des libertés et de la détention qui l'autorise. Pour l'instruction c'est le juge qui prend la décision pour une durée de quatre mois renouvelable sans limitation. En tout état de cause c'est le magistrat qui l'autorise qui doit contrôler sa mise en œuvre.

Il est opportun de se demander si une telle mesure à finalité probatoire pourrait avoir un intérêt pour une infraction commise sur le Darknet. La réponse est négative dans la mesure où les Darknautes utilisent des logiciels permettant d'être localisé en même temps à plusieurs endroits dans le monde. Le déréférencement est également inutile pour les agissements du Darknet (b).

b. Le déréférencement

En France et en Europe, la protection de la vie privée est une priorité. En Effet, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés assure aux internautes que leurs données ne sont pas conservées par les sites Internet. Dès 2009, « le droit à l'oubli numérique » est mis en avant par Nathalie Kosciusko-Morizet, ancienne secrétaire d'Etat chargée de la Prospective et du Développement de l'économie numérique.

La protection de la vie privée est garantie par la Cour de justice de l'Union européenne qui a rendu une décision sur le « *droit à l'oubli* ». Dans sa très riche décision du 13 mai 2014 la CJUE consacre l'existence de ce droit qui consiste en une obligation pour les moteurs de recherche qui sont tenus de supprimer, à la demande des internautes, le contenu lié à leur nom dans une liste de résultats proposés à la suite d'une recherche. Ce droit est la conséquence inévitable de la tentative de conciliation de plusieurs droits fondamentaux divergents. Le droit à l'oubli permet à un internaute de demander que d'anciennes données le concernant soient effacées. Sont compris le déréférencement et l'effacement des données.

Le déréférencement est défini comme « *l'opération par laquelle un distributeur supprime un produit des références qu'il commercialise*[1074] ». A propos d'Internet, *« il s'agit de supprimer certains résultats figurant dans la liste affichée par un moteur de recherche après une requête effectuée à partir du nom d'une personne. Cette suppression ne signifie pas l'effacement de l'information sur le site internet source. Le contenu original est inchangé et est toujours accessible via les moteurs de recherche en utilisant d'autres mots clés de recherche ou en allant directement sur le site à l'origine de la diffusion*[1075] ». L'effacement quant à lui consiste pour

[1074] Définition Larousse, disponible à cette adresse :
https://www.larousse.fr/dictionnaires/francais/déréférencement/23999.
[1075] https://www.cnil.fr/en/node/15816.

un utilisateur d'Internet à demander au modérateur d'un site d'effacer les données, photos ou textes le concernant.

Dès lors, si un internaute français effectue ce genre de demande auprès de *Google* pour une information le concernant, cette information ne sera plus accessible en France et dans l'Union européenne[1076]. Néanmoins, pour la CNIL, qui lutte en matière de protection des données personnelles, les moteurs de recherche ne respectent pas la décision de la CJUE puisqu'ils devraient appliquer le déréférencement à tous les domaines, même ceux rattachés à un pays extérieur à l'Union européenne : « *Pour la CNIL, ces données sont toujours visibles pour les curieux, qui peuvent simplement simuler leur adresse IP en prétendant effectuer une recherche depuis un pays non membre de l'UE pour les obtenir. La CNIL estime que le droit à l'oubli deviendra sans valeur s'il n'est pas appliqué universellement*[1077] ».

À une époque où les réseaux règnent en maître, des mesures doivent être mises en place pour éviter certaines menaces comme le terrorisme. Ainsi, le déréférencement pourrait être utilisé pour les sites illégaux terroristes qui aspirent à recruter des membres à distance grâce à une propagande efficace. Il serait même possible de l'envisager pour tous les sites Internet illégaux. Néanmoins, les sites terroristes ou pédopornographiques du Darknet ne sont pas référencés si bien qu'une telle mesure n'a pas vocation à s'appliquer sur le Darknet. Quant à l'effacement du contenu, il n'est pas envisageable dans la mesure où les réseaux Darknet sont décentralisés. En somme, les nouvelles procédures qui aspirent à s'appliquer pour le Web visible, semblent inefficaces sur le Darknet si bien qu'un renforcement des moyens a été nécessaire (2).

2. Un renforcement des moyens

Les techniques d'investigation sur Internet et sur le Darknet sont d'actualité, notamment depuis que la France est une cible prioritaire du terrorisme. Toutefois, même si la lutte contre la cybercriminalité repose sur des services spécialisés extrêmement compétents, les effectifs ne sont pas suffisants et aucun service n'est consacré qu'à la cybercriminalité dissimulée (a). En

[1076] Elle le sera toujours à partir de noms de domaines rattachés à des pays hors Union européenne.
[1077] LE CALME S., *CJUE : le droit à l'oubli devrait-il être appliqué au niveau mondial ? Google estime que non*, le 11 septembre 2018. Disponible à cette adresse : https://www.developpez.com/actu/223732/CJUE-le-droit-a-l-oubli-devrait-il-etre-applique-au-niveau-mondial-Google-estime-que-non-et-avance-ses-arguments-devant-la-Cour/.

outre, un ajustement de l'arsenal juridique est nécessaire (b).

a) Des effectifs insuffisants

L'enquête à l'ère du numérique est une enquête qui reste classique dans le respect des principes de la preuve pénale, tout en étant confrontée au numérique et à tous les objets connectés. Toutes les sources qui vont être recueillies seront susceptibles d'être changées en indice puis en charge. Les preuves peuvent donc être très variées, très diversifiées ce qui semble être un avantage pour les enquêteurs. Néanmoins, cette diversité de la preuve est minorée par un temps d'exploitation des indices, par la complexité des enquêtes et par la masse des affaires due au nombre élevées de victimes. Dès lors, il faut du personnel qualifié ce qui suppose du temps pour la formation, et du temps pour le travail sur le terrain. En outre, les éléments de preuves se trouvent partout à travers le monde, et peuvent disparaître d'un simple clic.

Est-ce que la justice peut se permettre de dépenser autant de temps et autant d'argent pour les dossiers cybercriminels et être à la hauteur des assaillants. La réponse semble être négative. En matière de cybercriminalité, la preuve est limitée par des dossiers volatils, par la transnationalité, par le défaut de formation des enquêteurs et par l'hyper protection des données à caractère personnel, alors que les cybercriminels ont du temps, de l'argent et profitent de l'absence de frontière. En somme, l'égalité des armes n'existe pas en la matière.

Les enquêteurs se heurtent à des difficultés financières et administratives. À titre d'exemple, la conservation des données par les opérateurs est d'un an en France alors qu'elle est de trois mois dans certains pays. Dès lors, le gel des données est inutile lorsqu'elles ne sont pas conservées suffisamment longtemps. Au sein de la Police nationale[1078] opère *« l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication qui dépend de la Sous-direction de lutte contre la cybercriminalité* » et pour la Gendarmerie nationale c'est le « *centre de lutte contre les criminalités numériques du Service Central du Renseignement Criminel* ». La Brigade d'enquête sur les fraudes aux technologies de l'information est également compétente pour Paris et la petite couronne[1079]. Enfin, en 2014, le Parquet de Paris

[1078] https://www.gouvernement.fr/risques/cybercriminalite.
[1079] 75, 92, 93 et 94.

a créé un pôle cybercriminalité qui dispose depuis 2016 d'une compétence nationale[1080].

Toutefois, les ressources humaines et financières sont insuffisantes. Le Parquet de Paris ne dispose que de quatre magistrats formés. Même problème pour les enquêteurs puisque les ressources sont distribuées au niveau national à l'OCLCTIC qui dispose d'une cinquantaine de personnes et à la gendarmerie qui dispose du même nombre de personnes pour agir sur l'ensemble du territoire français. Seule Paris et sa petite couronne bénéficient de moyens relativement suffisant puisque la BEFTI est composée de vingt enquêteurs et de cinq assistants techniques. Ainsi, sur l'ensemble du territoire, selon De Franco, enquêteurs à la BEFTI, il y aurait moins d'un millier de personnes spécialisées pour lutter contre la cybercriminalité. Compte tenu des 19,3 millions de victimes de la cybercriminalité en 2017[1081], il y aurait un enquêteur pour plus de 19 000 infractions. En somme, les moyens ne sont pas suffisants pour la cybercriminalité classique alors comment espérer une lutte efficace en matière de cybercriminalité dissimulée.

En outre, la marge de manœuvre de l'OCLCTIC, le principal organisme de la police nationale qui lutte contre la cybercriminalité, est limitée par d'autres services qui agissent en parallèle. Par exemple, pour la pédophilie, c'est l'Office central de répression des violences aux personnes qui est compétent. Le fait qu'il ne s'agisse pas d'un organisme interministériel limite son pouvoir d'action en matière de coordination avec d'autres services de lutte contre la cybercriminalité. De plus, la lutte est divisée entre plusieurs services spécialisés sans qu'une hiérarchie claire n'ait été établie.

Il serait judicieux de créer un service interministériel qui aurait vocation à enquêter sur toutes les infractions commises sur Internet et sur le Darknet. Cette délégation interministérielle serait alors composée d'un Président nommé par le Premier ministre pour une durée déterminée qui serait chargé de mettre en place des plans de luttes contre la cybercriminalité. Il travaillerait en liaison avec le ministère de la Justice afin de mettre en place des projets de lois relatifs à la cybercriminalité, veillerait à l'harmonisation des textes de loi, serait un lien entre les différents

[1080] *Le parquet de Paris renforce son arsenal contre la cybercriminalité*, 2 septembre 2014. Disponible à cette adresse : https://www.01net.com/actualites/le-parquet-de-paris-renforce-son-arsenal-contre-la-cybercriminalite-625774.html, [consulté le 2 février 2016].
[1081] *Rapport Norton sur les cyber risques*, Edition 2017, op. cit. p. 22.

services de police et de gendarmerie spécialisés ainsi qu'avec les acteurs du secteur privé comme les fournisseurs Internet et aurait un pouvoir de représentation au niveau supranational.

De plus, il serait judicieux de créer un service spécialisé chargé spécifiquement de la cybercriminalité dissimulée. En ce sens, des enquêteurs auraient la possibilité de n'aborder que les infractions commises sur le Darknet grâce à des moyens d'investigation améliorées et à une formation accrue. Outre les besoins relatifs aux effectifs, un ajustement constant de l'arsenal juridique est nécessaire lorsqu'il s'agit de lutter contre la cybercriminalité dissimulée qui ne cesse d'évoluer. L'efficacité d'une telle lutte Darknet suppose un encadrement plus restreint des connexions (b).

b) Un encadrement plus restreint des connexions

La suspension du droit d'accès à un service de communication au public en ligne en tant que peine complémentaire était prévue par la loi HADOPI, après de longs débats elle a été supprimée par décret le 8 juillet 2013[1082] (∂). Il convient également d'envisager la limitation de l'accès libre à Internet (ß).

∂) La suspension du droit d'accès à un service de communication au public en ligne

L'encadrement du droit d'accès à Internet pourrait être utile pour lutter contre les pédophiles qui agissent sur Internet et qui sont la plupart du temps bien intégrés dans la société. En effet, en lui interdisant la connexion à son smartphone, à son ordinateur ou à sa tablette le pédophile serait clairement limité puisqu'il n'aurait plus la possibilité de visionner son contenu. Une telle démarche l'amènerait à être dénoncé par les personnes se trouvant autour. Cela supposerait une forte collaboration entre l'Etat et les fournisseurs d'accès Internet mais également avec les opérateurs téléphoniques qui fournissent la 4G.

Cette mesure qui aurait également vocation à s'appliquer pour d'autres infractions comme le

[1082] Décret n°2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévues à l'article L.331-21 du Code de la propriété intellectuelle, JORF du 9 juillet 2013.

terrorisme sur Internet ou encore le trafic de stupéfiants pourrait être envisagée sans porter atteintes aux libertés individuelles puisque le Conseil Constitutionnel considère que le droit d'accès à Internet n'est pas un droit de l'homme mais qu'il résulte uniquement de la liberté de communication. Or, même si cette dernière à valeur constitutionnelle, une telle mesure n'aurait vocation à s'appliquer que pour des infractions graves menaçant les citoyens et les intérêts de l'État. Une telle suspension du droit d'accès à un service de communication au public en ligne ne serait efficace que si elle était associée à une limitation de l'accès à Internet (ß).

ß) La limitation de l'accès libre à Internet

D'après le point 15 de l'article 32 du Code des postes et des télécommunications un opérateur est « *toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques* ». Dès lors, il peut s'agir d'un endroit public comme un restaurant offrant une borne Wifi, ou d'un cybercafé. En ce sens, l'article 34-1 du Code des postes et des télécommunications 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* ».

Ce cadre législatif a été nécessaire en raison de l'apparition des points d'accès Wifi et des cybercafés qui ont contribué à l'accessibilité d'Internet. Ces points de connexion permettent un anonymat utilisable par les cybercriminels. En effet, il est possible d'imaginer un hackeur qui se rendrait dans un restaurant sans caméra avec un ordinateur neuf et jamais connecté pour y installer Tor et commettre des infractions avec un profil créé pour l'occasion. Même chose s'il se rendait dans un cybercafé. Son anonymat quasi-total lui permettrait d'agir en toute impunité. En effet, l'adresse IP de l'ordinateur ne serait pas celle de l'utilisateur si bien qu'elle ne pourrait pas être utilisée pour le retrouver.

Ce faisait, un contrôle efficace et systématique des clients est nécessaire. Cela semble facile pour les cybercafés puisqu'il suffirait que les patrons demandent la carte d'identité des clients mais qu'en est-il pour les lieux publics où toute personne ayant un appareil doté de la technologie Wifi peut se connecter à un point d'accès Wifi public. En France et dans de

nombreux pays, ils sont très nombreux. Ils se trouvent dans les aéroports, les restaurants, les hôtels ou les bars. Les cybercriminels les apprécient fortement dans la mesure où ils permettent une connexion anonyme. Or, le cadre légal n'est pas toujours respecté par ces opérateurs qui ne conservent pas toujours les données. Pourtant, l'article 32 du code des postes et des télécommunications ne fait pas de différence entre les opérateurs qui proposent une connexion à titre professionnel et ceux qui en propose une dans le cadre d'une activité afférente, et l'article 34-1 du même code soumet l'ensemble des opérateurs aux obligations légales[1083]. Ainsi, l'article 34-1 du code des postes et des télécommunications prévoit que « *les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes* ».

Le seul critère permettant d'établir s'il s'agit d'un opérateur et donc d'un fournisseur d'accès Internet, c'est la mise à disposition du public. Un restaurant aura cette qualification s'il offre un accès Wifi gratuit tandis qu'un individu qui offre la même chose à son domicile ne sera pas considéré comme fournisseur d'accès Internet.

En matière de lutte contre la cybercriminalité, les hébergeurs et fournisseurs d'accès Internet étrangers ne coopèrent pas toujours. Pour le Darknet, cette absence de coopération est encore plus vraie. Ainsi, certains voudraient poursuivre Tor sur le fondement de l'article 121-7 du code pénal pour avoir sciemment fourni une aide à la commission de l'infraction. Sa responsabilité pourrait être engagée en tant que mode de recrutement de terroriste et de communication entre eux pour la préparation d'un attentat. Toutefois, l'absence de rôle actif du réseau informatique ne permet pas d'envisager la complicité des infractions commises sur le Darknet. Une réponse rapide de la part du législateur est attendue.

[1083] A titre d'exemple, l'article 335-12 du Code de la propriété intellectuelle dispose que « *le titulaire d'un accès à des services de communication au public en ligne doit veiller à ce que cet accès ne soit pas utilisé à des fins de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation des titulaires des droits prévus aux livres Ier et II, lorsqu'elle est requise, en mettant en oeuvre les moyens de sécurisation qui lui sont proposés par le fournisseur de cet accès en application du premier alinéa du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* ».

CONCLUSION DU TITRE II
UN SYSTÈME JUDICIAIRE INADAPTÉ À LA CYBERCRIMINALITÉ DISSIMULÉE

La cybercriminalité évolue constamment et est difficile à cerner en raison de sa nature ambivalente. Son caractère transnational complique le travail des autorités qui doivent trouver des moyens efficaces pour éradiquer le phénomène ou du moins le limiter. Les nouvelles technologies ont permis la naissance d'un nouvel espace virtuel que le droit pénal ne peut pas méconnaitre, il s'agit du Darknet. S'y s'estdéveloppé un certain nombre d'infractions portant sur l'ensemble de la matière pénale et notamment sur l'application de la loi dans cet espace virtuel.

En effet, criminels du Darknet agissent de manière transnationale en utilisant des intermédiaires afin d'éviter d'être identifiés et localisés. Ils exploitent l'anonymat et le chiffrement afin d'échapper à leur arrestation. Ce sentiment d'impunité accentue le développement des activités illégales du Darknet. L'internaute se situe « *dans un espace géographique et temporel déterminé où tout ce qui est illégal « off line » est aussi illégal « on line ». Son comportement est également influencé par des pratiques de morale et d'éthique relevant des valeurs de la société dont il est le citoyen*[1084] ».

En France, l'application de la loi pénale dans l'espace repose sur quatre systèmes différents, celui de la compétence territoriale, celui de la compétence personnelle, celui de la compétence réelle et enfin celui de la compétence universelle. Ces systèmes sont fondés sur la commission de l'infraction d'une part, et sur la nationalité des protagonistes d'autre part.

De manière générale, le droit national et le droit international reconnaissent comme étant illégales la plupart des atteintes aux personnes, aux organisations et aux Etats, qu'elles soient commises sur Internet ou non. Toutefois, l'ubiquité permise dans le monde virtuel d'Internet, associé à l'invisibilité du Darknet complique fortement la tâche des autorités quant à la détermination des règles de compétences législatives et juridictionnelles. Les Etats se sont demandés s'il fallait adapter à la cybercriminalité les règles de droit commun ou s'il fallait

[1084] GHERMAOUTI-HELIE S., *La cybercriminalité : le visible et l'invisible*, collection le savoir suisse, page 51.

adopter des règles spécifiques. La difficulté réside dans le fait qu'une infraction commise sur Internet est intrinsèquement internationale contrairement aux règles de procédure qui sont prévues par le droit national. En France, malgré de nombreuses avancées ces dernières ne sont pas toujours adaptées au Darknet et méritent quelques modifications.

CONCLUSION DE LA 2nde PARTIE
LA FACE SOMBRE D'INTERNET, LES ASPECTS JURIDIQUES

La cybercriminalité est une notion difficile à appréhender pour les profanes et professionnels du droit. Lorsqu'elle est dissimulée, la notion se complexifie et les amalgames sont nombreux. L'adoption de la Convention de Budapest n'a rien changé puisqu'aucune définition n'a été apportée et aucune référence au Darknet faite.

Les lois relatives à la cybercriminalité se sont multipliées et ont modifié les codes pénal et de procédure pénale sans apporter de définition concrète de la cybercriminalité alors qu'elle semble indispensable. La notion est pourtant utilisée pour l'enquête européenne à l'article 695-32 du Code de procédure pénale[1085] qui dispose que « *les catégories d'infractions pour lesquelles une décision d'enquête ne peut être refusée en application du 8° de l'article 694-31 sont les suivantes : 8° Cybercriminalité* », par la loi LCEN ou par la loi du 14 mars 2011.

Une définition commune mondiale de la cybercriminalité permettrait de mieux appréhender le phénomène et ses évolutions. Ainsi, la cybercriminalité regrouperait « *toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet*[1086] *». Pour la cybercriminalité dissimulée, il conviendrait d'ajouter « à l'aide d'un réseau alternatif décentralisé garantissant un anonymat accru* ».

Concernant la circonstance aggravante pour les infractions commises sur l'Internet et le Darknet, des changements méritent d'être opérés. Pour les infractions commises contre ou au moyen d'un système d'information et de communication comme Internet, le quantum de la peine encourue devrait être augmenté. Tel pourrait être le cas pour l'escroquerie ou pour le trafic de stupéfiants. Pour l'instant, il n'y a qu'une circonstance aggravante lorsqu'est visé un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat.

[1085] Livre IV, Titre X, Chapitre II, Section 1, Sous-section 2, Paragraphe 1 : Reconnaissance des décisions d'enquête européenne.
[1086] Cette définition a été proposée par le procureur général près la Cour d'appel de Riom Marc Robert dans un rapport sur la cybercriminalité remis au Ministère de la Justice de l'époque le 30 juin 2014. Disponible à cette adresse : https://www.economie.gouv.fr/remise-du-rapport-sur-la-cybercriminalite.

Une telle circonstance aggravante mérite donc d'être étendue à d'autres situations.

Par ailleurs, le caractère international de la cybercriminalité a contraint les États à agir de manière concertée afin de mettre en place une politique de lutte efficace. Même si des efforts ont été faits en la matière, la coopération reste insuffisante notamment en ce qui concerne le Darknet. L'instrument juridique le plus efficace qu'est la Convention de Budapest sur la cybercriminalité a permis des améliorations en matière de cybercriminalité mais elle est limitée dans la mesure où elle n'aborde pas le Darknet.

En effet, en France de nombreuses règles de procédure facilitent le travail des enquêteurs qui disposent de nouveaux moyens d'investigation : l'enquête sous pseudonyme, le déchiffrement, les preuves numériques… Toutefois, les enquêteurs sont tenus de respecter une procédure pénale rigoureuse qui a tendance à les limiter dans l'appréhension des cybercriminels du Darknet.

CONCLUSION GÉNÉRALE

Globalement, la cybercriminalité est présentée « *comme comportant des infractions cyberdépendantes, des infractions cyberactivisées et, en tant que type spécifique de criminalité, l'exploitation et les abus sexuels d'enfants en ligne*[1087] ». Il y a tout d'abord la cybercriminalité qui suppose l'utilisation d'une technologie de l'information et de la communication et qui se caractérise par la création et l'utilisation de logiciels malveillants ou par cyberattaques ciblées. Il y a ensuite la cybercriminalité qui existe dans le monde non connecté mais qui peut être facilité par les technologies de l'information et de la communication. Tel est le cas pour le terrorisme ou pour le trafic de stupéfiants. Enfin, il y a la cybercriminalité qui affecte les enfants sur Internet et sur les forums du Darknet.

Ce dernier jouit encore d'une mauvaise réputation malgré les solutions qu'il apporte en matière d'anonymat et de chiffrement. Son fonctionnement totalement décentralisé est basé sur à une architecture *peer-to-peer* améliorée grâce à la confiance entre utilisateurs. L'accès a un darknet est extrêmement simple et repose sur un principe clair ; l'idée d'anonymat est fondée sur le fait que les utilisateurs sont cachés parmi les autres utilisateurs. Les différents darknets permettent de mettre en place ce type de réseau *friend-to-friend*. À titre d'exemple les utilisateurs de Retroshare peuvent utiliser une paire de clés cryptées afin d'échanger de manière cryptée avec leurs pairs de confiance. D'autres réseaux *peer-to-peer* anonyme rendent possible l'accès à des navigateurs en passant par des réseaux de communications chiffrées et anonymes. Dès lors, l'accès au Darkweb de manière anonyme est possible. Ce terme désigne l'ensemble du contenu présent sur les darknets qui sont les infrastructures.

Au départ dans les années 80 et 90, le Darknet était surtout une arme permettant de lutter contre la censure et l'espionnage des gouvernements. Ce genre de pratique a d'ailleurs été dénoncé par Snowden un ancien agent de la *NSA*. En outre, l'évolution récente d'Internet a permis aux

[1087] « *As having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse* ». Disponible à cette adresse : https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

différents darknets et aux cryptomonnaies d'avoir un impact incroyable en matière de nouvelles technologies et de finance. En effet, face au contrôle sociale et économique mis en place par les États et les GAFA, ils ont créé une sorte de résistance numérique. Même si l'anonymat total n'est que fantasme, en tant qu'alternative à l'Internet classique le Darknet permet donc de protéger les données des utilisateurs. Concernant le bitcoin, la plus populaire des cryptomonnaies, il fonctionne également de manière décentralisée afin d'éviter le contrôle des gouvernements. Toutefois l'idéologie de départ n'aura été qu'illusion dans la mesure où le contrôle des États ne s'est pas fait attendre.

L'approche idéaliste de ce nouvel endroit numérique a très rapidement été modéré en raison des nouvelles vulnérabilités qu'il offre aux criminels qui n'ont pas manqué d'imagination pour s'en accaparer. Grâce aux nouvelles techniques, la cybercriminalité dissimulée a permis l'éclosion de nouvelles formes de cybercriminalité. Le Darknet est rapidement devenu un lieu propice au développement des infractions informatiques mais aussi relevant de la criminalité classique et son arrivée a clairement révolutionné les infractions qui se sont créées avec l'essor d'Internet et celles préexistant avec son arrivée.

Dans cette lutte contre la cybercriminalité classique, celle qui existe depuis Internet, il existe un arsenal juridique complet qui se renforce de plus en plus en raison de la menace terroriste constante. Les infractions relatives à la cybercriminalité et à la cyberdélinquance sont visées par le Code pénal comme des infractions classiques. Ces infractions ont également vocation à s'appliquer au Darknet qui a permis la mise en place d'une criminalité nouvelle similaire à la cybercriminalité. Pour cette dernière, le législateur s'est adapté et a créé de nouvelles dispositions sanctionnant ces nouvelles infractions. Ainsi, il est possible d'affirmer que l'arsenal juridique en matière de lutte contre la cybercriminalité transposable à la cybercriminalité dissimulée.

Il est possible de conclure cette partie en mettant en avant l'inadaptation des règles juridiques à la cybercriminalité dissimulée malgré un arsenal répressif existant en raison des difficultés territoriales et de compétences inhérentes au Darknet. La coopération entre les États n'est toujours pas efficace dans la mesure où les ils préfèrent appliquer leur propre régime qui peut être fondamentalement différent de celui du voisin. Des efforts ont été entrepris mais les moyens mis en œuvre ne sont pas suffisants. Ce travail de recherche s'est soldé par une vision

d'échec de la matière pénale à l'endroit de la cybercriminalité dissimulée où les vrais criminels ont encore de belles perspectives d'avenir.

Bibliographie

I. REVUES, MANUELS, OUVRAGES GÉNÉRAUX

- B -

BOULOC B., *Droit pénal général*, 23e éd., Paris, Dalloz, 2013.

BOUZAT P., *Traité de droit pénal et criminologie,* 2e éd., Dalloz, 1970.

- C -

CONTE P., MAISTRE DU CHAMBON P., *Droit pénal général*, 4e éd., Armand Colin, 2004.

CONTE P., FOURNIER S., LARGUIER J., Droit pénal spécial, Dalloz, 15e édition, 2013.

CONTE P., *Droit pénal spécial, 5e ed.*, LexisNexis, 2016.

CONTE P., Procédure pénale, 24e ed., Dalloz, 2016.

- D -

DEBOVE F., *L'overdose législative*, LexisNexis, 2004.

DESPORTES, (F.) et LE GUNEHEC, (F.), *Droit pénal général*, 17e éd., Economica, 2010.

DONNEDIEU DE VABRES H., *Les principes modernes du droit pénal international*, LGDJ, 2004.

- F -

Fouchard I., *Crimes internationaux : Entre internationalisation du droit pénal et pénalisation du droit international,* Emile Bruylant, 2014.

- G -

GUINCHARD S. et BUISSON J., *Procédure pénale,* 9e éd., LexisNexis, 2013.

- L -

LEPAGE A., et Matsopoulou H., *Droit pénal spécial*, Presses Universitaires de France, 2015.

- M -

MERLE R. et VITU A., *Traité de droit criminel*, tome 2, Procédure pénale : Cujas, 5e éd., 2001.

- P -

PRADEL, (J.), *Droit pénal général*, 19e éd., Cujas, 2012.

PRADEL J.et VARINARD A., *Les grands arrêts du droit pénal général*, 8e éd, Dalloz, 2012.

- R -

REBUT D, *Droit pénal international*, 2e éd., Dalloz, 2014.

ROUJOU DE BOUBEE V-G., BOULOC B., FRANCILLON J., MAYAUD Y., *Code pénal commenté* , Dalloz, 1996.

- T -

THOUVENIN J-M., *Le principe de non extradition des nationaux*, Extrait de l'ouvrage Droit international et nationalité, Colloque SFDI de Poitiers, 2012.

II. OUVRAGES SPECIAUX, THÈSES, MONOGRAPHIES

- B -

BALLE F., COHEN T., *Dictionnaire du Web*, Dalloz.

BARLOW J.P, *Déclaration d'indépendance du Cyberespace, Traduction édition-Hache,* 1996.

BARTIN E. *Etude de droit international*, Université Paris Descartes, 2016.

BARTLETT J., The Darknet, Cornerstone Digital, 2014.

BIDDLE P., ENGLAND P., PEINADO M., and WILLMAN B., *The darknet and the future of content distribution*. In Proceedings of the 2002 ACM Workshop on Digital Rights Management, Washington DC, USA, 2002.

BRACH-THIEL D., *Conflits positifs et conflits négatifs en droit pénal international*, Université de Lorraine, 2000.

- C -

CASILE J-F., *Le Code pénal à l'épreuve de la délinquance informatique,* Presses Universitaires d'Aix-Marseille - P.U.A.M., 2002.

CHAUM D.L., *Blind signatures and untraceable payments, Advances in Cryptology Proceedings*, volume 82, n°3, pages 199-203, 1981.

CHAUM D.L., *Untraceable electronique mail, return adresses and digital pseudonyms*, *Communications of the ACM*, volume 32, 1981.

CHAUM D.L., *Security without identification : transaction systems to make big brother obsolete*, *Communications of the ACM*, volume 28, octobre 1985.

CHAWKI M., *Combattre la cybercriminalité*, Editions de Saint-Amans, 2008.

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

CLARKE, HONG T., MILLER S., SANDBERG O., WILEY B., *Protecting free expression online with Freenet*, IEEE Internet Computing, 2002.

- D -

DERIEUX E., *Déchiffrement forcé d'un moyen de cryptologie*, La revue européenne des médias et du numérique, n°46-47 Printemps – été 2018.

DIFFIE W., HELLMAN M., *Department of Electrical Engineering*, Université Stanford, 1971.

DIFFIE W., HELLMAN M., *New Directions in Cryptography*, Université Stanford, 1976.

- F -

FRANCILLON J., *Le droit pénal face à la cyberdélinquance et à la cybercriminalité*, Revue Lamy droit de l'immatériel (n°81), 2012.

FREYSSINET E., *La cybercriminalité en mouvement*, Lavoisier, Cachan, 2012.

- G -

GAYARD L., Darknet, GAFA, Bitcoin, *l'anonymat est un choix*, Slatkine & Cie, 2018.

GAYARD L., *Géopolitique du Darknet : Nouvelles Frontières et Nouveaux Usages du Numérique*, Iste édition, 2017.

GHERNAOUTI-HÉLIE S., *La cybercriminalité, le visible et l'invisible*, presses polytechniques et universitaires romandes, 2009.

GUILLOT P., *Histoire de la cryptologie*, Université Paris 8, 2014.

- H -

HUET J., DREYER E., *Droit de la communication numérique*, LGDJ, 2011.

HUET A., KOERING-JOLIN R., *Compétence des tribunaux répressifs français et de la loi pénale française*, fascicule 30, 11 mars 2013, page 20.

HENNINGER L., *Espaces fluides et espaces solides : nouvelle réalité stratégique ?* Revue de Défense Nationale, octobre 2012.

- J -

JABBER A., *Les infractions commises sur Internet*, L'Harmattan, 2009.

- K -

KEMPF O., *Interdire Telegram ?* Conflits, 2016.

KEMPF O., Introduction à la cyberstratégie, Economica, 2012.

- L -

LUCAS A., DEVEZE J., et FRAYSSINET, *Droit de l'informatique et de l'Internet*, Presses Universitaires de France, 2001.

- M -

MOORE D., RID T., Cryptopolitik and the Darknet, Survival : Global Politics and strategy, International Institute for Strategic Studies, volume 58, 2016.

- N -

NAHAI N., *Webs of Influence : The psychology of Online Persuasion,* The web psychologist*,* 2012

- O -

OMAR F., *Cadre conceptuel et théorique de la cybercriminalité*, Université de Lorraine, 2014.

- P -

PAILLER L., *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, 2012.

- Q -

QUÉMÉNER M., *Cybermenaces, entreprises, Internautes,* Economica, 2008.

- R -

RENNARD J.-P, *Darknet, Mythes et réalités*, Ellipses, 2016.

- S -

SENELLART P., *Comprendre le Web caché,* Université Paris-Sud 11, 2007.

SUETON, *La vie des douze Césars, Classiques de poche, 2002.*

- Y -

YOGODA B., *A Short History of Hack*, The New Yorker, 6 mars 2014

III. ETUDES, RAPPORTS

- B -

BOUHADANA I., GILLE W., HARIVEL J., *Darknet le côté obscur du Net*, Panthéon Sorbonne Magazine n°6, Janvier-Février 2014.

- C -

CIOTTI E. et MENNUCI P., *surveillance des filières et des individus djihadistes*, Rapport parlementaire, 2 juin 2015.

CNCDH, *Avis sur la refondation de l'enquête pénale*, Journal officiel du 10 mai 2014, texte n°84.

- D -

DAVADIE P., La théorie du Darknet, juin 2015, Article n°IV.7

DINGLEDINE, MATHEWSON R., N. et SYVERSON N., *Tor : The Second-Generation Onion Router,* In 13th USENIX Symposium, 2014.

- E -

ENISA REPORT, *the 2017 cyber threat landscape*, 15 janvier 2018.

EUROPOL REPORT, *Drugs and the Darknet. Perspectives for enforcement research and policy*.

- G -

GROUPE DE TRAVAIL INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE, *Rapport sur la cybercriminalité*, février 2014. Disponible à cette adresse : http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf.

- I -

Institut national des hautes études de la sécurité et de la justice, *Enjeux et difficultés de la lutte contre la cybercriminalité*, juillet 2015.

- J -

JAVANOVIC M., F. ANNEXTEIN F. et BERMAN K., *Scalability Issues in Large Peer-to-Peer Networks - A Case Study of Gnutella*, ECECS Department, University of Cincinnati, Cincinnati, OH 45221.

- L -

LEVALLOIS-BARTH C., LAURENT M., *La difficile anonymisation des données personnelles*, Revue TELECOM, n° 177, 2015.

- M -

MAY T., *The Crypto Anarchist Manifesto*, 1992. Disponible à cette adresse : https://www.activism.net/cypherpunk/crypto-anarchy.html.

MALKIN GS., *Internet Users' Glossary*, 1993. Disponible à cette adresse: https://tools.ietf.org/html/rfc1392.

MODICA B., *Mondialisation et criminalité*, Présentation du n°40 de la revue Questions internationales, décembre 2009. Disponible à cette adresse : https://www.diploweb.com/Mondialisation-et-criminalite.html.

- N -

NAKAMOTO, S., *Bitcoin : A Peer-to-Peer Electronic Cash System*, 2009. Disponible à cette adresse : https://bitcoin.org/bitcoin.pdf.

NYSTEDT D., *Wikileaks leader talks of courage and wrestling pigs*, PC World Australia, Sydney, 28 octobre 2009.

- O -

OCDE, *La fraude liée à l'informatique : analyse des politiques juridiques*, O.C.D.E, Paris, 1986.

- T -

TAN Z., W. FOSTER W., GOODMAN S., *China's state-coordinated internet infrastructure Communications of the ACM*, 1999.

TESQUET O., *Darknet, immersion en réseaux troubles*, Télérama, n°3322 du 14 septembre 2013.

THERY J-F et FALQUE PIERROTIN I., Internet et les réseaux numériques, collection Etudes du Conseil d'Etat, 1998.

IV. ARRÊTÉS, DÉCRETS, DIRECTIVES, LOIS, RÈGLEMENTS

- Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie, JORF n°66, 19 mars 1999.

- Arrêté du 16 juin 2009 portant création d'un système dénommé « PHAROS », JORF n°0141 du 20 juin 2009.

- Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable, JORF n°66 du 19 mars 1999.

- Décret n°2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n°2001-1062 du 15 novembre 2001 relative à la quotidienne et portant création du Centre technique d'assistance, JORF n°186, 10 août 2002.

- Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, JORF n°0050 du 1er mars 2011.

- Décret n°2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévues à l'article L.331-21 du Code de la propriété intellectuelle, JORF du 9 juillet 2013.

- Décret n°2017-614 du 24 avril 2017 portant création d'un service à compétence nationale dénommé « Agence nationale des techniques d'enquêtes numériques judiciaires » et d'un comité d'orientation des techniques d'enquêtes numériques judiciaires, JORF, n°97, 25 avril 2017.

- Directive 1999/93/C.E. du 13 décembre 1999 sur un cadre commun pour les signatures électroniques, JOCE. (L.) 13 du 19 janvier 2000.

- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

- Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

- Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie.

- Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information.

- Loi du 29 juillet 1881 sur la liberté de la presse.

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Loi n°90-1170 du 29 décembre 1990 sur la réglementation des communications, JORF n°303, publiée le 30 décembre 1990.

- Loi n°96-659 du 26 juillet 1996 de réglementation des télécommunications, JORF n°174, publiée le 27 juillet 1996.

- Loi n°2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice, JORF du 10 septembre 2002

- Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF n°59 du 10 mars 2004.

- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF, n°143, 22 juin 2004.

- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004.

- Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet, JORF n°0135 du 13 juin 2009.

- Loi n°2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet, JORF n°0251 du 29 octobre 2009.

- Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORFR n°0061 du 15 mars 2001.

- 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.

- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF n°0171 du 26 juillet 2015.

- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF, n°0235 du 8 octobre 2016.

- Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, JORF n°0287 du 10 décembre 2016.

- Loi n°2017-242 du 27 février 2017 portant réforme de la prescription de la matière pénale, JORF n°0050, publiée le 28 février 2017.

- Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique, JORF n°0051, publiée le 1er mars

2017.

- Règlement CE n°45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

- Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

V. NOTES, JURISPRUDENCE

Cour d'Appel de Douai, 7 octobre 1992, Gazette du Palais, 1993, n°22.

Cour d'appel de Paris, 5 avril 1994, D. 1994. IR 130.

Cour d'appel de Douai, 6 mai 2003, n°2003/573.

Cour d'appel de Paris, 12 juin 2013, n°13/06106.

Cour d'appel de Reims, 12 février 2014 n° 12/02936.

Cour de cassation, Assemblée Plénière, 29 juin 2001, n°99-85.973.

Cour de cassation, Assemblée Plénière, 7 novembre 2014, n° 14-83.739.

Cour de cassation, chambre criminelle, 12 juin 1952, Bulletin criminel n°153

Cour de cassation, chambre criminelle, 21 décembre 1961, dame Le Roux, D. 1962, page 162.

Cour de cassation, chambre criminelle, 9 novembre 1966, n° 65-93.832.

Cour de cassation, chambre criminelle, 3 janvier 1973, n°71-91820

Cour de cassation, chambre criminelle, 5 décembre 1978, n°78-91.826.

Cour de cassation, chambre criminelle, 23 avril 1981, n°81-90.489.

Cour de cassation, chambre criminelle, 13 octobre 1981, n°80-93.302.

Cour de cassation, chambre criminelle, 11 avr. 1988, n°87-83.873.

Cour de cassation, chambre criminelle, 13 juin 1989, n°89-81.709.

Cour de cassation, chambre criminelle, 20 février 1990, Bulletin criminel n°84, note Fournier.

Cour de cassation, chambre criminelle, 8 juin 1994, Droit pénal 1994, commentaire n° 235.

Cour de cassation, chambre criminelle, 17 octobre 1994, n°93-85.517.

Cour de cassation, 26 mars 1996, n°95-81.527.

Cour de cassation, chambre criminelle, 28 novembre 1996, n°95-80.168.

Cour de cassation, chambre criminelle, 21 octobre 1998, n°98-83.843.

Cour de cassation, 24 novembre 1998, n°98-80.048.

Cour de cassation, chambre criminelle, 3 décembre 1998, Bulletin criminel n°331.

Cour de cassation, chambre criminelle, 10 février 1999, Bulletin criminel n°15

Cour de cassation, chambre criminelle, 30 mars 1999, Bulletin criminel n°59.

Cour de cassation, chambre criminelle, 19 mai 1999 : Bulletin criminel n° 99,

Cour de cassation, chambre criminelle, 8 novembre 2000, n° 00-83570.

Cour de cassation, chambre criminelle, 22 août 2001, Bulletin criminel n° 169.

Cour de cassation, chambre criminelle, 7 mai 2002, Bulletin criminel n°108.

Cour de cassation, chambre criminelle, 11 juin 2002, Bulletin criminel n°131.

Cour de cassation, chambre criminelle, 11 juin 2003, Bulletin criminel n°119.

Cour de cassation, chambre criminelle, 5 janvier 2005, n°04-82.524.

Cour de cassation, chambre criminelle, 8 juin 2005, Bulletin criminel n°173.

Cour de cassation, chambre criminelle, 7 juillet 2005, n°05-81.119.

Cour de cassation, chambre criminelle, 11 mai 2006, Bulletin criminel n°132.

Cour de cassation, chambre criminelle, 7 juin 2006, Bulletin criminel n°161.

Cour de cassation, chambre criminelle, 9 août 2006, Bulletin criminel n°202

Cour de cassation, chambre criminelle, 19 juin 2007, Bulletin criminel n°169.

Cour de cassation, chambre criminelle, 5 septembre 2007, 07-80.263.

Cour de cassation, chambre criminelle, 26 septembre 2007, Bulletin criminel n°224.

Cour de cassation, chambre criminelle, 14 novembre 2007, Bulletin criminel n°281.

Cour de cassation, chambre criminelle, 15 janvier 2008, n°07-86.944.

Cour de cassation, chambre criminelle, 4 mars 2008, n°07-84.002.

Cour de cassation, chambre criminelle, 4 juin 2008, Bulletin criminel n°141.

Cour de cassation, chambre criminelle, 9 septembre 2008, n°07-97.281.

Cour de cassation, chambre criminelle, 30 septembre 2008, Bulletin criminel n°197.

Cour de cassation, chambre criminelle, 21 janvier 2009, n°08-83.482.

Cour de cassation, chambre criminelle, 12 mai 2009, Bulletin criminel n°89.

Cour de cassation, chambre criminelle, 14 décembre 2010, n°10-80.088.

Cour de cassation, chambre criminelle, 20 juin 2012, Bulletin criminelle n°156.

Cour de cassation, chambre criminelle, 30 avril 2014, Bulletin criminel n°119.

Cour de cassation, chambre criminelle, 16 décembre 2014, n°14-82.939.

Cour de cassation, chambre criminelle, 20 mai 2015, n° 14-81.336.

Cour de cassation, chambre criminelle, 4 octobre 2017, n°17-90017.

Cour de cassation, chambre criminelle, 9 mai 2018, n° 17-86.558.

Cour de cassation, chambre mixte Cour de cassation, 24 mai 1975, n°73-13556.

Tribunal des conflits, 5 juillet 1951, Avranches et Desmarets.

TGI Paris, 13 novembre 1998 : Gaz. Pal. 2000. 1. Doctrine 697, observation MANSEUR-RIVET.

TGI de Paris, référé, 20 novembre 2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France.

TGI de Paris, 17ème chambre, 26 février 2002.

VI. RESSOURCES ÉLECTRONIQUES

CNIL, *Marketing ciblé sur internet : vos données ont de la valeur*, 26 mars 2009. Disponible à cette adresse : http://www.cnil.fr/es/linstitution/actualité/article/article/marketing-cible-sur-internet-vos-donnees-ont-de-la-valeur.

BOUZOU L*., Les* perspectives pénales de la loi LOPSI 2 en matière de cybercriminalité, 10 février 2010. Disponible à cette adresse : http://www.e-juristes.org/les-perspectives-penales-de-la-loppsi-2-en-matiere-de-cybercriminalite.

HERBET M., *Wikileaks, une machine à scoops efficace mais opaque*, 26 juillet 2010. Disponible à cette adresse : http://www.lefigaro.fr/international/2010/07/26/01003-20100726ARTFIG00516-wikileaks-une-machine-a-scoops-efficace-mais-opaque.php

OURDAN R., *WikiLeaks : dans les coulisses de la diplomatie américaine*, 28 novembre 2010. Disponible à cette adresse : https://www.lemonde.fr/international/article/2010/11/28/wikileaks-dans-les-coulisses-de-la-diplomatie-americaine_1446078_3210.html.

DELCROIX M., *Wikileaks s'attaque au secret bancaire*, 18 janvier 2011. Disponible à cette adresse, http://www.rfi.fr/europe/20110117-wikileaks?utm_medium=twitter.

Magret D., *Un ancien de WikiLeaks prépare un site concurrent*, 10 septembre 2011. Disponible à cette adresse : https://www.nouvelobs.com/les-internets/20101211.OBS4515/un-ancien-de-wikileaks-prepare-un-site-concurrent.html.

VINTON G. CERF, *Internet access is not a human right, New York Times*, 4 janvier 2012. Disponible à cette adresse : https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

E. PECK M., *How Bitcoin brought privacy to electronic transactions*, 30 mai 2012. Disponible à cette adresse : http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash.

LAMENDE M-J*., FIC : Manuel Valls souhaite évaluer la cybercriminalité au plus juste*, janvier 2013. Disponible à cette adresse : https://www.globalsecuritymag.fr/FIC-Manuel-Valls-souhaite-evaluer,20130130,35132.html.

Ordonnance du TGI de Paris, *UEJV contre Twitter*, 24 janvier 2013. Disponible à cette adresse : https://cdn2.nextinpact.com/medias/ordonnance-tgi-paris-24-janvier-2013-uejf-vs-twitter.pdf.

GREENWALD G*., NSA collecting phone records of millions of Verizon customers daily*, 6 juin 2013. Disponible à cette adresse : https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

THE GUARDIAN, *Verizon forced to hand over telephone data – full court ruling*, 6 juin 2013. Disponible à cette adresse : https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

MACASKILL E., *Interview Edward Snowden*, NSA files source, 10 juin 2013. Disponible à cette adresse : https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why.

Courrier international, *« Moi, Edward Snowden, je vous écris… »,* 25 juin 2013. Disponible à cette adresse :

http://www.courrierinternational.com/revue-de-presse/2013/06/25/moi-edward-snowden-je-vous-ecris.

LOGEART A., Comment les enquêteurs traquent les pédophiles sur Internet, 30 mars 2014. Disponible à cette adresse : https://www.nouvelobs.com/l-enquete-de-l-obs/20130329.OBS6181/comment-les-enqueteurs-traquent-les-pedophiles-sur-internet.html

Y4N4UDEL, *Tueurs à gages sur le Deep Web : mythe ou réalité ?* 21 mars 2014. Disponible à cette adresse : https://www.undernews.fr/undernews/tueurs-a-gages-sur-le-deep-web-mythe-ou-realite.html

DECROIX C., *Cyberguerre : au cœur de la quatrième armée,* 9 octobre 2014, RTL. Disponible à cette adresse : https://www.rtl.fr/actu/justice-faits-divers/cyberguerre-au-c-ur-de-la-quatrieme-armee-7774738194.

GREENBERG A., *Over 80 percent of darkweb visits relate to pedophilia*, study finds, 30 décembre 2014. Disponible à cette adresse : https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/

UNTERSINGER M., *Les critiques de la CNLIL contre le projet de loi sur le renseignement*, 8 mars 2015. Disponible à cette adresse : http://www.lemonde.fr/pixels/article/2015/03/18/les-critiques-de-la-cnil-contre-le-projet-de-loi-sur-le-renseignement_4595839_4408996.html.

REES M., *Affaire Bluetouff : la Cour de cassation consacre le vol de fichiers informatiques*, 22 mai 2015. Disponible à cette adresse : https://www.nextinpact.com/news/95165-affaire-bluetouff-cour-cassation-consacre-vol-fichiers-informatiques.htm, [consulté le 22 mai 2015].

ROLLAND S., *La cybercriminalité est la nouvelle menace du XXIème siècle*, 27 juillet 2015. Disponible à cette adresse : https://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html.

LES ECHOS, *Les Etats-Unis ont espionné gouvernement et entreprises au Japon*, le 31 juillet 2015. Disponible à cette adresse : https://www.lesechos.fr/31/07/2015/lesechos.fr/021239469249_les-etats-unis-ont-espionne-gouvernement-et-entreprises-au-japon.htm

O'LEARY M., *The Mysterious Disappearance of Satoshi Nakamoto, Founder & Creator of Bitcoin*, 5 août 2015. Disponible à cette adresse : http://www.huffingtonpost.com/martin-oaleary/the-mysterious-disappeara_2_b_7217206.html.

VANCE JR. MOLINS F., LEPPARD A., ZARAGOZA J., *When Phone Encryption Block Justice*, 11 août 2015. Disponible à cette adresse : https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0,

BRIAN M., *TalkTalk hacked in significant and sustained cyberattack*, 23 octobre 2015. Disponible à cette adresse : http://www.engadget.com/2015/10/23/talktalk-hacked/.

GOFFI, *Centralisé, décentralisé, P2P, mais c'est quoi tout ça ?* 10 novembre 2015.
Disponible à cette adresse : https://www.goffi.org/post/2015/11/10/centralisé,-décentralisé,-P2P,-mais-c-est-quoi-tout-ça

BLUE V., *The myth of Marianas web the darkest cornet of the Internet*, 18 décembre 2015. Disponible à cette adresse : https://www.engadget.com/2015/12/18/the-myth-of-marianas-web-the-darkest-corner-of-the-internet.

LORRIAUX A., *Le FBI a pris le contrôle d'un site pédopornographique pour arrêter des criminels. Est-ce*

éthique, 26 janvier 2016. Disponible à cette adresse : http://www.slate.fr/story/113193/fbi-pedopornographie.

CHEVALIER H., *Chiffrement des données : la guerre est lancée*, 28 janvier 2016. Disponible à cette adresse : https://www.franceinter.fr/societe/chiffrement-des-donnees-la-guerre-est-lancee

MOREIRA E., *Comment le FBI traque les pédophiles sur le dark web*, 30 janvier 2016. Disponible à cette adresse : https://www.lesechos.fr/30/01/2016/lesechos.fr/021642681509_comment-le-fbi-traque-les-pedophiles-sur-le-dark-web.htm

CHEMINAT J., *Cyberattaques : un cru 2015 très actif et plus criminalisé*, 12 février 2016. Disponible à cette adresse : https://www.silicon.fr/cyberattaques-un-cru-2015-tres-actif-et-plus-criminalise-138826.html,

CHAFFIN Z., *Paris dénonce une privatisation de la gouvernance d'Internet*, 24 mars 2016. Disponible à cette adresse : https://www.lemonde.fr/economie/article/2016/03/24/icann-paris-denonce-une-privatisation-de-la-gouvernance-d-internet_4889567_3234.html

LAUSSON J., *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*, 22 avril 2016. Disponible à cette adresse : https://www.numerama.com/politique/165488-pedopornographie-quand-un-piratage-par-le-fbi-sur-tor-prive-les-victimes-dune-justice.html.

PAQUETTE E., WESFREID M., *Telegram, l'appli favorite des politiques pour chiffrer leurs messages*, L'Express, 14 juillet 2016. Disponible à cette adresse : https://lexpansion.lexpress.fr/high-tech/telegram-l-appli-favorite-des-politiques-pour-crypter-leurs-messages_1811791.html.

WALTER D. (adapté par FILIPPONE D.), *Les 5 meilleures apps de messagerie chiffrée*, 16 septembre 2016. Disponible à cette adresse : https://www.lemondeinformatique.fr/actualites/lire-comment-salesforce-s-est-prepare-au-rgpd-71829.html.

20 minutes, *Piratage des e-mails de la campagne Clinton : Les dégâts d'une simple faute de frappe*, 14 décembre 2016, https://www.20minutes.fr/high-tech/1980199-20161214-piratage-e-mails-campagne-clinton-degats-simple-faute-frappe.

BFM TV, *Il commande de la drogue sur Internet, les douaniers lui livrent son colis*, 21 mai 2017. Disponible à cette adresse : https://www.bfmtv.com/police-justice/il-commande-de-la-drogue-sur-internet-les-douaniers-lui-livrent-son-colis-1168716.html.

FRANCE TV INFO, *Drogues : le nombre de morts par overdose*, le 6 juin 2017. Disponible à cette adresse : https://www.francetvinfo.fr/societe/drogue/drogues-le-nombre-de-morts-par-overdose-augmente-en-europe_2224935.html

MEKKI M., *Droits et algorithmes : de la blockchain à la justice prédictive*, 6 juin 2017. Disponible à cette adresse : https://actu.dalloz-etudiant.fr/le-billet/article/droitss-et-algorithmes-de-la-blockchain-a-la-justice-predictive/h/d66e9db5333715c8ff6d88221cf44721.html.

TRUJILLO E., *CybelAngel lève 3 millions d'euros pour surveiller le dark Web et les objets connectés*, 7 juin 2017. Disponible à cette adresse : http://www.lefigaro.fr/secteur/high-tech/start-up/2017/06/07/32004-20170607ARTFIG00003-cybelangel-leve-3-millions-d-euros-pour-surveiller-le-dark-web-et-les-objets-connectes.php.

FARREL P., *Inside the darknet : where Australians buy and sell illegal goods*, 4 juillet 2017. Disponible à cette adresse : https://www.theguardian.com/technology/2017/jul/04/inside-the-darknet-where-australians-

buy-and-sell-illegal-goods.

MONTREAL GAZETTE, *RCMP's Dark web investigation leads to searches in Montreal,* 5 juillet 2017. Disponible à cette adresse : http://montrealgazette.com/news/local-news/rcmps-dark-web-investigation-leads-to-searches-in-montreal-trois-rivieres.

CIMPANU C., *Alphabay Dark Web Market Taken Down after Law Enforcement Raids*, 14 juillet 2017. Disponible à cette adresse : https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids.

LE MONDE, *Comment la police australienne a infiltré et administré un site pédopornographique*, 19 octobre 2017. Disponible à cette adresse : http://www.lemonde.fr/pixels/article/2017/10/09/comment-la-police-australienne-a-infiltre-et-administre-un-site-pedopornographique_5198556_4408996.html.

MOORE D., RID T., *Cryptopolitik and the Darknet*, février 2018. Disponible à cette adresse : https://www.crypto-france.com/darknet-bitcoin-litecoin.

CASTRO V., *Impôts & bitcoin : comment bien déclarer ses cryptomonnaies, notre guide en 10 questions*, 2 février 2018. Disponible à cette adresse : https://www.numerama.com/business/325205-impots-bitcoin-comment-bien-declarer-ses-cryptomonnaies-notre-guide-en-10-questions.html.

REES M., *La neutralité du Net s'invite dans la lutte contre la cybercriminalité*, 14 mars 2018. Disponible à cette adresse : https://www.nextinpact.com/news/106304-lpm-2019-2025-neutralite-net-sinvite-dans-lutte-contre-cybercriminalite.htm.

DUNAWAY J*., Sen. Dick Durbin Proves Mark Zuckerberg Is As Awkward As the Rest of Us*, 10 avril 2018. Disponible à cette adresse : https://slate.com/technology/2018/04/dick-durbins-questionat-the-senate-congressional-hearing.html.

LE PARISIEN, *Facebook : ce qu'il faut retenir du mea culpa de Mark Zuckerberg devant le Congrès*, 10 avril 2018. Disponible à cette adresse : http://www.leparisien.fr/high-tech/facebook-ce-qu-il-faut-retenir-du-mea-culpa-de-mark-zuckerberg-devant-le-congres-10-04-2018-7657422.php.

LAUSSON J., *Hadopi : le gouvernement va recycler de vieilles idées pour lutter contre le piratage*, 19 avril 2018. Disponible à cette adresse : https://www.numerama.com/politique/346996-hadopi-gouvernement-va-recycler-de-vieilles-idees-lutter-contre-piratage.html.

Le Point, *La justice ordonne le blocage de la messagerie Telegram*, 30 avril 2018. Disponible à cette adresse : https://www.lepoint.fr/high-tech-internet/iran-la-justice-ordonne-le-blocage-de-la-messagerie-telegram-30-04-2018-2214876_47.php.

LE MONDE, *Gal Vallerius, Le barbu du dark web, plaide coupable de trafic de stupéfiants*, 12 juin 2018. Disponible à cette adresse : https://www.lemonde.fr/pixels/article/2018/06/12/gal-vallerius-le-barbu-du-dark-web-plaide-coupable-de-trafic-de-stupefiants_5313737_4408996.html.

ADAM L., *Cybercriminalité en France : les autorités adaptent leur dispositif, mais la route est longue*, 22 juin 2018. Disponible à cette adresse : https://www.zdnet.fr/actualites/cybercriminalite-en-france-les-autorites-adaptent-leur-dispositif-mais-la-route-est-longue-39870090.htm.

TANNAM E., *How does ENISA help EU member states with their cybersecurity strategies ?* 9 août 2018. Disponible à cette adresse : https://www.siliconrepublic.com/enterprise/steve-purser-enisa-cybersecurity.

LE CALME S., *CJUE : le droit à l'oubli devrait-il être appliqué au niveau mondial ? Google estime que non*, le

11 septembre 2018. Disponible à cette adresse : https://www.developpez.com/actu/223732/CJUE-le-droit-a-l-oubli-devrait-il-etre-applique-au-niveau-mondial-Google-estime-que-non-et-avance-ses-arguments-devant-la-Cour/.

GAUTRONNEAU V., et DÉCUGIS J-M., *Repéré par le FBI, il gérait des sites de pornographie infantile*, 16 octobre 2018. Disponible à cette adresse : http://www.leparisien.fr/oise-60/oise-un-pedopornographe-interpelle-avec-l-aide-du-fbi-16-10-2018-7920762.php#xtor=AD-1481423552#xtor=AD-1481423551.

Index alphabétique

UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

Tables des matières

L'applicabilité de la loi pénale à l'endroit de la cybercriminalité dissimulée

Résumé : Les formes de la criminalité varient selon la personnalité des auteurs d'infractions mais aussi en fonction de l'évolution des technologies. A ce titre, le développement très rapide de l'internet constitue un facteur susceptible de bouleverser les règles ordinaires du droit et de la procédure pénale en raison des problèmes particuliers que crée cet outil qui peut aisément devenir un moyen de commettre de multiples infractions pénales. En outre, l'internet présente des formes plus variées qu'il n'y paraît au premier abord car, au-delà de sa partie visible aisément accessible, les spécialistes ont mis en lumière l'existence de ce qu'ils appellent le « *Deep web* » ou « *Web profond* ».

Ce « *Deep web* » est une partie du web en ligne non référencée par les moteurs de recherche habituels tels que Google ou Yahoo par exemple. Et selon Chris Sherman et Gary Price, dans leur livre *The Invisible Web*, seuls 3 à 10 % des pages seraient indexés sur internet. Le reste, non accessible pour les internautes ordinaires, constitue le web invisible et il existerait ainsi plus d'un milliard de données « cachées ». Les raisons pour lesquelles certains sites ne sont pas référencés sont diverses. Dans certains cas, les documents sont trop volumineux ou les bases de données sont trop complexes pour que leur contenu soit indexé, mais dans d'autres cas, des individus décident de ne pas référencer leur site afin de « privatiser » l'information puisque seuls ceux connaissant la dénomination du site pourront y accéder. Il s'agit donc de ce qui pourrait être appelé « *partie immergée* » d'Internet. Mais au delà du web profond, des outils de reconnaissance indétectables par les moteurs de recherches habituels sont apparus, ce sont les darknets Ils permettent de décrypter les pages invisibles et garantissent un anonymat quasi absolu et surtout un accès au Darkweb, aussi appelé Web sombre.

C'est ainsi que ce dernier a hébergé divers types de marchés noirs, de la drogue aux armes en passant par le trafic d'êtres humains. Le *Hidden Wiki*, sorte de Wikipédia illégal, se charge de référencer ces portes d'entrées sur cette partie d'Internet. De nombreux sites, commerciaux ou non, sont alors créés. A titre d'exemple, le site « *Shroomtastic* » permet d'apprendre à faire pousser des champignons hallucinogènes, activité illicite. Le site *Silkroad*, quant à lui, constitue un marché clandestin permettant d'acheter toutes sortes de drogues et il existe d'autres sites

permettant de blanchir de l'argent, offrant les services de tueurs à gage, ou permettant d'obtenir de fausses cartes d'identité… En pratique, il est possible d'obtenir nombre de produits ou marchandises illégaux et, pour la livraison, cette couche d'internet possède même sa propre monnaie, le bitcoin. Il suffit alors au client de se mettre en relation avec le vendeur pour lui envoyer l'adresse de livraison de manière cryptée et anonyme grâce à une méthode de communication décentralisée.

Sur le plan juridique, le thème présente de multiples intérêts et pose de nombreuses questions, la principale étant de savoir dans quelle mesure la répression peut-elle avoir lieu et comment peut s'organiser la lutte contre cette forme de cybercriminalité. Le sujet conduit notamment à se demander comment la loi pénale doit s'appliquer dans l'espace, de quelle manière le droit international peut appréhender efficacement le phénomène, comment coordonner la répression entre les différents États et quelles règles de procédure appliquer, la question se posant encore de savoir si des infractions spéciales devraient être créées ou si, au contraire, les incriminations de droit commun sont suffisantes pour permettre une répression efficace. Le sujet touche donc de nombreux thèmes essentiels du droit pénal général, du droit pénal spécial, de la procédure pénale, du droit pénal international ou même de la criminologie.

Mots-clés : Cybercriminalité - Darknet - Droit pénal - Bitcoin - Terrorisme - Stupéfiants - Pédopornographie - Atteintes aux systèmes informatisés de données.

Abstract : The "Deep web" is a part of the web which isn't referenced by usual search engines. According to Chris Sherman and Gary Price, these only refer to 3 to 10% of the pages. The rest which isn't accessible to regular web users consists in the "Deep Web" and more than one billion hidden datas remain. In a few cases, the documents are too heavy, or the databases are too complicated to have their contents indexed, but in other cases, individuals decide not to reference their websites in order to make the information private. We can consider this as the tip of the Internet. It hosts several black market types such as, drugs, weapons or human trafficking. On a judicial point of view, this topic is quite meaningful and raises a lot of questions. The main issue is to determine how to organise the repression on that medium. This leads us to think about the application of the law through different countries, how can the international law comprehend the phenomenon effectively. How the different states should

coordinate their repressive measures and agree on the proper procedural rules to apply. We could ask ourselves rather regular law enforcements are relevant enough to allow an adequate repression, or if specific infractions should be created. So the topic deals with essential thoughts on the international law.

Keywords : Cybercriminality - Darknet - Criminal law - Bitcoin.