La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité

Brigitte Pereira

LA LUTTE CONTRE LA CYBERCRIMINALITE : DE L'ABONDANCE DE LA NORME A SA PERFECTIBILITE

Brigitte PEREIRA,

Professeur de Droit et de Responsabilité Sociale des Entreprises à l'EM Normandie- HDR

Laboratoire Métis- EM NORMANDIE

***Résumé* :** Le développement des réseaux de communication, la généralisation d'internet, de même que l'accès facilité et continu aux informations sensibles au sein des entreprises, ont conduit à l'accroissement de la cybercriminalité. Si la criminalité est inhérente aux sociétés, elle n'en demeure pas moins une problématique quant à son évolution : liée au développement économique des espaces terrestre, maritime et aérien, la criminalité l'est désormais aussi à celui du cyberespace. C'est la raison pour laquelle la lutte contre la cybercriminalité a fait l'objet d'un développement normatif dense. Toutefois, la norme de nature répressive, même très développée, recouvre une certaine relativité quant à son efficacité. Alors qu'il existe une multitude d'infractions commises dans le cyberespace, la détermination des responsabilités comporte des difficultés qu'il s'agisse des hébergeurs, des fournisseurs d'accès à internet ou des éditeurs. Par ailleurs, parce que cette délinquance recouvre une dimension mondiale, la localisation des actes, suscite des débats sur l'application de la territorialité du cybercrime. Compte tenu des difficultés spécifiques à appréhender ce type de délinquance affectant fortement le secteur économique, la coopération internationale est présentée comme un moyen efficace de l'enrayer. Or, le développement de la coopération internationale est conditionné.

Mots clés : Système de traitement automatisé de données ; cybercrime ; hébergeurs ; éditeurs ; coopération internationale ; insécurité

1 INTRODUCTION

Le développement des réseaux de communication, la généralisation d'internet dans les entreprises, de même que l'accès facilité et continu aux informations ou données sensibles [1] au sein des organisations, ont conduit à l'accroissement de la cybercriminalité. Si la criminalité est inhérente aux sociétés [2], elle n'en demeure pas moins une problématique quant à son évolution : liée au développement économique des espaces terrestre, maritime et aérien, la criminalité l'est désormais aussi à celui du cyberespace [3]. En effet, c'est dans l'espace cybernétique, dit en apparence virtuel et immatériel, que de multiples infractions sont effectivement commises, ces dernières produisant des dommages considérables aux dépens des acteurs économiques et de la société civile [4]. Dès lors, la cybercriminalité est une réalité qui ne peut être ignorée par le droit.

Néanmoins, le concept de cybercriminalité n'est pas défini par le droit, même si plus de 470 infractions sont liées aux systèmes d'information. Le préfixe « cyber » vient du grec « *kubernêsis* » signifiant « gouverner ou action de diriger » [5]. Ce préfixe est aussi emprunté au terme « cybernétique » issu des travaux du mathématicien américain Norbert Wiener, traitant de l'étude de la commande et de la communication chez l'animal et dans la machine [6]. Aujourd'hui, les termes « cybersécurité, cyberdéfense et cybercriminalité » sont employés de manière interdépendante sans que des définitions précises n'aient été consacrées par le droit. Dès lors, même si ce dernier appréhende la cybercriminalité par la consécration de nombreuses infractions, la cybercriminalité se prête mal à une définition, ce que la Commission européenne a explicitement avancé dans une communication au Parlement européen en 2007 : « faute d'une définition communément admise de la criminalité dans le cyberespace, les termes de cybercriminalité, criminalité informatique ou criminalité liée à la haute technologie sont souvent utilisés indifféremment » [7]. Pour autant, la cybercriminalité est comprise à travers la commission d'infractions pénales à l'encontre ou au moyen d'un système d'information et de communication, principalement internet utilisant les réseaux ou les systèmes d'information comme moyens, ou les ayant pour cible. Selon l'O.N.U., il s'agit de « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes d'information et des données qu'ils traitent » [8]. Selon l'O.C.D.E., la cybercriminalité comprend « tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de la transmission de données » [9]. Aux Etats-Unis, le concept de

---

[1] Les « données » désignent les informations créées et utilisées par le biais d'un logiciel, ou qui se prêtent à un système de traitement automatisé (voir l'article 2 de la Loi n° 78-17 du 6 janvier 1978, J.O.R.F. 7 janvier 1978 (Légifrance)

[2] E. Durkheim, *Les règles de la Méthode sociologique*, Paris, PUF, 1983

[3] W. Capeller et G. Vermelle, « Le droit et l'immatériel », *Archives de philosophie du droit, tome 43*, Dalloz/Sirey, p. 167 s et p. 213 s ; M. Quéméner et J. Ferry, *Cybercriminalité, Défi mondial*, 2e édition, Economica, 2009 ; Rapport Digital, Social and Mobile, We are social's compendium of global digital statistics, Rapport de 2015, 376 pages

[4] M. Robert (sous la direction de), Rapport sur la cybercriminalité, Protéger les internautes, Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, 276 pages, spéc. p. 7 et 8 ; W. Dubost, « La cybercriminalité doit être contrée par une cybersécurité efficace », *Revue Banque*, mars 2015, p. 75 s.

[5] M. Quéméner et J. Ferry, *Cybercriminalité, Défi mondial*, 2e édition, Economica, op. cit

[6] N. Wiener, *Cybernetics or control and communication in the animal and the machine*, Paris (Hermann et Cie), 1948

[7] Commission européenne, Vers une politique générale en matière de lutte contre la cybercriminalité, Communication MEMO/07/199, 22 mai 2007

[8] Dixième Congrès des Nations Unies, à Vienne, sous le titre « la prévention du crime et le traitement des délinquants », [10 – 17 avril 2000], http://www.uncjin.org/

[9] H. Alterman et A. Bloch, « La Fraude Informatique », *Gazette du Palais*, 3 septembre 1988, p. 530

cybercriminalité comporte des distinctions selon les Etats [10]. Selon le Département de la justice (*United States Department of Justice*), la cybercriminalité est considérée comme « *une violation du droit pénal impliquant la connaissance de la technologie de l'information* »[11]. En réalité, s'il existe une pléthore de définitions de la cybercriminalité, elles tendent à regrouper les infractions en deux catégories : les unes sont tentées ou commises contre les systèmes de traitement automatisé de données (STAD), tandis que les autres le sont grâce à ces systèmes. Les premières concernent notamment l'accès non autorisé à ces systèmes, les atteintes à l'intégrité des données et des systèmes informatiques, ou les atteintes à leur confidentialité ; les secondes regroupent les infractions de droit commun commises au moyen d'un système de traitement automatisé de données, comme l'escroquerie ou la contrefaçon. C'est dire que la cybercriminalité recouvre une dimension importante eu égard à la diversité des actes illicites commis, à son caractère internationalisé et aux dommages causés aux Etats, aux entreprises et aux personnes.

Alors que la quasi-totalité des entreprises [12], 3 025 milliards d'internautes, soit 42 % de la population mondiale disposent d'un accès internet [13], les chiffres de la cybercriminalité ne sont pas connus avec précision, compte tenu de la difficulté de la mesure. Cette difficulté, connue également pour l'ensemble des infractions, est particulièrement accrue s'agissant de la cybercriminalité : l'ensemble des infractions relevant spécifiquement de la criminalité informatique ne sont pas répertoriées avec celles relevant du droit commun en lien avec les systèmes d'information. De plus, les victimes, et particulièrement les entreprises, sont peu enclines à divulguer les attaques informatiques dont elles ont fait l'objet, afin de ne pas porter atteinte à leur notoriété. Néanmoins, sur le produit criminel mondial brut de 1000 milliards de dollars annuels (faits découverts et constatés par les autorités), soit 20 % du commerce mondial dans les années 2000, 200 milliards de dollars concernent les profits issus du piratage informatique [14]. Certaines études ont révélé que plus d'un milliard vingt-trois millions de données ont été soustraites durant l'année 2014 [15] . Ces opérations de vol de données, ayant pour victimes les Etats et les entreprises (Sony, Ebay, Areva, Total…) ont pu être réalisées par l'intermédiaire de milliers d'opérations d'intrusion dans les systèmes. De même, les usurpations d'identité représentent 54% des attaques informatiques [16]. Les secteurs d'activité les plus touchés sont la vente de détail et les services financiers. Par ailleurs, cette délinquance est accompagnée d'un sentiment d'impunité qu'éprouvent les auteurs (hackers et pirates) eu égard à la volatilité des données, l'anonymat, de même que l'évolution constante des technologies et la dimension internationale des actes commis.

C'est la raison pour laquelle les Etats se sont mobilisés afin de faire évoluer les normes dans le sens d'une répression efficace. Ainsi, par exemple, en France, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a été créé

---

[10] E. LAWTA: Law enforcers report spike in cybercrime (USAtoday.com). Disponible sur : <http://www.usatoday.com/> (11/11/2004).

[11] *U.S.Department of Justice* <http://www.justice.gov/>.

[12] Eurostat, Statistiques sur la société de l'information-entreprises, juin 2015 : en 2013, 96 % des entreprises employant au moins 10 salariés avaient un accès internet

[13] Digital, Social et Mobile, We are social's compendium of global digital statistics, Rapport de 2015 préc.

[14] B. Pereira, *La responsabilité pénale des entreprises et de leurs dirigeants*, EMS, 2011, p. 17

[15] Rapport SafeNet 2014, http://www.breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf

[16] Loi n° 2011-267 du 14 mars 2011 d'Orientation et de programmation pour la performance de la sécurité intérieure, Loi LOPSI II, JO n° 62, 15 mars 2011

en 2000 [17] : placé au sein de la Direction centrale de la police judiciaire, cet office est doté d'une compétence judiciaire nationale étendue en matière d'enquête sur les fraudes à la carte bancaire et les piratages. En outre, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) a été créée en 2009 afin d'assurer la partie technique de la sécurité des systèmes d'information. Cette agence interministérielle joue alors un rôle préventif. Aussi, doit-on rappeler que les instruments européens et internationaux ont été multipliés afin d'accroître la coopération internationale tant cette criminalité a créé une nécessité commune de la combattre. A cet égard, la Convention de Budapest de lutte contre la cybercriminalité constitue l'instrument international de référence [18].

Cependant, en dépit de l'accroissement de la norme et de celui des moyens de coopération, on soulève une problématique d'efficacité qui nous conduit à la question de savoir si le droit répressif est à même de constituer la seule réponse à la cybercriminalité ; et s'il est doté des moyens suffisamment efficients pour répondre à l'ingéniosité du cybercrime. On remarque une superposition de multiples normes au point de constater un droit dense, mais nécessitant une mise en cohérence ; on souligne également le développement d'organisations, d'institutions et d'associations destinées à jouer un rôle préventif au même moment que les pouvoirs de police et de surveillance connaissent un accroissement considérable, parfois aux dépens des libertés individuelles. En réalité, il existe des attentes très fortes, à la fois de protection contre les actes des cyberdélinquants et de garantie des libertés individuelles, dont la liberté d'entreprendre fait partie. Cet équilibre difficile conduit au constat de la perfectibilité de la lutte contre la cybercriminalité, moins pour des raisons d'absence de norme que pour celles liées à son intelligibilité.

Plus précisément, alors que les infractions concernant la cyberdélinquance sont nombreuses, on relève des hésitations quant à la détermination de la responsabilité des prestataires techniques. De surcroît, ces derniers, revendiquant leur extranéité [19], posent des problématiques de localisation de leurs agissements sur le plan territorial. Qu'il s'agisse des fournisseurs d'accès à internet, des hébergeurs, des abonnés, ou des auteurs de blogs, la responsabilité n'est pas déterminée de manière univoque. L'étendue de la responsabilité de chacun d'entre eux est distincte pour un acte commis dans le cyberespace. Or, cette distinction est d'autant plus disparate qu'elle est appréhendée différemment selon les Etats. Aussi, l'applicabilité de la norme et la compétence des juridictions nationales posent-elles des difficultés : de quelle manière appliquer le principe de territorialité, compte tenu de la spécificité du web ? S'agit-il de viser la source du dommage, le lieu de commission, le lieu d'envoi des messages ou de la commission des attaques, ou encore celle de la réception et celle de l'accessibilité des sites ? Or, la jurisprudence est parfois contradictoire selon les infractions concernées, particulièrement en matière de contrefaçon [20].

---

[17] Décret n° 2000-405 du 15 mai 2000 portant création de l'Office Central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), NOR : INTX0004111D

[18] Convention du Conseil de l'Europe et des Etats non membres relative à la lutte contre la cybercriminalité du 23 novembre 2001 complété par son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

[19] E. Dreyer, « L'internationalisation de la communication. Les lois applicables. Le droit pénal international » *in* Traité du Droit de la presse et des médias, Litec, 2009, p. 1269 s.

[20] Cassation criminelle 9 septembre 2008, n° 07-87.281, Dalloz 2009, p. 1992, observations J. Larrieu, C. Le Stanc et P. Tréfigny ; Cassation criminelle 14 décembre 2010, n° 10-80.088, Dalloz 2011, p. 1055, observations E. Dreyer

Enfin, la dimension internationale impose une coopération entre les Etats afin de mieux appréhender les actes commis simultanément dans plusieurs Etats. Or, les cyberdélinquants, sont enclins à opérer depuis des territoires plus permissifs, pour garantir leur impunité. Par ailleurs, les entreprises-prestataires techniques (fournisseurs d'accès, hébergeurs) peuvent aussi souhaiter délimiter leur responsabilité en s'installant dans les Etats plus souples en matière de règlementation. Ces éléments expliquent que la coopération internationale doit être le résultat de la prise en compte de ces différents éléments : l'intérêt des entreprises sous l'angle de leur responsabilité, mais également sous celui de leur protection et celle des libertés individuelles. La coopération internationale, et particulièrement celle européenne, a fortement été développée depuis ces dernières années. Les instruments d'entraide judiciaire sont en effet prévus comme les échanges d'informations entre autorités judiciaires de différents Etats afin de garantir une recherche de preuves efficace. Cependant, la mise en œuvre de l'entraide judiciaire souffre encore de nombreuses conditions rendant l'efficacité de cette coopération limitée, ce qui ne répond pas aux enjeux cruciaux de la lutte contre une délinquance astucieuse, rapide, mondiale et pourvue d'ubiquité. Dès lors, nous analyserons dans un premier temps l'outil répressif pour en réaliser sa relative efficacité (2). Nous appréhenderons dans un second temps pour quelles raisons la coopération internationale demeure encore hésitante, afin de mettre en évidence les moyens d'amélioration entrepris (3).

2 L'EFFICACITE RELATIVE DE L'OUTIL REPRESSIF

L'outil répressif recouvre une densité importante, ce qui pourrait conduire à penser que le droit répressif permet d'appréhender tous les agissements relevant de la cybercriminalité. Néanmoins, la multiplicité des infractions (2.1.) rend davantage compte d'une problématique d'accessibilité de la norme. De plus, la détermination des responsables, qu'il s'agisse des fournisseurs d'accès à internet ou des hébergeurs, recouvre de nombreuses difficultés (2.2.).

2.1 Quant à la multiplicité des infractions concernées

Si l'on se réfère à la Convention du Conseil de l'Europe du 23 novembre 2001 (Convention de Budapest), instrument international traitant spécifiquement de la cybercriminalité, on relève neuf types d'infractions [21] : l'accès illégal aux systèmes et données informatiques tel que le piratage ; l'interception illégale ; l'atteinte à l'intégrité des données ; l'atteinte à l'intégrité des systèmes (virus, spam et déni de service) ; le marché noir de la production ou la vente de moyens de commettre les infractions (infractions d'abus de dispositif) ; la fraude informatique ; la falsification informatique ; les infractions se rapportant à la pornographie enfantine ; les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes [22].

En France, la lutte contre la cybercriminalité a été prise en compte par le législateur depuis la loi relative à l'informatique et aux libertés du 6 janvier 1978 [23]. Par la suite, c'est la loi Godfrain du 5 février 1988 relative à la fraude informatique [24] qui a permis de sanctionner la suppression et la modification des données, de même que les atteintes aux systèmes d'information [25]. Depuis lors, de nombreuses lois ont été votées pour prendre en compte le caractère multiforme de la

[21] La Convention relative à la lutte contre la cybercriminalité s'étend au-delà des seuls Etats membres du Conseil de l'Europe. 55 pays l'ont adoptée dont le Canada (en 2015), l'Australie (2013), les Etats-Unis (2007) et le Japon (2012).
[22] Articles 2 à 10 de la Convention ; Voir not. B. Pereira, La responsabilité pénale des entreprises et de leurs dirigeants, op. cit, spéc. p. 165 à 175
[23] Loi n° 78-17 du 6 janvier 1978, J.O.R.F. 7 janvier 1978 (Légifrance)
[24] Loi n° 88-19 du 5 janvier 1988, JORF 6 janvier 1988, p. 231
[25] Articles 323-1 et suivants du Code pénal

cyberdélinquance telles que les lois du 15 novembre 2001 relative à la sécurité quotidienne [26], du 18 mars 2003 sur la sécurité intérieure [27] ou encore celle du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité [28]. On assiste même à une inflation législative en la matière attestant de l'intégration de la Convention de Budapest. Ainsi, on cite les importantes lois du 21 juin 2004 pour la confiance dans l'économie numérique [29], du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle [30], celle du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers [31], la loi du 5 mars 2007 relative à la prévention de la délinquance [32]. On doit encore ajouter les textes règlementaires tels que le décret du 24 mars 2006 sur la conservation des données de trafic, complétant la loi sur la sécurité quotidienne [33]. Par ailleurs, compte tenu des dommages colossaux causés aux personnes et aux entreprises, la loi du 14 mars 2011 d'orientation et de programmation pour la performance, dite Loi LOPSI II, consacre l'infraction d'usurpation d'identité [34]. Mais, il convient également de compléter ce vaste corpus normatif par les lois plus récentes telles que celle du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme et qui consacre le vol des données informatiques [35], et la loi du 24 juillet 2015 relative au renseignement [36]. Cette liste, non exhaustive, atteste d'un accroissement normatif « quelque peu ésotérique, y compris pour les praticiens qui n'utilisent pas ces textes au quotidien » [37]. Il en est résulté une liste d'infractions très étendue relevant de la cybercriminalité, soit 475 qualifications pénales. Plus précisément, le Pôle d'évaluation des politiques pénales de la Direction des Affaires Criminelles et des Grâces (Ministère de la Justice) a établi une liste de ces infractions. Ces listes résultent d'une extraction de la table NATINF (Nature d'Infraction) qui recense l'ensemble des infractions définies par les normes précédemment citées. Ainsi, ont été dénombrées 248 infractions concernant spécifiquement la cybercriminalité, soit par leur objet, soit par leur mode de commission. Il s'agit notamment des atteintes relatives aux traitements de données personnelles, des atteintes aux systèmes de traitement automatisé de données, des atteintes aux réseaux, des infractions commises par la voie électronique visant la protection des œuvres, des infractions relatives à la captation frauduleuse de programmes, des atteintes aux intérêts fondamentaux de la Nation. Par ailleurs, 181 autres infractions ont été répertoriées parce qu'elles correspondent à des infractions commises par le moyen d'un système de traitement automatisé de données. En d'autres termes, si ces infractions ne relèvent pas directement de la cyberdélinquance, elles intègrent son domaine parce qu'elles sont commises par le biais d'un système d'information. Il s'agit, par exemple, des menaces contre les biens ou des atteintes à la propriété intellectuelle. Enfin, une autre liste de 46 infractions doit être ajoutée. Ces infractions concernent les communications électroniques prévues par le Code des Postes et des communications électroniques. La multiplicité des infractions concernant la cybercriminalité est donc manifeste. Pour autant, ce

[26] Loi n° 2001-1062 du 15 novembre 2001, JORF 16 novembre 2001, p. 18 215
[27] Loi n° 2003-239 du 18 mars 2003, JORF 19 mars 2003, p. 4761
[28] Loi n° 2004-204 du 9 mars 2004, JORF 10 mars 2004
[29] Loi n° 2004-575 du 21 juin 2004, JORF n° 0143 du 22 juin 2004, p. 11 168
[30] Loi n° 2004-669 du 9 juillet 2004, JORF n° 159 du 10 juillet 2004, p. 12 483
[31] Loi n° 2006-64 du 23 janvier 2006, JORF n° 0020 du 24 janvier 2006, p. 1129
[32] Loi n° 2007-297 du 5 mars 2007, JORF n° 0056 du 7 mars 2007, p. 4297
[33] Décret n° 2006-358 du 24 mars 2006, JORF n° 73 du 26 mars 2006, p. 4609
[34] Loi n° 2011-267 du 14 mars 2011 d'Orientation et de programmation pour la performance de la sécurité intérieure, Loi LOPSI II, loi précitée ; article 226-4-1 du Code pénal
[35] Loi n° 2014-1353 du 13 novembre 2014, JORF 14 novembre 2014, p. 19162 ; E. Chauvin, Quand la lutte anti-terroriste fait évoluer la notion de vol : les modifications de l'article 323-3 du Code pénal introduites par l'article 16 de la loi du 13 novembre 2014, Gazette du palais, Ed. G., Mercredi 15-jeudi 16 avril 2015, n° 105 à 106, p. 6-8
[36] Loi n° 2015-912 du 24 juillet 2015, JORF n° 171 du 26 juillet 2015, p. 12735
[37] M. Quémener et J. Ferry, *Cybercriminalité, Défi mondial*, op.cit., spéc. p. 6

n'est pas la densité de la norme répressive qui rend celle-ci effective. En réalité, la multiplicité des infractions en matière de cybercriminalité crée le risque d'un concours de qualifications, alors que la règle est l'unicité de la qualification pour un seul fait commis. Si la problématique du concours de qualifications n'est pas nouvelle, elle recouvre depuis les années 2000 une dimension particulière en matière de délinquance d'affaires, notamment s'agissant de la corruption internationale, de la concurrence déloyale et des ententes illicites [38]. Or, en matière de cybercriminalité, le problème du concours de qualifications se pose avec une dimension d'autant plus particulière compte tenu de la spécificité de cette délinquance : non seulement 475 infractions sont concernées, soit autant de normes traitant de la commission d'actes dans le cyberespace, mais celui-ci offre des modes de commission très diversifiés conférant une certaine ubiquité de l'acte infractionnel. Ainsi, on peut citer l'exemple de la consécration du vol de données en 2014, interférant avec l'infraction de vol classique. Il s'agit de protéger les informations, notamment économiques des entreprises. Dès lors, le fait « …d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient » est sanctionné de 5 ans d'emprisonnement et de 150 000 euros d'amende [39]. D'abord, ces qualifications peuvent entrer en conflit avec les dispositions relatives à la contrefaçon [40]. Ensuite, s'agissant plus particulièrement du vol des données, on note une surabondance normative parce que les juridictions ont déjà admis le vol des données sur la base du vol de droit commun. En effet, la jurisprudence en matière de vol d'informations a été riche et très évolutive : elle a admis le vol de données lorsque celui-ci a été matérialisé par un support [41]. Elle est même allée plus loin en admettant le vol de données sans nécessité de support [42]. Ainsi, dans une affaire récente, le vol d'informations par le truchement du texte classique relatif à « la soustraction frauduleuse de la chose d'autrui » [43] a été à nouveau consacré, même si la jurisprudence s'est montrée prudente [44]. Si l'on peut affirmer que cette nouvelle norme consacre une autre forme de protection de l'information [45], il n'en demeure pas moins des risques de redondances et de conflits de qualifications attestant de la relative efficacité répressive.

De surcroît, cette densité normative est matérialisée à travers un outil répressif éclaté : il s'agit de la parcellisation de l'outil pénal. Celui-ci, certes riche, n'en demeure pas moins dispersé dans des supports distincts, ce qui pose la problématique de son accessibilité. Dès lors, les incriminations citées précédemment, existent dans le Code pénal (les atteintes aux STAD), dans le Code de propriété intellectuelle (atteintes à la propriété intellectuelle), dans le Code monétaire et financier (contrefaçon des moyens de paiement), dans le Code de la consommation, dans la loi sur la liberté de la presse et dans la loi pour la confiance dans l'économie numérique. Il en ressort un éparpillement de textes normatifs attestant d'intentions législatives distinctes. De

[38] C. Grynfogel, « Le concours de volontés entre entreprises, une notion protéiforme en droit communautaire des ententes » *Revue de Jurisprudence de Droit des Affaires* 2005, p. 551 s ; B. Pereira, « Ethique commerciale, bonne gouvernance des entreprises et corruption internationale », *Revue Internationale de Droit Economique* 2008, 1, pp. 5-25, spéc. P. 14

[39] Article 323-3 du Code pénal

[40] Article L. 335-2 du Code de propriété intellectuelle

[41] Cassation criminelle 12 janvier 1989, Bourquin, Bull. crim. n° 14, Revue des Sciences criminelles 1990, p. 346 et s., observations P. Bouzat ; Cassation criminelle 1er mars 1989, Antoniolli, Bull. crim. n° 100

[42] Cassation criminelle 4 mars 2008, n° 07-84002 ; Cassation criminelle 20 mai 2015, n° 14-81336 PB ; E. Chauvin, « Hacker n'est pas jouer : maintien et vol dans un système automatisé de traitement de données », *Les PA*, 29 juillet 2015, n° 150, pp. -15-18

[43] Article 311-1 du Code pénal

[44] P. Berlioz, « Quelle protection pour les informations économiques secrètes de l'entreprise », *Revue Trimestrielle de Droit commercial* 2012, p. 263

[45] M. Vivant, « La privatisation de l'information par la propriété intellectuelle », *Revue Internationale de Droit Economique* 2006, 4, pp. 361-388

même, on a soulevé un défaut de cohérence, les outils normatifs souffrant « d'hétérogénéité » [46]. Ainsi, diverses dispositions visent à la fois « la voie électronique » [47], « le moyen de communication électronique » [48] ou encore le « réseau de communication au public en ligne » [49]. Or, si la loi pénale est d'interprétation stricte, tant il est question de caractérisation de la fraude entraînant une peine privative de liberté, cette hétérogénéité rend la tâche peu aisée.

Cependant, les actes des cyberdélinquants sont évolutifs, ce qui explique en partie l'accroissement de la norme. Ainsi, les modes opératoires susceptibles de caractériser, notamment, les atteintes aux systèmes de traitement automatisé de données des entreprises, connaissent sans cesse des mutations, ce qui nous conduit à la question de la détermination des responsables.

2.2 L'extension répressive freinée par les difficultés de détermination des responsables

Sur le plan pénal « nul n'est responsable que de son propre fait » [50]. La commission d'actes de cyberdélinquance conduit alors à la responsabilité pénale de son propre fait, qu'il s'agisse de l'auteur de l'infraction ou du complice de celle-ci. Toutefois, les actes infractionnels commis sur le web recouvrent des spécificités : qu'en est-il des prestataires techniques et prestataires de service, tels que les fournisseurs d'accès à internet, les hébergeurs (2.2.1.) ? Par ailleurs, comment localiser les actes compte tenu des éléments d'extranéité propres au cyberespace, les hébergeurs, pouvant exercer depuis plusieurs territoires distincts (2.2.2.) ?

2.2.1 La qualité des responsables

Le principe de responsabilité personnelle conduit à se demander quelle responsabilité pénale peut être encourue par les différents acteurs opérant dans le cyberespace : il s'agit des fournisseurs d'accès à internet (FAI), des hébergeurs, et des éditeurs. Or, si ces différents acteurs sont présents lorsqu'une infraction est commise dans le cyberespace, tous ne peuvent être tenus responsables. D'abord, les hébergeurs sont des personnes physiques ou morales qui assurent, à titre onéreux ou à titre gratuit, des services de communication en ligne permettant le stockage d'écrits, d'images, de sons, de signaux ou de messages de toute nature. Les bénéficiaires peuvent être les entreprises comme le public. Selon le principe de responsabilité personnelle, les hébergeurs ne peuvent être déclarés pénalement responsables à raison des informations stockées à la demande d'un destinataire, si ces hébergeurs n'ont pas eu connaissance de l'information illicite [51]. Les hébergeurs ne seront pas non plus responsables si dès le moment où ils ont eu une connaissance effective de l'information illicite, ils ont agi promptement pour retirer ces informations ou en rendre l'accès impossible. Ainsi, dans une affaire relative à des propos diffamatoires à l'encontre d'une société commerciale, il a été jugé que l'hébergeur ne pouvait être déclaré pénalement responsable parce qu'il avait promptement rendu le site litigieux inaccessible [52]. Il s'agit d'un régime de responsabilité dérogatoire issu de la directive européenne du 8 juin 2000 relative au commerce électronique. Ce régime de non responsabilité est fondé sur le fait que l'activité de stockage ne conduit les hébergeurs à être ni

[46] M. Robert, Rapport sur la cybercriminalité, rapport précité, p. 159
[47] Article 226-15 du Code pénal
[48] Article 227-22-1 du Code pénal ; articles 706-25-2, 706-35-1, 707-47-3 du Code de procédure pénale
[49] Article 226-4-1 du Code pénal ; articles L. 335-7 et suivants du Code de propriété intellectuelle
[50] Article 121-1 du Code pénal ; B. Pereira, « Responsabilité pénale », *Encyclopédie- Répertoire* Dalloz, 2002
[51] Directive européenne 2000/31 CE sur le commerce électronique du 8 juin 2000, JOUE n° 178 du 17 juillet 2000, p. 1
[52] TGI de Paris, Ordonnance de référé du 9 juillet 2004, Affaire Groupama/ Gérard D, Free, http// :www.legalis.net

des auteurs, ni des complices des contenus infractionnels. Il en est de même dans les autres Etats. Par exemple, en Allemagne, l'hébergeur est celui qui fournit des contenus d'une personne à d'autres personnes en hébergeant les informations [53]. La responsabilité des hébergeurs ne peut être retenue que s'ils ont eu connaissance des contenus illicites et s'ils n'ont pas informé les autorités publiques. L'Espagne, l'Italie et la Belgique vont dans le même sens conformément à la Directive [54].

Le principe est le même pour les fournisseurs d'accès à Internet (FAI), la responsabilité pénale ne pouvant être retenue si les faits ne leur sont pas personnellement imputables. Les FAI, prestataires de service, sont des acteurs qui permettent l'accès à un réseau de télécommunications et qui assurent l'activité de transmission de contenu. Les FAI peuvent être à la fois des fournisseurs d'hébergement. Il s'agit de l'irresponsabilité de principe. Comme pour les hébergeurs, ils ne sont pas soumis à une obligation générale de surveillance des informations.

En revanche, il en va différemment pour les éditeurs, la responsabilité pénale pouvant être retenue eu égard à la maîtrise qu'ils ont du contenu informationnel. L'éditeur correspond à l'acteur dont l'activité est d'éditer un service de communication au public en ligne [55]. Il est alors responsable de plein droit de l'ensemble des informations qu'il publie à l'inverse des prestataires techniques. En effet, l'éditeur répond de ses actes si les messages publiés ont un caractère public. Si l'auteur du contenu illicite publié est responsable directement sur le plan pénal, l'éditeur l'est également parce qu'il assure la maitrise éditoriale. Ainsi, le directeur de publication est responsable lorsqu'il est en mesure de prendre connaissance et de contrôler les informations avant leur diffusion [56]. Cette distinction entre la non-responsabilité d'un hébergeur et la responsabilité de l'éditeur est bien comprise parce que l'éditeur est celui qui est personnellement à l'origine de la diffusion des contenus : en exerçant un choix éditorial, il peut être déclaré responsable des contenus illicites. Il en est de même pour les auteurs de blogs qui sont à la fois les auteurs des articles mis en ligne et l'éditeur [57].

Toutefois, selon les circonstances, la distinction entre hébergeur et éditeur n'est pas toujours évidente, ce qui rend la détermination des responsables difficile. Il en est ainsi lorsqu'on s'intéresse aux plateformes. Les juges ont eu l'occasion de requalifier un hébergeur en éditeur parce que son activité dépassait celle du simple stockage. Dès lors, certaines plateformes ont pu être requalifiées en éditeur parce qu'en plus de l'activité de stockage de données, elles exercent, un choix éditorial, soit en organisant des rubriques, des thèmes, soit en intégrant une publicité sur les pages hébergées [58]. De même, il a été jugé que la plateforme qui développe une activité commerciale rémunérée sur la vente aux enchères, ne se limite pas à une activité d'hébergement de sites. Cette plateforme doit alors être requalifiée d'éditeur [59]. En réalité, compte tenu de

---

[53] Article 9 de la loi du 14 janvier 2001 de la loi allemande : voir notamment Lionel Thoumyre, « Valse constitutionnelle à trois temps sur la responsabilité des intermédiaires techniques », *Légipresse, tribune*, septembre 2004

[54] Article 14 de la loi espagnole n° 34/2002 du 11 juillet 2002 sur les services de la société de l'information et sur le commerce électronique ; Article 16 du décret italien du 9 avril 2003 ; loi du 9 avril 2003 (Italie) : L. Toumyre, « Comment les hébergeurs français sont devenus juges du manifestement illicite », *juriscom.net, Droit des technologies de l'information,* 2004

[55] Article 6-III-1° de la loi pour la confiance dans l'économie numérique

[56] Cour EDH 30 mars 2004, Requête n° 53984/00 (deuxième section), Affaire RadioFrance et autre c/ France

[57] CA Paris, 6 juin 2007, http : //www.legalis.net

[58] CA de Paris, 29 octobre 2008, MySpace c/ Lafesse ; Ph. Stoeffel-Munck, Communication, Commerce électronique, Revue Juris classeur, 2009, p. 36

[59] Tribunal de commerce de paris, 30 juin 2008, Christian Dior Couture c/eBay Inc., eBay International AG

l'absence de précision légale sur la distinction exacte entre les hébergeurs et les éditeurs, il appartient au juge de qualifier ces acteurs. Or, cette qualification selon les circonstances est lourde de conséquences : si la qualification d'hébergeur est retenue, il s'agira d'une non-responsabilité ; si la qualification d'éditeur est retenue, la condamnation pénale sera possible. Certes, la Cour de Justice de l'Union européenne [60] nous donne des éléments permettant de distinguer l'hébergeur de l'éditeur. Il s'agit du critère de la passivité du prestataire technique. Dès lors que le prestataire technique ne joue qu'un rôle neutre et n'a qu'un comportement technique, automatique et passif qui conduit à l'absence de connaissance ou de contrôle des données qu'il stocke, on ne peut retenir sa responsabilité. L'activité d'hébergeur correspond à ce comportement technique et à l'absence de connaissance empêchant toute reconnaissance de la responsabilité. En revanche, l'éditeur dispose d'un rôle actif et de la connaissance des contenus qu'il publie. Toutefois, les critères de neutralité et de passivité dégagés par la CJUE n'empêchent pas les hésitations pour qualifier tous les acteurs agissant dans le cyberespace. Ces hésitations se manifestent encore aujourd'hui lorsqu'il est question de soulever la responsabilité des moteurs de recherche. Les moteurs de recherche permettent de procéder à une interrogation par mots clés et d'accéder aux références de documents, en très grand nombre, qui ont été indexés. Afin de garantir des recherches rapides et effectives, des suggestions de recherche peuvent être automatiquement formulées aux utilisateurs. Dès lors, les moteurs de recherche peuvent mettre à disposition selon les lettres d'un mot saisies, un menu déroulant de propositions qui comportent une liste de requêtes possibles. Ce procédé dispense les utilisateurs de taper le libellé complet de leur recherche. La question du rôle passif ou actif des moteurs de recherche est alors posée : sont-ils des hébergeurs irresponsables ou des éditeurs responsables pénalement ? La Cour de cassation y a répondu en 2013 s'agissant de la Société Google et de la Société Lyonnaise de garantie [61] : « la fonctionnalité aboutissant au rapprochement critiqué (des mots) est le fruit d'un processus purement automatique dans son fonctionnement et aléatoire dans ses résultats, de sorte que l'affichage des mots clés qui en résulte est exclusif de toute volonté de l'exploitant du moteur de recherche »[62]. En d'autres termes, le rôle du moteur de recherche correspond à celui d'un hébergeur, compte tenu de l'automaticité de sa fonction, cette automaticité ne lui conférant pas de rôle actif. Cependant, un jugement postérieur prend le contrepied de la décision de la Cour de cassation s'agissant du même moteur de recherche Google : « si l'éventuelle responsabilité de l'exploitant ne peut être appréciée en fonction du régime applicable à celui de l'expression de la pensée humaine, cette analyse ne saurait conduire à l'exclusion de toute responsabilité »[63]. Cette décision est à rapprocher des conclusions de l'avocat général de la Cour de Justice de l'Union européenne du 25 juin 2013 concernant l'affaire *Google contre Agencia Espanola de Proteccion de Datos* [64] : l'accessibilité universelle des informations sur internet dépend des moteurs de recherche qui jouent un rôle déterminant pour la société de l'information. Ces moteurs de recherche peuvent alors renforcer la portée des contenus infractionnels. Aussi, pouvons-nous rappeler que sur le plan civil, la Cour de cassation française avait déjà rendu une décision en ce sens en précisant que la fonctionnalité Google

[60] CJUE 23 mars 2010, C-236/08, Google France c/ Louis Vuitton (Grande chambre), CuriaEUR-Lex ECLI :EU :C : 2010 : 159

[61] Cassation civile 1ère, 19 juin 2013, C.CASS : 2013 : C 100625, Sté Google Inc c./ Sté Lyonnaise de Garantie ; C. Castets-Renard, « La fonctionnalité Google Suggest mise hors de cause », *Revue Lamy Droit de l'immatériel,* n° 96, pp. 67-69, août 2013 ; E. Derieux, « Exclusion de la responsabilité des suggestions d'un moteur de recherche », *Revue Lamy Droit de l'immatériel*, n° 96, pp. 63-66, août 2013

[62] Cassation civile 1ère, 19 juin 2013, arrêt préc.

[63] TGI Paris 17ème Chambre, 23 octobre 2013, B. Lallement c./ Sté Google France et autres : E. Derieux, « Editeur ou hébergeur : la responsabilité d'un moteur de recherche », *La Revue Européenne des médias et du numérique*, n° 29, hiver 2013-2014

[64] CJUE 13 mai 2014, C-131/12, *Google contre Agencia Espanola de Proteccion de Datos*

Suggestion permettant une association des termes de recherche avec des suggestions automatiques, contribuait au téléchargement illégal [65]. Mais, il n'en demeure pas moins que ces décisions ne sont pas uniformes et relatent de nombreuses hésitations. Il en ressort une forme d'insécurité juridique tenant à l'appréciation des activités des acteurs dans le cyberespace. De surcroît, aux difficultés de détermination des responsables, on doit ajouter celles de la localisation des actes infractionnels.

2.2.2 La localisation des actes : quelle territorialité ?

La localisation des infractions recouvre une importance capitale quant à l'applicabilité de la norme sur le plan territorial et à l'identification des cyberdélinquants. Néanmoins, traiter de la localisation des cyberinfractions revient à concilier le caractère délimité de la règle pénale au niveau de l'espace et le caractère universel des réseaux numériques. Ces derniers offrent l'ubiquité et l'immédiateté des échanges d'informations. Or, au sein du cyberespace mondial, l'efficacité du droit répressif souffre d'une certaine relativité compte tenu de son caractère essentiellement souverainiste [66]. En dépit d'une coopération interétatique, la cybercriminalité est régie par les droits pénaux nationaux. Si les conventions internationales permettent de s'acheminer vers l'harmonisation des législations, les souverainetés nationales coexistent, de même que leurs expressions sous forme de réserves étatiques. Ainsi, le droit répressif demeure une expression territorialisée de la souveraineté des Etats. Dès lors, on se pose la question de savoir si le critère de la territorialité répond efficacement aux enjeux de la lutte contre la cybercriminalité. Dès lors que l'infraction peut être localisée sur le territoire national, la loi et les juridictions de l'Etat visé sont compétentes. Ainsi, la loi pénale française est applicable aux infractions commises ou réputées commises sur le territoire de la République [67]. Il en est de même dans les autres Etats, la tendance consistant à étendre le critère de compétence de territorialité pour sanctionner les crimes et délits localisés même partiellement sur un territoire [68]. Les infractions commises dans le cyberespace sont alors réprimées par les normes nationales territorialement compétentes [69]. Néanmoins, même étendue, l'applicabilité du principe de territorialité souffre de certaines limites face à l'universalité d'internet. Ces limites tiennent moins à « un inquiétant vide juridique en raison du caractère insaisissable des flux transfrontaliers » qu'à la multiplication des normes et juridictions compétentes [70]. En réalité, tous les Etats du monde sont susceptibles de se déclarer compétents à travers l'application du principe de territorialité, ce qui conduit à des conflits de compétences, en dépit du principe Non bis in idem. Dès lors, l'harmonisation des législations nationales n'empêche pas les juridictions et les Etats de se déclarer compétents en dépit de la chose jugée à l'étranger [71]. Il en ressort des risques de chevauchements des poursuites.

Plus concrètement, les infractions commises dans le cyberespace impliquent un réseau électronique. Pour les localiser, faut-il privilégier le lieu d'émission des messages lorsqu'il

---

[65] Cassation civil (1ère chambre), 12 juillet 2012, n° 11-20.358

[66] M. Delmas-Marty, *Les forces imaginantes du droit*, t. 1, Le relatif et l'universel, éd. Du Seuil, 2004, spéc. p. 336

[67] Article 113-2 du Code pénal

[68] D. Rebut, *Droit pénal international*, Précis Dalloz, 2014, 2ème édition ; Cassation criminelle 12 février 1979, Bull. crim. n° 60 ; 1er octobre 1986, n° 262 ; 26 septembre 2007, n° 224

[69] Cassation criminelle 11 septembre 2007, n° 07-82018 ; 4 février 2004, Bull. crim. n° 32, D. 2005, p. 621, note V. Malabat ; 6 août 2008, n° 08-83490

[70] J. Francillon, « Cybercriminalité- Aspects de droit pénal international », *Revue électronique de l'Association Internationale de droit pénal*, 2014, RH-7, 37 pages, spécialement page 7

[71] Conseil de l'Europe, Rapport d'évaluation : les dispositions de la convention de Budapest sur la criminalité concernant l'entraide, T-CY, Comité de la Convention de cybercriminalité, Strasbourg, France, 3 décembre 2014, 216 p.

s'agit de messages litigieux, le lieu de réception de ces messages, ou encore l'accessibilité lorsqu'il s'agit de sites ? Or, sur ce point la jurisprudence est contradictoire. Si l'on se réfère au lieu d'émission des informations ou au lieu d'origine, cela conduirait les cybercriminels à s'établir dans des pays à la législation permissive ; si l'on se réfère au lieu de réception, celui où le site étranger peut être accessible, cela permettrait à tous les pays où le site est accessible de se déclarer territorialement compétents : il s'agirait alors d'une problématique de chevauchement de compétences et corrélativement d'une insécurité juridique [72]. Dans un premier temps, la jurisprudence a privilégié le critère de réception pour les messages, et celui de l'accessibilité des sites s'agissant d'internet (apologie des crimes de guerre) [73]. Puis, la jurisprudence est allée dans le même sens en matière d'infractions relatives à la presse [74]. Il en a été de même dans une affaire de dénigrement de produits pharmaceutiques [75] et en matière d'infraction à la règlementation des jeux et paris en ligne [76].

En revanche, il en a été autrement en matière de contrefaçon de droits d'auteurs et de droits voisins. En effet, il a été décidé que la condition nécessaire pour que le délit soit réputé commis en France, était le critère de la focalisation : le délit doit être orienté vers le public français [77]. Cette jurisprudence est plus restrictive que la précédente parce qu'elle impose de rechercher si le public de telle nationalité est bien le destinataire du site infractionnel. Le critère de la focalisation est donc plus étroit que celui de l'accessibilité du site. En réalité, on observe que les cyberinfractions sont diverses et que l'expression du principe de la territorialité diffère selon les infractions. En matière de contrefaçon et de cyberdélit de nature économique, la territorialité trouve une application distincte des autres infractions commises dans le cyberespace. Il convient alors de se rapprocher de la jurisprudence communautaire qui a traité de cette problématique dans la sphère délictuelle. Or, la problématique recouvre des similitudes.

Les décisions de la Cour de Justice de l'Union européenne ont été rendues sur la base de l'interprétation de l'article 5.3 du Règlement de Bruxelles I lequel permet de déterminer le juge compétent en matière délictuelle [78]. Selon cet article, une personne domicilée sur le territoire d'un Etat membre peut être attraite dans un autre Etat membre, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire. La CJUE s'est prononcée sur la problématique de la localisation du cyberdélit notamment en matière de droit de la personnalité et de marque [79]. Cette jurisprudence a également évolué en admettant le critère de l'accessibilité, puis celui de la focalisation. Cependant, l'évolution de la jurisprudence communautaire n'en demeure pas moins « éclectique » ou « plurale » [80]. Ainsi, en matière de contrefaçon de marque,

---

[72] M. Vivant, « Cybermonde : droit et droits des réseaux », *JCP* 1996-1-3969

[73] TGI Paris, Référé 22 mai et 20 novembre 2000, *Revue Communication, Commerce Electronique* 2000, commentaire n° 92 ; TGI Paris 17ème Ch. 26 février 2002, *Revue Communication, Commerce Electronique* 2002, n° 77, Observations A. Lepage ; Paris 11ème Ch., 17 mars 2004, *Revue Communication, Commerce Electronique* 2005, commentaires n° 72, observations A. Lepage

[74] TGI Paris, 13 novembre 1998, Gazette du Palais-1-doctrine 697 ; Limoges, 8 juin 2000, BICC 2001, p. 210 ; Paris, 11ème ch., 17 mars 2004, arrêt préc.

[75] Cassation criminelle 15 janvier 2008, Bull. crim. n° 5

[76] Tribunal Corr. Nanterre, 15ème ch., 15 mars 2007, Revue des Sciences criminelles 2008, p. 101, Observations J. Francillon

[77] Cassation criminelle 14 décembre 2010, n° 10-80.088, Dalloz 2011, 1055, Observations E. Dreyer ; 12 février 2013, Société Coutellerie de la Gravona et autres, n° 11-2594

[78] Règlement CE du Conseil du 22 décembre 2000 sur la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile, commerciale : article 5 point 3 du règlement, CE n° 44/2001 du Conseil du 22 décembre 2000

[79] CJUE 12 juillet 2011, C-324/09, L'Oréal SA e.a. c./ eBay International e. a.

[80] F. Polland-Dulian, « Compétence juridictionnelle. Contrefaçon en ligne. Internet-Accessibilité », *Revue Trimestrielle de Droit commercial,* 2013, p. 733

dans l'arrêt Wintersteiger, la CJUE a considéré que peuvent être saisis les juges de l'Etat membre dans lequel est établi l'annonceur, en tant que juges du lieu où se réalise l'évènement causal ; soit les juges de l'Etat membre dans lequel la marque est enregistrée [81]. Cela revient à écarter les critères d'accessibilité ou de focalisation pour préférer l'Etat de l'enregistrement de la marque compte tenu de la spécificité du délit de contrefaçon [82].

Il ressort de ces éléments que si en matière répressive, le principe de territorialité connaît des expressions diversifiées, il en est de même sur le plan civil et commercial. Cette analyse permet de comprendre que la spécificité de la commission des cyberinfractions a conduit à un droit très dense, mais également hétéroclite souffrant d'un défaut de mise en cohérence. Or, cette relativité de l'outil répressif n'est pas compensée par la coopération internationale, celle-ci comportant certaines faiblesses.

3 LES FAIBLESSES DE LA COOPERATION INTERNATIONALE

La coopération internationale en matière de cybercriminalité recouvre une importance cruciale parce que la lutte contre ce type de délinquance internationalisée répond à un besoin commun des Etats. Toutefois, le développement de l'entraide demeure conditionné (3.1.). Par ailleurs, s'agissant de la spécificité de cette délinquance, la coopération internationale intègre aussi les entreprises prestataires techniques jouant un rôle majeur. Cependant, la coopération entre les autorités publiques et les prestataires techniques est protéiforme (3.2.).

3.1 Le développement de l'entraide pénale conditionné

Si l'ouverture des frontières conduit à la multiplication des échanges, elle accroît la criminalité transfrontalière. Dès lors, s'agissant de la cybercriminalité, on comprend que l'espace, notamment européen, ne peut être découpé en autant de sous-espaces pénaux nationaux en dépit du caractère territorialiste du domaine répressif. Il s'est donc agi de promouvoir une entraide policière et judiciaire dans la perspective de l'amélioration de la lutte contre ce type de délinquance. Ainsi, depuis la Convention du Conseil de l'Europe du 20 avril 1959 relative à l'entraide judiciaire en matière pénale [83], constituant le droit commun de la coopération interétatique, des progrès notables ont été réalisés. L'objectif poursuivi consiste à remédier aux limites des droits internes au service d'une lutte plus effective de la criminalité internationalisée. C'est le principe de la reconnaissance mutuelle des décisions judiciaires pénales qui matérialise le développement de la coopération parce qu'il vise à consacrer un espace pénal européen en permettant l'échange d'informations directement entre les autorités judiciaires et non plus seulement à travers le canal diplomatique. Partant, cette consécration, reposant sur la confiance mutuelle entre Etats membres, permet d'accélérer la recherche des preuves et l'identification des auteurs des cybercrimes. Ainsi, il existe plusieurs décisions-cadres visant à promouvoir une coopération développée comme celle du 18 décembre 2008 relative au mandat européen d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre d'une enquête [84]. Cette dernière décision-cadre présente un intérêt particulier pour la lutte contre la cybercriminalité et complète la Convention de Budapest. En effet, ces outils se révèlent particulièrement utiles quant à la recherche des cyberdélinquants sur

[81] CJUE 19 avril 2012, affaire C-523-10 Wintersteiger, Dalloz 2012, p. 1926, note T. Azzi
[82] CJUE 19 avril 2012, affaire C-523-10 Wintersteiger, arrêt précité, pt 28
[83] Convention européenne d'entraide judiciaire en matière pénale, Strasbourg 20 avril 1959, STCE n° 030
[84] Cons. UE, DC n° 2008/978/JAI, JO n° L 350, 30 décembre 2008, p. 72

le plan international eu égard au risque de déperdition des preuves dans le cyberespace. Ils permettent les échanges d'informations afin d'améliorer le mode d'obtention des preuves numériques. La possibilité d'effectuer des enquêtes extraterritoriales est également renforcée. En réalité, à l'internationalisation de la cybercriminalité, on tend vers celle de la répression. Dès lors, on comprend que le développement de la coopération tend à l'abandon de l'exigence du principe de la double incrimination selon lequel la poursuite et le jugement du délinquant ne sont possibles que si l'infraction visée existe à la fois dans l'Etat requis et dans l'Etat requérant. Le principe de la reconnaissance mutuelle des décisions judiciaires conduit alors à supprimer le contrôle de la double incrimination et facilite les échanges d'informations et de données entre les Etats.

Cependant, le développement de la coopération internationale est subordonné au respect des souverainetés nationales, et aux réserves étatiques qui en découlent : la possibilité d'enquêtes communes et d'échanges d'informations entre les autorités judiciaires des Etats membres n'est donc pas automatique. De surcroît, cette possibilité ne se substitue pas aux normes d'entraide classique issue de la convention de 1959 et conservant la possibilité de maintenir les autorisations diplomatiques pour l'échange d'informations. En d'autres termes, la confiance mutuelle entre Etats peut être écartée. La reconnaissance mutuelle des décisions judiciaires et des modes de recherche des preuves directs entre les autorités judiciaires n'est qu'une alternative aux mécanismes participant de la coopération judiciaire traditionnelle. Dès lors, les différents types de coopération (l'échange direct d'informations entre les autorités judiciaires des Etats membres ; et les autorisations Etatiques par les ministères de justice comprenant des délais très longs) coexistent [85], ce qui comporte une incidence directe en matière de lutte contre la cybercriminalité. Ainsi, ce sont les autorités étatiques qui constituent les principaux acteurs de la coopération, cette dernière intégrant une dimension intergouvernementale. Dès lors, il coexiste des positions diplomatiques fluctuantes constituant autant de conditions à la mise en œuvre de la coopération en matière de cybercriminalité. Nous sommes alors en présence d'un processus à plusieurs niveaux comprenant à la fois une coopération et une compétition, principalement entre les acteurs étatiques, le Conseil européen, et la Commission européenne [86]. Ces analyses concernent, il est vrai, l'ensemble de la lutte contre la délinquance. Toutefois, ces limites ainsi soulignées, prennent une dimension particulière lorsqu'il s'agit de cybercriminalité. En effet, de tels conditionnements de la coopération ne peuvent être en adéquation avec le développement d'une délinquance pourvue d'ubiquité et d'ingéniosité dans le cyberespace mondialisé. Ces limites sont directement exprimées à travers l'exemple du mandat d'obtention des preuves, élément crucial pour l'établissement de la preuve numérique et pour l'identification des cyberdélinquants. Or, celui-ci peut être refusé par l'Etat sollicité qui pourra préférer procéder par voie diplomatique. Le risque de déperdition des preuves est alors important, et encore davantage en matière de cybercriminalité : la réunion des éléments de preuve, comme des données et des documents immatériels, nécessite une entraide judiciaire plus directe. Cette problématique a encore été soulignée en mars 2015 par le Secrétaire exécutif du Comité de la Convention sur la Cybercriminalité : « le processus de demande d'entraide judiciaire est jugé inefficient, et en particulier pour ce qui concerne l'obtention des preuves électroniques ; les Parties semblent ne pas mettre pleinement à profit les opportunités offertes par la Convention de Budapest sur la Cybercriminalité et par d'autres accords afin de parvenir à une entraide efficace

[85] A. Mégie, « Généalogie du champ de la coopération judiciaire européenne », *Revue Cultures et Conflits*, n° 62, mars 2007, spéc. P. 7, (http://conflits.revues.org/2053)
[86] R. Putman, « Diplomacy and Domestic Politic s : the Logic of Two-Level Games», *International Organisation*, n° 42, 1988, pp. 427- 460

… » [87]. On soulève alors un certain paradoxe : si sur le plan international la norme d'entraide est conditionnée dans sa mise en œuvre, les Etats accroissent la répression sur leur territoire, démontrant alors une volonté sans équivoque de lutter contre la cyberdélinquance. Ainsi, l'entraide internationale pour la poursuite des cybercriminels est subordonnée au respect des souverainetés nationales, tandis que sur le plan national la norme répressive augmente, mais ne trouve d'expression que sur un territoire délimité pour une délinquance internationalisée. En d'autres termes, une répression accrue sur le plan national ne comporte qu'une utilité relative, si les moyens de lutte internationaux sont conditionnés eu égard au caractère transnational de cette délinquance.

Dès lors, l'accroissement des mesures coercitives développées sur chaque territoire recouvre une efficacité réduite si les données permettant de poursuivre les cyberdélinquants ne sont pas partagées entre les autorités. C'est le cas des saisies informatiques : les enquêteurs peuvent procéder à la saisie des données informatiques nécessaires à la manifestation de la vérité [88]. Par ailleurs, les saisies peuvent concerner tout un réseau d'ordinateurs. Les enquêteurs nationaux peuvent même procéder à des fouilles alors même que les systèmes informatiques sont situés à l'extérieur du territoire national [89]. Cependant, ces dernières fouilles ne sont possibles que si les données visées ne font pas l'objet d'un refus par l'Etat visé, ou si elles sont accessibles au public. On voit bien les limites caractérisant la problématique d'efficacité de la lutte contre la cybercriminalité : ces limites tiennent aux conditions de consentement des Etats. De plus, les autorités judiciaires nationales ne peuvent communiquer entre elles que si les services destinataires donnent des garanties suffisantes quant au respect des droits fondamentaux des personnes visées par l'enquête. Dès lors, l'accroissement répressif national ne peut être utile que s'il est susceptible d'être partagé avec d'autres autorités nationales, ou s'il est susceptible d'une portée extraterritoriale. Ainsi, on peut citer l'exemple des nouvelles dispositions relatives au renseignement issues de la loi du 24 juillet 2015, attestant de l'accroissement répressif national. Cette nouvelle loi permet, sur le plan administratif et non plus judiciaire, de procéder au recueil de renseignements par des techniques spéciales (algorithmes) dans le domaine de la sécurité nationale, des intérêts essentiels de la politique étrangère, des intérêts économiques ou scientifiques essentiels, de la prévention du terrorisme, de la prévention de la reconstitution ou du maintien de groupements dissous, de la prévention de la criminalité organisée et de la prévention des violences collectives pouvant porter gravement atteinte à la paix publique [90]. La cybercriminalité est directement concernée par ces nouvelles dispositions. Mais, il s'agit d'un dispositif interne qui ne peut intégrer le critère d'efficacité que si les renseignements font l'objet d'un échange réciproque entre les Etats. Il en est de même en dehors du cadre européen. Les conventions bilatériales de coopération promeuvent les échanges d'informations en même temps que leur conditionnement. Ainsi, le nouvel accord UE-Etats-Unis, l'accord PNR adopté le 19 avril 2012 par le Parlement européen et le 26 avril 2012 par le Conseil de l'Union européenne [91] vise à mettre en place un cadre juridique régissant le transfert de données des dossiers-passagers par les compagnies aériennes et maritimes, assurant le transport de passagers entre l'UE et les

[87] A. Seger, « La coopération internationale contre la cybercriminalité : stratégie et défis », *Conseil de l'Europe*, 9-10 mars 2015, p. 12
[88] Articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale ; D. Bénichou, « Cybercriminalité : jouer d'un nouvel espace sans frontière », *Revue AJ pénal* 2005, p. 224
[89] Article 57-1 alinéa 2 du Code de procédure pénale
[90] Article L. 811-3 du Code de sécurité intérieur, issu de la loi du 24 juillet 2015
[91] Accord Passenger Name Record, doc. 17434/11

Etats-Unis[92]. Cet accord visant principalement la lutte contre le terrorisme, comprend aussi la cybercriminalité puisque cette dernière intègre les infractions relatives au financement du terrorisme et celles relatives à l'apologie des crimes terroristes. Cependant, cet accord trouve encore des difficultés de mise en œuvre eu égard au souci de protéger les droits fondamentaux [93]. C'est alors le difficile dialogue transatlantique sur la conciliation sécurité et liberté eu égard à une conception différente de la protection des droits individuels qui constitue le frein à une coopération en matière d'échanges d'informations [94]. Dès lors, si la coopération interétatique est conditionnée, il convient de rechercher d'autres moyens permettant de mieux asseoir cette lutte : la coopération entre les autorités publiques et les acteurs économiques, soit les prestataires techniques.

3.2 Le caractère protéiforme de la coopération entre les autorités publiques et les prestataires techniques

La lutte contre la cybercriminalité recouvre une spécifique en matière de preuve numérique, celle-ci étant fragile. Dès lors, la poursuite des cyberdélinquants conduit les autorités publiques à traiter avec les acteurs économiques. Sur ce point, les mécanismes de régulation sont multiformes : d'abord, les autorités judiciaires peuvent procéder à des mesures d'injonction, soit de fournitures d'informations, soit de blocage de sites auprès des prestataires techniques. Il s'agit d'une coopération contrainte aux résultats peu effectifs ; ensuite, une forme d'autorégulation a été mise en place à travers le développement de chartes et codes de conduite. Il s'agit d'une coopération contractualisée souffrant d'un défaut d'encadrement et révélant l'absence d'une politique globale de lutte contre la cybercriminalité.

D'abord, s'agissant des mesures d'injonction, les autorités judiciaires peuvent s'adresser aux fournisseurs d'accès à internet et hébergeurs afin d'obtenir des informations sur des infractions commises et les auteurs de celles-ci. Certes, comme il l'a été soulevé précédemment, les FAI et les hébergeurs bénéficient du principe de l'irresponsabilité civile et pénale. Ils ne sont pas non plus soumis à une obligation générale de surveillance des informations qu'ils stockent et transmettent, ni même à celle de rechercher des infractions [95]. Toutefois, les mesures d'injonction judiciaire auprès de ces prestataires sont possibles. Il peut s'agir de réquisitions informatiques prévues lors des enquêtes et instructions : les prestataires de service sont alors tenus sous peine d'amende de fournir les informations sollicitées [96]. Cela conduit à la question de la conservation des données par les prestataires techniques. Or, la conservation des données n'obéit pas à un régime univoque permettant une coopération sur le plan international. L'obligation de conservation des données constitue le moyen d'obtenir les éléments de preuve. Par ailleurs, la Directive 2006/24/CE du 15 mars 2006 impose aux Etats membres de prévoir

---

[92] S. Peyrou, « De l'accord PNR à Prism, Bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », *Réseau Universitaire Européen, Droit de l'Espace de Liberté, sécurité et Justice* (ELSJ), CNRS, 2013 (http://www.gdr-elsj.eu/2013)

[93] P. Tavola, « Un premier feu vert donné par le Parlement européen. Un compromis entre sécurité et droit à la vie privée, des nouvelles pressions pour l'adoption du dossier après l'attaque du Thalys, Amsterdam-Paris », 8 septembre 2015, *ELSJ* (http://europe-liberté-securite.org/2015

[94] Article 8 de la Charte des Droits fondamentaux de l'Union européenne ; Douzième Congrès des Nations Unies pour la prévention du crime et de la justice pénale- Une coopération internationale insuffisante permet aux cybercriminels de s'en tirer à bon compte, Salvador (Brésil), 12-19 2010

[95] CJUE 16 février 2012, C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) ; E. Derieux, « Neutralité de l'internet. Fournisseurs d'hébergement. Impossible obligation générale mais possibles obligations particulières de surveillance et de filtrage », *Revue Lamy Droit de l'Immatériel* 2012/80, n° 2666

[96] W. Duhen, « Réquisitions judiciaires et conservation de données de connexion en ligne », *Revue AJ Pénal* 2011, p. 184

cette obligation de conservation à la charge des opérateurs de téléphonie fixe et mobile et des fournisseurs d'accès à internet pour une durée comprise entre 6 et 24 mois à compter de la communication. Le droit français prévoit une durée d'un an. Toutefois, si en Europe, la durée de conservation des données ne pose pas de grande difficulté, il en va différemment pour les sociétés commerciales américaines : ces dernières connaissent des pratiques diversifiées. Par exemple, le moteur de recherche Google efface les données des comptes devenus inactifs après une durée indéfinie ; Twitter fait référence à une durée maximale de 18 mois, alors que la pratique a révélé une durée de conservation de 2 à 3 mois. De plus, cette hétérogénéité est aggravée par des refus de se soumettre aux réquisitions. La volonté de coopérer comporte alors des degrés variables selon les entreprises et leurs localisations. Ainsi, Google et facebook ne répondent que partiellement aux réquisitions d'informations sous la condition que les utilisateurs soient européens et si la communication de l'information se limite au critère de l'adresse IP. Certains prestataires refusent toute transmission d'informations, mais avisent les autorités du pays visé (Facebook) ; Twitter limite la transmission d'informations au « serious crime » éliminant toute coopération en matière de délit de presse [97]. Il en ressort une coopération fortement ralentie en matière de cybercriminalité. Ces refus de coopération des grands opérateurs dénotent avec une coopération élargie de ces mêmes prestataires auprès des services du Federal Bureau Investigation (FBI) et de la National Security Agency (NSA) [98]. La problématique est la même en matière d'injonction de blocage des sites illicites, la coopération suscitant des difficultés de mise en œuvre et révélant le caractère protéiforme des pratiques [99].

Ainsi, face au refus de coopération des prestataires techniques selon leur localisation [100], il reste la possibilité de la démarche volontaire. Cette dernière a pu être matérialisée à travers le développement de chartes de conduite. Ce procédé a par ailleurs été préconisé par le Conseil de l'Europe afin de permettre de développer des partenariats entre les prestataires techniques et les autorités. Par exemple, lors de la conférence Octopus en avril 2008, des lignes directrices pour la coopération entre organes de répression et fournisseurs de service internet contre la cybercriminalité ont été adoptées. Ces lignes ont alors permis de concrétiser un accord entre le Conseil de l'Europe et Microsoft en décembre 2013 [101]. Il s'agit d'une contractualisation relevant du partenariat public-privé [102] qui présente l'avantage de faire progresser la lutte contre la cybercriminalité sur la base de l'initiative volontaire. On peut, par exemple, citer la Charte des fournisseurs d'accès dans la lutte contre le piratage de la musique (Juillet 2004) ; la Charte des plateformes en matière de commerce électronique (juillet 2006) ; la Charte de déontologie des sites comparateurs de prix (décembre 2009) [103]. L'utilité de ces partenariats réside dans l'incitation faite aux prestataires techniques de coopérer pour détecter la fraude. Mais, cette

[97] M. Robert (sous la direction de), Rapport sur la cybercriminalité, rapport précité, spéc. page 179

[98] En effet, Google, Yahoo, Microsoft, Skype, YouTube, Apple, AOL, Facebook, PalTalk ont permis l'accès aux données de leurs utilisateurs par le biais du système Prism : Cf not. S. Peyrou, « De l'accord PNR à Prism, Bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », article précité, p. 3

[99] A. Neri, « L'injonction de filtrage rendue à l'égard d'un intermédiaire : une mesure controversée aux conséquences redoutables », *Revue Communication, Commerce Electronique* 2012, étude 3

[100] A. Desforges, « La coopération internationale et bilatérale en matière de cybersécurité : enjeux et rivalités », *ISERM, Institut de Recherche Stratégique de l'Ecole Militaire*, 15 pages, spécialement p. 9 sur « une coopération qui reste superficielle ».

[101] M. Robert (sous la direction de), Rapport sur la cybercriminalité, rapport précité, spéc. page 170

[102] L. Cohen-Tanugui, *Le droit sans l'Etat*, PUF, Paris, 1985 ; G. Cliquet et G. Orange (sous la dir.), *Organisations privées, Organisations publiques*, Mélanges Robert Le Duff, 2002, Publications de l'Université de Rouen ; P. Le Galès, « Aspects idéologiques du partenariat public-privé », *Revue d'Economie Financière*, n° 1, pp. 51-63

[103] Pour l'ensemble des exemples, voir notamment le Rapport sur la cybercriminalité, rapport précité, p. 170 et suivantes

démarche est symptomatique du caractère protéiforme des pratiques et révèle en réalité l'absence d'une politique globale de lutte contre la cybercriminalité. En effet, à côté de l'accroissement des démarches éthiques, des partenariats publics-privés, et celui de la norme répressive, c'est le caractère global de la politique de lutte qui fait défaut pour une cyberdélinquance mondialisée. Aussi, ne faut-il pas s'étonner de voir la multiplication d'organismes et d'associations destinés à travailler avec les opérateurs privés dans cette finalité de lutte sans qu'une coordination entre tous ces organismes soit certaine. Par exemple, on cite l'Observatoire de la sécurité des cartes de paiement (OSCP) créé par la loi sur la sécurité quotidienne de 2001. Cet observatoire composé à la fois des pouvoirs publics (Banque de France) et des acteurs économiques, de même que d'experts vise à assurer le suivi des mesures adoptées par les émetteurs et les commerçants et à assurer la sécurité des cartes bancaires. Il procède alors à une veille technologique afin de proposer de nouveaux moyens de lutte contre la fraude informatique à la carte bancaire. Mais, on cite encore PHAROS et Info-escroqueries, plateformes placées sous la direction de l'OCLCTIC qui visent à signaler les activités illégales sur internet, comme les escroqueries, la fraude à la carte bancaire pouvant constituer une escroquerie. En outre, on soulève l'existence de l'association Phishing Initiative créée en 2011 regroupant Microsoft, PayPal et le CERT-Lexsi qui a pour mission de prévenir les tentatives de hameçonnage par lesquelles les escroqueries peuvent être commises. Sans les citer de manière exhaustive, ces trois derniers organismes ont d'ores et déjà un point commun : qu'il s'agisse de la carte bancaire ou d'un autre procédé faisant intervenir un système de traitement automatisé de données, la prévention vise la commission des infractions d'escroquerie dans le cyberespace. Mais, on cite encore l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) créée en juillet 2009 et qui a pour mission d'assurer la partie technique de la sécurité des systèmes d'information. Ne disposant d'aucune capacité juridique en matière de recherche de preuves, elle renvoie cette mission à l'OCLCTIC. On note alors la coexistence d'entités publiques et privées jouant un rôle à la fois de prévention et d'enquête pour la répression de la cyberdélinquance. En réalité, on soulève l'existence de multiples organisations qu'elles soient institutionnalisées ou contractualisées sous forme de partenariat public-privé sans qu'entre toutes ces organisations existe encore une coordination émanant d'une politique globale de lutte contre la cybercriminalité. Néanmoins, ces analyses révèlent que ce développement de partenariats publics-privés est en cours de construction. On peut en effet rapprocher cette construction de celle plus avancée en matière de lutte contre la corruption internationale (partenariats entreprises- Service Central de Prévention de la Corruption) [104].

Force est donc de relever que la lutte contre la cybercriminalité est en cours de construction. Cette construction n'est pas due au défaut ou à l'absence de la norme, mais à son abondance sans qu'une politique globale internationale soit déterminée. Alors que celle-ci est déterminante tant la cybercriminalité recouvre une dimension mondiale, la coopération demeure limitée. Dès lors, si l'outil répressif est dense, son efficacité est tempérée par une coopération interétatique multiforme. La lutte contre la cybercriminalité pourrait alors être orientée vers la mise en cohérence de la norme préexistante, plutôt qu'au développement de celle-ci en associant les autorités publiques et les acteurs privés.

[104] Sénat, Les contrats de partenariat public-privé, Direction de l'initiative parlementaire et des délégations, LC 246, juillet 2013

SUMMARY : THE FIGHT AGAINST CYBER-CRIME: FROM THE ABUNDANCE OF THE STANDARD HAS ITS PERFECTIBILITY

The development of communication networks, the spread of the internet, as well as easy and continuous access to sensitive data within companies, have led to the increase of cybercrime. If the crime is inherent in societies, it is not less a problem regarding its evolution: linked to the economic development of land, sea and air spaces, crime is now also in cyberspace. This is the reason why the fight against cybercrime was the subject of a dense normative development. However, the standard of nature repressive, even very highly developed, covers a certain relativity. While there are a multitude of offences committed in cyberspace, the determination of responsibilities includes the difficulties whether hosting providers, internet access providers, or publishers. Moreover, because this crime covers a global dimension, the localization of the acts, arouses discussions on the application of the territoriality of cybercrime. In light of the specific difficulties to understand this type of crime strongly affecting the economic sector, international cooperation is presented as an effective means to counter it. However, the development of international cooperation is conditioning.

Key words: Automated data processing system; cybercrime; hosting providers; publishers; international cooperation; insecurity