PANTHÉON-ASSAS
UNIVERSITÉ
PARIS

BANQUE DES MÉMOIRES

Master de Droit pénal et sciences criminelles
Dirigé par M. Édouard VERNY et Mme Agathe LEPAGE
2024

L'enquête pénale à l'épreuve de la cybercriminalité

Par Habiba BENTELHI

Sous la direction de M. le Professeur Didier REBUT

Avertissement

L'Université n'entend accorder aucune approbation, ni aucune improbation aux opinions émises dans les mémoires : ces opinions doivent être considérées comme propres à leurs auteurs.

Remerciements

J'adresse mes remerciements les plus sincères à tous ceux qui m'ont facilité la rédaction de ce mémoire :

À mon directeur de mémoire, Monsieur le Professeur Didier Rebut, pour sa bienveillance, sa supervision et ses conseils tout au long de la rédaction ;

À l'experte en informatique près de la Cour d'appel de Paris, Madame Elina Nikooazm, pour ses précieux enseignements sur la recherche et la collecte de preuves numériques ;

À mon directeur de master, Monsieur le Professeur Edouard Verny, pour avoir organisé la rencontre avec l'experte et dispensé une séance d'enseignement sur mon sujet ;

À mon grand frère, Sifedine, sans qui je n'aurais jamais pu prétendre à une telle réussite académique ;

Enfin, je remercie chaleureusement mon père et ma mère pour leur soutien indéfectible et leurs sacrifices, ainsi que mes frères et sœurs bien-aimés pour leur soutien émotionnel et moral.

LISTE DES PRINCIPALES ABRÉVIATIONS

ANSSI : Agence nationale de la sécurité des systèmes d'information

ARRP : Anti-Money Laundering Rapid Response Protocol

C3N : Centre de lutte contre les criminalités numériques

CA : Cour d'appel

CJUE : Cour de justice de l'Union européenne

CEDH : Cour européenne des droits de l'Homme

CNAIP : Centre national d'analyse des images de pédo-pornographie

CNIL : Commission nationale de l'informatique et des libertés

EC3 : European cybercrime center (Centre européen de la lutte contre la cybercriminalité)

FBI : Federal Bureau of Investigation (Bureau fédéral d'investigation)

HADOPI : Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet

IA : Intelligence artificielle

IP : Internet protocol

JLD : Juge des libertés et de la détention

NSA : National Security Agency (Agence nationale de sécurité)

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

OFAC : Office anti-cybercriminalité

SDLC : Sous-direction de lutte contre la cybercriminalité

STAD : Système de traitement automatisé de données

VPN : Virtual Private Network (Réseau privé virtuel)

Sommaire

Introduction

Dans son ouvrage "*Le crime, un phénomène normal"*, le sociologue français Émile Durkheim établissait le juste constat de l'ordinarité du crime auquel n'échappe aucune société. La criminalité y est décrite comme étant une fatalité universelle, présente en tout lieu et en toute époque, dont seule la forme et le taux varient et évoluent. Le crime n'est alors autre que le fruit de la vie en société dont il est le reflet, ou plutôt le symptôme. C'est pour cette raison que l'évolution de la criminalité, notamment de sa nature, est elle-même tributaire de l'évolution de la société, de ses instabilités politiques, économiques et sociales, mais également de façon paradoxale, de ses progrès.

Du latin *progressus*, dérivé de progradi, le terme de progrès est issu de l'association de *pro* qui signifie "en avant", ainsi que de *gradi* c'est-à-dire "s'avancer". Théoriquement, évoquer un progrès c'est donc faire référence à une avancée, et ainsi exposer un état meilleur que le précédent. Cependant, il est indéniable que l'idée d'un progrès uniquement bienfaiteur relève davantage d'un mythe que de la réalité en ce que chaque nouvelle invention est *per se* créatrice de nouveaux risques.

De notre temps, le numérique constitue un bel exemple de cette ambivalence en ce qu'au-delà d'apporter des solutions, les nouvelles technologies créent également de nouvelles problématiques. Ainsi, la digitalisation de la société a eu pour inévitable fatalité d'ouvrir la voie à une nouvelle forme de criminalité, la cybercriminalité, décrite par le spécialiste en sécurité Pierre Berthelet comme « *un phénomène endogène à la civilisation occidentale fondée sur le progrès technique* ». Il convient alors à titre préliminaire d'établir brièvement les contours de cette nouvelle menace (**Chapitre 1**) à l'étendue considérable (**Chapitre 2**).

CHAPITRE 1. TENTATIVE DE DÉFINITION DE LA CYBERCRIMINALITÉ

Alors que la cybercriminalité est un phénomène unanimement constaté, sa définition quant à elle, ne fait l'objet d'aucun consensus, et ce, tant au niveau national qu'international. L'universalité du phénomène n'emportant pas l'universalité de la définition, l'absence de définition dans la première Convention sur la cybercriminalité[1] alors même qu'elle contient un *Chapitre 1 - Terminologie* est très significative. Bien qu'une définition unique du contenu reste impossible, au vu du caractère protéiforme et évolutif de la cybercriminalité, il reste cependant concevable de cerner les éléments communs aux diverses définitions.

§1. L'utilisation d'un espace inédit : le cyberespace

À défaut de soumettre une définition de la cybercriminalité, la Convention de Budapest rappelle dans son préambule la *ratio legis* du traité, à savoir "*mener une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace*". Se faisant, il s'agit de la première reconnaissance juridique de la notion de cyberespace, et bien que le texte s'abstienne encore une fois de livrer une définition, cette précision permet d'enserrer matériellement le champ de ce phénomène. En effet, l'une des innovations majeures qu'apporte la cybercriminalité consiste dans la circonstance de commission d'une infraction en dehors de toute notion de territoire, laquelle est remplacée par le terme de « *cyberespace* », se référant alors à un espace informatique dématérialisé et non délimité à l'origine de nouveaux défis pour les Etats. À ce jour, plusieurs définitions s'affrontent, et en pratique le cyberespace reste largement confondu avec Internet. De même que la cybercriminalité, il fait partie de ces notions qu'il est facile de comprendre, mais qui restent difficiles à définir notamment en raison de leur technicité. L'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) le définit par exemple comme un "*espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques*". Une définition pertinente qui peut néanmoins être retenue est celle du Professeur Frédérick Douzet, selon qui "*le cyberespace, c'est à la fois l'Internet, et l'espace qu'il génère : un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toute nation, à une vitesse instantanée qui abolit toute notion de distance*" [2].

[1] Convention sur la cybercriminalité du 23 novembre 2001, dite Convention de Budapest
[2] La géopolitique pour comprendre le cyberespace , Frédérick Douzet, dans Hérodote 2014/1-2 (n° 152-153)

Or, c'est justement en raison de sa nature même que le cyberespace génère des difficultés pour les États, notamment en ce qu'il s'affranchit et se joue des frontières nationales. À ce titre, contrairement aux eaux territoriales et à l'espace aérien, le cyberespace n'est affecté à aucun régime particulier et échappe majoritairement au contrôle étatique, au point d'avoir pu être qualifié de zone de "non-droit". Par simplicité, et par conformité avec l'objet de l'étude, il sera fait référence au cyberespace comme étant l'espace numérique immatériel dans lequel se développe et s'opère la cybercriminalité.

§2. Le modus operandi : déterminant de la cybercriminalité

Le maître de conférence, Sarah-Marie Cabon, soutenait très justement que "*la cybercriminalité renvoie moins à une liste d'infractions bien déterminées qu'à une manière d'opérer*" [3]. En effet, la cybercriminalité embrasse un large champ infractionnel composé de comportements diversifiés de sorte qu'elle ne peut être restreinte à une liste exhaustive d'infractions. À défaut de pouvoir alors la définir par son contenu, le mode opératoire s'envisage quant à lui comme une bonne clé de définition. Cela apparaît très clairement dans la définition proposée en 2014 par un groupe de travail interministériel, selon lequel "*la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet*."[4]. Ainsi, cette définition opère une dichotomie selon que le numérique est le moyen de l'infraction, ou au contraire, la cible de l'infraction. Stricto sensu, il existe plusieurs modes opératoires qui diffèrent d'une infraction à une autre. À titre d'exemple, le hameçonnage, communément connu sous le nom de *phishing*, consiste à obtenir des données personnelles en usurpant l'identité d'un tiers de confiance en ligne. Le rançongiciel, lui, suppose l'infiltration d'un logiciel malveillant chargé de chiffrer les données d'un système informatique, et auquel l'accès ne sera rétabli qu'une fois le paiement d'une rançon effectué. Les manières d'opérer sont multiples, et continuent de se multiplier, au gré des évolutions technologiques et de l'ingéniosité malveillante des cybercriminels.

---

[3] L'influence du cyberespace sur la criminalité économique et financière, Sarah Marie Cabon, dans Revue de droit pénal n°3 du 1 mars 2018, p12-17.

[4] Rapport sur la cybercriminalité « Protéger les internautes », Groupe de travail interministériel sur la lutte contre la cybercriminalité, Février 2014

Enfin, il faut noter que très souvent les cybercriminels combinent différents modes opératoires entre eux, décuplant considérablement l'ampleur des attaques tout en alourdissant le travail des enquêteurs. Leur étude est alors essentielle dans la lutte contre la cybercriminalité : d'une part, à titre préventif pour pouvoir se prémunir de potentielles attaques, et d'autre part, à titre répressif puisque la constitution de l'infraction suppose l'usage de tel ou tel mode opératoire.

CHAPITRE 2. L'ÉTENDUE DU PHÉNOMÈNE

§1. La cybercriminalité en chiffre

L'ouverture de l'ère du numérique à la fin du XXème siècle couplée à la mondialisation a eu pour dramatique conséquence l'évolution continue de la cybercriminalité, dont l'ampleur se mesure par des chiffres très révélateurs. Par exemple, en 2016, la société Symantec - spécialisée dans les logiciels informatiques - avait indiqué dans son rapport la découverte de près de 430 millions de programmes malveillants et la fuite de plus de 500 millions de données personnelles[5] à l'échelle mondiale. Au terme d'une approche cette fois-ci temporelle, une étude réalisée par l'université de Maryland affirmait qu'une cyberattaque se produisait en moyenne toutes les 39 secondes. Le constat général est celui d'une mondialisation de la menace qui touche tous les pays, et même ceux aux faibles ressources numériques.

S'agissant du cas particulier de la France, la 24ème édition du rapport annuel de Symantec parue en 2019 plaçait le pays au 4ème rang européen des États où la cybercriminalité est la plus active. Il faut noter par ailleurs que la montée en puissance des cyberattaques est elle-même tributaire du contexte sociétal. Ainsi, il avait été recensé une hausse de 400% des cybermenaces depuis le début de la crise sanitaire du Covid 19. Plus généralement, la digitalisation de la société et le recours croissant au numérique conduisent à une augmentation notable du nombre d'attaques au fil des années. En 2022, la magistrate Myriam Quémener soulignait une hausse des saisines cyber de 540% au parquet de Paris, ainsi qu'une augmentation constante des cyber infractions[6].

[5] Symantec, Rapport sur les menaces de sécurité Internet, Volume 21, avril 2016
[6] Actualité en matière de lutte contre la cybercriminalité, Revue Lamy Droit de l'Immatériel, du 1er juin 2022 Myriam QUEMENER

L'année suivante, la Commission nationale informatique et libertés (CNIL) avait enregistré 16 433 plaintes relatives à des cyberattaques, soit 35% de plus par rapport à 2022. Les chiffres sont également assez significatifs s'agissant des modes opératoires privilégiés par les cybercriminels. Selon la plateforme Cybermalveillance.gouv.fr, l'hameçonnage est la première menace informatique en France avec près de 1,9 million de recherches d'assistance et consultations d'articles à ce sujet. En outre, dans le rapport de l'ANSSI de 2023, l'agence avait révélé que le nombre de rançongiciels dont elle avait eu à connaître avait augmenté de 30%, en comparaison avec la valeur de l'année précédente. Ces chiffres marquants renseignent sur la nécessité pour les États d'agir rapidement afin d'endiguer ce danger grandissant aux conséquences dramatiques.

§2. Les victimes de la cybercriminalité

L'étendue du phénomène se mesure également au regard des divers profils de victimes des cyberattaques. Que ce soit des personnes physiques, des personnes morales ou même des États : nul n'y échappe. S'agissant des personnes morales, les cyberattaques les plus médiatisées et certainement parmi les plus dramatiques sont celles ciblant fréquemment les hôpitaux. Agissant à coups de rançongiciels, les cybercriminels vont procéder au chiffrement des données de l'établissement de soin - indispensables à son fonctionnement - afin d'exiger en retour une somme d'argent colossal. C'est ainsi que le deuxième mois de l'année 2024 s'est malheureusement ouvert sur une énième attaque de données ciblant l'hôpital d'Armentières, qui avait alors dû fermer temporairement son service d'urgence.

Les entreprises quant à elles, représentent des victimes de premier plan pour les cybercriminels, notamment en raison de la perspective de gain associée. Selon le rapport CESIN[7] de 2023, "49% des entreprises ont constaté au moins une cyberattaque réussie en 2023 contre leurs infrastructures". Plus alarmant encore, le baromètre de la cybersécurité en entreprise CESIN 2022 avait révélé que 54% des entreprises françaises avaient été attaquées en 2021. Il est à noter que cette année est très évocatrice puisqu'elle correspond à la période de la pandémie du coronavirus durant laquelle le recours accru au télétravail avait malencontreusement ouvert une brèche de sécurité aux cybercriminels.

[7] CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)

Alors qu'initialement les cyberattaques ne ciblaient principalement que les grandes entreprises au chiffre d'affaires attrayant, on assiste aujourd'hui à un renversement de la perspective. En effet, dans son rapport annuel de 2022, l'ANSSI avait établi que les petites entreprises étaient désormais devenues les cibles privilégiées des cybercriminels, et pour cause, leur fragilité financière ou encore leur manque de conscience quant aux risques cyber conduisant très souvent à l'absence de mesures de cybersécurité au sein de la structure.

Ainsi, il apparaît que la vulnérabilité de la proie est un élément déterminant pour le cybercriminel, et ce constat s'observe en particulier s'agissant des victimes personnes physiques. En effet, si la valeur marchande d'une entreprise est attrayante, les données personnelles d'un particulier le sont d'autant plus. Le vol de données personnelles ou bancaires, le phishing[8], les piratages ou encore le rançongiciel[9] représentent autant de menaces pour les particuliers qui sont quotidiennement victimes de ces cyberattaques, ou du moins de leur tentative. Très souvent, les cybercriminels profitent de la vulnérabilité des potentielles victimes, de leur manque de connaissances en informatique, ainsi que de leur crédulité pour opérer. C'est notamment pour ces raisons précises que les personnes âgées constituent une proie attrayante pour ces prédateurs de données. Selon Microsoft, parmi les 175 000 plaintes reçues en 2015 au sujet d'escroqueries au support technique[10], une grande majorité de ces plaintes émanaient de seniors. De même, en février 2019, les personnes âgées représentaient un nombre conséquent sur les 8000 victimes françaises de cette technique d'escroquerie[11].

Les particuliers peuvent être victimes de cyberattaques de deux manières : soit ils en sont directement la cible, soit l'attaque concerne un établissement qui détient leurs données. C'est ainsi que le mois de janvier 2024 s'est soldé sur la plus grande faille de sécurité en France, ayant touché 33 millions de français par le vol massif de données à des gestionnaires du tiers payant. En outre, les cybercriminels font régulièrement usage de l'identité de ces établissements, reconnus pour être des tiers de confiance, afin de soutirer des données ou de l'argent à des particuliers.

[8] *Phishing* ou hameçonnage est une technique d'escroquerie sur internet qui consiste à inciter le destinataire à communiquer des données personnelles ou bancaires en prenant l'apparence d'un tiers de confiance

[9] Rançongiciel : cyberattaque qui consiste pour le cybercriminel à bloquer l'accès à des données personnelles par le biais d'un logiciel malveillant, et demander une rançon en échange de l'accès.

[10] Escroquerie au support technique : arnaque qui consiste à faire croire à l'existence de problèmes techniques qui sont en réalité fictifs, avant de proposer une assistance technique payante en affichant l'apparence d'un service officiel tel que Microsoft.

[11] "Les seniors, cible privilégiée des cybercriminels", Chronique de Franck Trognée, juillet 2020.

L'année 2023 avait notamment connu une montée exponentielle du nombre de phishing par l'envoi de messages téléphoniques trompeurs usurpant la qualité de service de livraison, d'administration de justice ou encore d'un centre de formation. Sur ce point, il est à noter que le cyberespace a permis une multiplication spectaculaire des potentielles victimes. En effet, en piratant les données personnelles d'une messagerie électronique par exemple, le cybercriminel aura accès à une liste de contact dans laquelle il pourra librement piocher ses prochaines victimes. De plus, le numérique présente l'ultime avantage de pouvoir cibler un nombre considérable de victimes, et ce en un seul clic.

Enfin, les États subissent également la malveillance des cybercriminels, qui tantôt s'en prennent aux organes étatiques pour extirper des données financières, administratives ou personnelles, et tantôt affaiblissent les États dans leur souveraineté en se jouant des territoires nationaux. À ce titre, l'ANSSI[12] a dressé une typologie des différentes attaques qui comprend les attaques à but lucratif, les attaques à des fins de déstabilisation politique -dit *hacktivisme*- et enfin les attaques à but d'espionnage réalisées majoritairement en faveur d'autres États. Il est à noter que les collectivités territoriales se trouvent parmi les organes étatiques particulièrement visés par les cybercriminels, notamment en raison du statut d'intermédiaire qu'elles occupent entre les administrés et l'État. Entre janvier 2022 et juin 2023, l'ANSSI avait recensé et traité un total de 187 cyberattaques ciblant des collectivités territoriales. Au-delà des multiples cyberattaques des centres hospitaliers, qui sont les plus fréquentes, les cybercriminels visent également d'autres organismes publics. Ainsi, en 2022, un pirate avait commercialisé sur Internet près d'un million d'identifiants de connexion au site de l'Assurance maladie *Ameli.fr*. La même année, en septembre 2022, plus de 420 000 personnes avaient été victime d'un hameçonnage par la diffusion de messages frauduleux usurpation d'identité de l'Assurance maladie. En somme, il apparaît que les victimes de la cybercriminalité ont des profils aussi diversifiés que ceux de leurs auteurs, dont les mobiles diffèrent d'une attaque à une autre.

[12] ANSSI : Agence Nationale de Sécurité des Systèmes d'Information

§3. Le coût de la cybercriminalité

Après avoir établi un rapide panorama relatant le nombre de cyberattaques, ainsi que la diversité et la multitude de leurs victimes, il convient de s'intéresser au dernier élément de mesure, à savoir le coût de la cybercriminalité

a. Le coût matériel

Au-delà du nombre effréné de cyberattaques réussies et tentées chaque année, le constat est encore plus surprenant lorsqu'il s'agit d'en étudier le coût. Il est à noter avant tout que la diversité des approches, des critères et des méthodes d'étude s'observe dans les différences de résultats affichés d'un rapport à l'autre. À y ajouter le prix inconnu des attaques invisibles menées avec discrétion, ainsi que l'évaluation parcellaire par les victimes du coût global d'une cyberattaque, chiffrer ce coût ne paraît alors possible qu'au terme d'une estimation. Pour autant, tous concluent à l'ampleur démesurée de ces attaques.

Selon le graphique d'estimation établi par Statista Technology Market Insight, le coût annuel de la cybercriminalité en France aurait atteint 93,5 milliards de dollars américains en 2023 et devrait atteindre 129 milliards de dollars en 2024. Si ces nombres sont alarmants, le constat est d'autant plus préoccupant quand il s'agit d'étudier ce coût à l'échelle mondiale. En effet, selon le congrès d'expert Rome Cybertech 2022, le coût mondial de la cybercriminalité aurait atteint en 2021 plus de 6 000 milliards de dollars américains.

À ce coût direct, déjà considérable, s'ajoute un coût caché qui n'est généralement pas pris en compte lors des calculs. En effet, selon l'entreprise Deloitte France, "*le calcul des coûts d'une attaque se limite habituellement à la partie émergée de l'iceberg*.", c'est-à-dire aux pertes directement visibles après une attaque. Qu'en est-il donc de la partie immergée de l'iceberg ? Selon le cabinet d'audit, en plus des coûts à moyen terme, la cybercriminalité affecte également l'entreprise dans la durée en lui faisant notamment supporter le coût de la perturbation ou de l'interruption de l'activité, la perte de contrats clients ou encore la dépréciation de la valeur de la marque. De la même manière, ce raisonnement est transposable pour les attaques à l'égard des particuliers ou encore des administrations étatiques, qui souffrent également sur le long terme des conséquences dramatiques d'une attaque.

b. Le coût moral

Bien que moins intuitif et peu mentionné, la cybercriminalité représente également un coût moral pour les victimes à la fois physiques et morales. Les données personnelles étant une proie attrayante pour les cybercriminels, leur vol a inévitablement pour conséquence de susciter du stress voire de l'anxiété chez les victimes personnes physiques. À ce propos, dans un arrêt du 14 décembre 2023[13], la Cour de justice de l'Union Européenne avait admis que la crainte d'un potentiel usage abusif de données personnelles pouvait constituer un préjudice moral à elle seule. S'ajoute généralement à cette crainte un sentiment d'insécurité ainsi qu'une détresse psychologique résultant de la perte d'argent dont la somme est souvent considérable.

S'agissant des entreprises, bien qu'elles ne puissent pas subir de préjudice émotionnel[14], les cyberattaques non déjouées peuvent également avoir pour conséquence de porter atteinte à leurs intérêts extra-patrimoniaux et ainsi causer un préjudice moral. Ainsi, dans une décision du 30 juin 2021 concernant une attaque par rançongiciel, la Cour d'appel de Versailles avait rappelé qu'une personne morale pouvait réclamer l'indemnisation d'un préjudice moral si elle parvenait à démontrer "*la dégradation concrète de sa réputation ou de son image auprès de ses clients*".

[13] CJUE, 14 déc. 2023, aff. C-340/21

[14] CA de Versailles, 30 juin 2021 : rappelle selon une jurisprudence constante que « *seules les personnes physiques peuvent se prévaloir d'un préjudice de stress, d'anxiété, de déception ou d'affection* »

ANNONCE DU PLAN

L'ampleur considérable de cette forme de criminalité inédite, complexe et universelle, a fait émerger la nécessité pour les États d'intervenir pour tenter d'endiguer le phénomène. Diversité des procédés, diversité des auteurs ou encore diversité des mobiles, la cybercriminalité constitue un nouveau défi pour les sociétés du XXIème siècle mises face aux dérives des innovations technologiques qu'elles ne cessent de louer. Désormais, un simple clic à distance permet de perturber l'ordre public d'un État, en emportant des conséquences humaines et financières désastreuses. Alors que le constat de cette nouvelle menace relève aujourd'hui d'une affirmation péremptoire des États qui s'accordent majoritairement sur la nécessité d'intervenir conjointement, la manière d'opérer face à ce phénomène demeure néanmoins une source de divergence.

De plus, malgré cette prise de conscience collective, les moyens traditionnels de lutte contre la criminalité - tant légaux qu'opérationnels - ont laissé rapidement apparaître leurs limites dans le traitement de ce nouveau phénomène. À ce propos, l'ancien directeur adjoint d'Interpol, Michel Quille, reconnaissait en 2012 que "*nous combattons un crime du futur avec des outils du passé*". Tandis que le droit pénal de fond a su relativement s'adapter à cette criminalité, en ce qu'elle se calque majoritairement sur des comportements traditionnellement incriminés, le droit pénal de forme a quant à lui été exposé à de nouvelles difficultés propres au numérique et au caractère transfrontalier de la cybercriminalité.

En quoi la cybercriminalité, reconnue comme la nouvelle forme de criminalité du XXIème siècle, a-t-elle bouleversé les schémas traditionnels de l'enquête pénale créant ainsi pour les États la nécessité de revisiter leur arsenal de lutte ?

Il convient de voir que le caractère inédit de cette nouvelle criminalité est à l'origine de l'impuissance des États (**Partie I**), avant de voir que s'amorce positivement les prémices d'une lutte d'avantage effective (**Partie II**).

PARTIE 1. LA CYBERCRIMINALITÉ : NOUVEAU DÉFI DE L'ENQUÊTE PÉNALE

Titre 1. Une criminalité d'exception

Section 1. Une criminalité protéiforme

L'une des spécificités de la cybercriminalité tient du fait qu'elle entraîne d'une part, un renouvellement de la criminalité classique, et d'autre part, l'émergence de nouvelles infractions spécifiques. S'opère alors une summa divisio entre les infractions classiques commises au moyen d'une technologie informatique, et les infractions de cybercriminalité -stricto sensu- qui impliquent, par essence, une commission sur ou au moyen d'un système informatique.

§1. L'extension de la criminalité classique vers l'univers du numérique

De manière regrettable, l'avènement du numérique a participé à la complexification des infractions classiques par l'élargissement de leur champ d'application initial et l'enrichissement des moyens de commission. En outre, la dématérialisation des infractions traditionnelles les a rendu d'autant plus faciles à commettre, mais simultanément d'autant plus difficile à déceler.

A. Le numérique : moyen de l'infraction classique

Force est de constater qu'un grand nombre d'infractions classiques ont reçu le préfixe "*cyber*"[15] dans leur appellation : de la "cyberviolence", à la "cyberescroquerie", ou encore au "cyber harcèlement", la liste ne cesse de s'accroître. Non explicitement nommés par le législateur, ces comportements vont tout de même être sanctionnés par le jeu de l'interprétation dynamique du juge. Qu'il s'agisse d'infractions contre les personnes, contre les biens ou contre l'État, rares sont celles qui parviennent à se soustraire à cette contamination du numérique. À défaut de parvenir au listage exhaustif de ces dernières, certaines méritent un rapide développement à raison de leur importance et de leur fréquence.

[15] Selon une définition donnée par Les Assises De La Cybersécurité, le terme cyber est un "*Préfixe généralement utilisé pour signifier une dimension informatique et réseau à la notion qu'il accompagne*"

a. Les atteintes contre les personnes

Cette catégorie regroupe principalement les infractions dites de "contenu", comprenant la pédopornographie ou encore l'incitation à la haine, et plus généralement les infractions sexuelles commises sur Internet. L'un des facteurs déterminant de ce transfert vers le numérique est celui du mouvement d'anonymisation des échanges, d'autant plus facilité par l'illustre *dark web*[16], qui permet la dissimulation de l'identité de ses utilisateurs. Par essence, l'anonymisation est particulièrement criminogène en ce qu'elle procure un sentiment d'impunité chez les utilisateurs, motivant donc le passage à l'acte. Il apparaît donc que le numérique facilite la commission de l'infraction, constitue le moyen de sa commission, et en est le lieu de commission.

S'agissant de la facilitation du crime -lato sensu- , le législateur l'a érigé en circonstance aggravante au sein de nombreuses incriminations. Ainsi, le proxénétisme est aggravé lorsqu'il a été commis "*grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique*" (article 225-7 alinéa 10 du Code pénal). De même, la répression est aggravée "*lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique*". Tel est le cas pour le viol (article 222-24 alinéa 8 du Code pénal) , ou encore la prostitution de mineurs (article 225-12-2 alinéa 2 du Code pénal).

Lorsque le numérique est le moyen de l'infraction, cela suppose qu'y recourir constitue une condition pour la constitution de l'infraction autonome. Ainsi, en matière de *grooming*[17], l'article 227-22-1 du Code pénal réprime "*le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique*". Dans le même courant, l'article 227-22-2 du Code pénal sanctionne "l*e fait pour un majeur d'inciter un mineur, par un moyen de communication électronique, à commettre tout acte de nature sexuelle, soit sur lui-même, soit sur ou avec un tiers, y compris si cette incitation n'est pas suivie d'effet*".

[16] Dark web : navigateur caché accessible par des configurations spécifiques et techniques, et qui permets d'échapper à la surveillance étatique

[17] *Grooming* : pratique qui consiste, pour un prédateur, à se faire passer pour un enfant afin d'obtenir des faveurs sexuelles voire rencontrer le mineur avec qui il est en contact.

Enfin, une dernière catégorie d'incriminations sanctionne l'usage d'Internet en tant que support de l'infraction. L'infraction phare en la matière est celle de la diffusion à un public indéterminé, de l'image ou de la représentation à caractère pornographique d'un mineur par le biais d'un réseau de communication électronique (article 227-23 alinéa 3 du Code pénal). Ici, Internet est le support de l'infraction, à savoir la fixation d'une image ou la représentation pédopornographique d'un mineur.

b. Les atteintes contre les biens

Comme le souligne à juste titre le maître de conférence Sarah-Marie Cabon, "*la criminalité en col blanc*[18] *n'est aujourd'hui plus l'affaire unique d'une classe supérieure, mais d'une communauté d'individus qui partage la maîtrise et les codes du monde virtuel*"[19]. Il est notable que les infractions contre les biens sont quantitativement celles qui se développent le plus au sein de l'espace numérique en ce qu'elles sont motivées par l'appât du gain. En plus de l'avantage précité tiré de l'anonymat, le cybercriminel va également pouvoir mener des actions à grande ampleur, rendues possibles notamment par l'accroissement des transactions à distance. En cette matière, le droit pénal de fond a su particulièrement bien s'adapter. De ce fait, les atteintes aux biens commises par la voie électronique ne font pas l'objet d'incriminations autonomes au sein du Code pénal, mais sont réprimées sous la qualification des incriminations classiques, telles que l'escroquerie ou encore l'extorsion.

L'infraction la plus répandue, et sans doute la plus lucrative, est celle de l'escroquerie par Internet par laquelle le cybercriminel va déterminer une remise généralement en faisant usage d'une fausse qualité ou d'un faux nom. Ce dernier va par exemple reproduire un site internet légitime, tel que celui d'une banque, pour pouvoir récupérer les données inscrites par les victimes crédules ayant préalablement cliqué sur le lien contenu dans des courriels envoyés massivement.

---

[18] Expression introduite par le sociologue Edwin Sutherland pour décrire la criminalité d'affaire "commise par une personne respectable et de haut rang social dans le cadre de sa fonction"

[19] L'influence du cyberespace sur la criminalité économique et financière Revue DP n°3 du 1 mars 2018, p12-17.

Un second type d'escroquerie commise fréquemment sur Internet est qualifiée d'escroquerie sentimentale en ce qu'elle consiste pour l'auteur de l'infraction à feindre des sentiments amoureux ou amicaux pour pouvoir soutirer de l'argent à la victime en usant notamment d'une fausse identité. Une autre forme d'escroquerie qui se développe essentiellement ces dernières années est celle du *carding*, qui désigne le trafic et l'usage illégal des données bancaires de la victime, facilité par le mouvement de numérisation des transactions. Dans la majorité des cas, les informations bancaires vont être recueillies frauduleusement par *phishing*, ou par l'exploitation de failles de sécurité sur des sites légitimes avant d'être utilisées soit sur des sites internet n'exigeant pas de validation d'achat du propriétaire de la carte, soit pour acquérir des cartes cadeaux prépayées et ainsi, éviter la traçabilité des actions.

S'agissant de l'extorsion en ligne, celle-ci va prendre la forme d'un cyber chantage par lequel le criminel va faire croire à la victime à un prétendu piratage de ses appareils électroniques ou de ses conversations avant de la menacer de divulguer ses informations sensibles et privées si elle ne paie pas une certaine somme. Ce piratage, peut à l'inverse, être réel et dans ce cas le hacker va prendre possession de données sensibles, et demander de l'argent à la victime afin de mettre fin à l'attaque et rétablir son accès.

Enfin, la cybercriminalité affecte particulièrement la propriété intellectuelle par les atteintes aux droits d'auteur qu'elle occasionne, privant ainsi les propriétaires des gains de leur création. En effet, par le piratage des œuvres, l'accès et l'enregistrement du contenu protégé deviennent gratuit, et ce, sans l'autorisation du propriétaire. Que ce soit des livres, des films ou encore de la musique, toutes les œuvres sont exposées au piratage en ligne. C'est pourquoi, face à la montée en puissance de cette pratique, a été promulguée une loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, instituant une "Haute autorité pour la diffusion des œuvres et la protection des droits sur l'Internet" (HADOPI), chargée de la prévention et de la sanction de ce type de piratage. En outre, il peut être noté que souvent des sites prétendent donner l'accès à un tel contenu illégal gratuit pour pouvoir ensuite mener des cyberattaques sur le système informatique des utilisateurs qui auront tenté d'y accéder en cliquant sur de multiples liens. Les stratagèmes des cybercriminels sont multiples, et toujours d'autant plus ingénieux, engendrant ainsi une menace omniprésente.

c. Les atteintes contre l'État

Comme en témoignent les événements récents qui se sont produits en Ukraine en 2022, les cyberattaques peuvent servir d'artillerie afin d'instaurer une politique de la terreur. En effet, les Russes avaient piraté le satellite KA-SAT afin de couper les moyens de communication de l'Ukraine, et ainsi, paralyser son action militaire. Plus de 70 sites gouvernementaux avaient par ailleurs été attaqués, en remplaçant leur contenu par des textes tels que "*ayez peur et attendez le pire*". De même, en France, une quinzaine d'espaces numériques de travail (ENT) avaient été piratés en mars 2024, afin d'afficher un message menaçant plus de 120 établissements scolaires d'une attaque terroriste. Ces attaques, loin d'être des cas isolés, ne cessent de se multiplier ces dernières décennies sous l'effet de l'appropriation du numérique et de l'Internet par des groupes radicalisés.

Dès le milieu des années 80, un chercheur à l'Institut de Sécurité et de Renseignement de Californie, Barry C. Collin, avait alors élaboré la notion de "*cyberterrorisme*" pour désigner "*la convergence de la cybernétique et du terrorisme*". Selon une définition donnée par le dictionnaire Larousse, le cyberterrorisme se réfère à "*l'ensemble des attaques graves et à grande échelle des ordinateurs, des réseaux et des systèmes informatiques d'une entreprise, d'une institution, d'un État, commis dans le but d'entraîner une désorganisation générale susceptible de créer la panique*". Alors que les activités illégales précitées reposent sur une déviance personnelle ou sur un objectif financier, le cyber terrorisme est quant à lui inspiré par des motivations politiques et idéologiques. Par ailleurs, les plans d'actions sont multiples puisque Internet permet à la fois aux groupes terroristes de recruter de nouveaux membres, de récolter des fonds pour financer l'action physique et armée, ou encore de promouvoir leur idéologie. S'affiche alors une réelle volonté de désorganiser et de déstabiliser l'État visé, en ciblant notamment les infrastructures essentielles tel que le réseau électrique, ou encore en s'attaquant aux services de la défense.

B. Le numérique : outil de l'infraction classique

Cette dernière catégorie concerne les infractions hybrides, qui combinent à la fois une délinquance physique classique et une délinquance immatérielle par l'usage de l'informatique. Dans ce cas de figure, le délinquant physique se trouve tantôt sur le territoire national, tantôt à l'étranger. Soit la délinquance physique et immatérielle se commettent conjointement par la même personne, soit plusieurs personnes interviennent dans le processus, les uns étant chargés d'accomplir physiquement un acte et les autres opérant à distance depuis un support informatique.

Il existe en effet une pratique courante dite "*jackpotting*" - appelée également "*black boxing*"- qui consiste à pirater des distributeurs automatiques de billets (DAB) afin d'extirper l'argent qu'ils contiennent. Cette méthode requiert la présence d'un délinquant "physique" chargé d'ouvrir le distributeur pour y connecter un dispositif numérique, qui va à son tour permettre à un hacker -le commanditaire- agissant depuis l'étranger, de prendre le contrôle du logiciel et provoquer ainsi la distribution de billets. En décembre 2018, le service d'analyse criminelle de la police judiciaire soutenait que les auteurs étaient des techniciens « *d'un haut niveau d'organisation et d'un professionnalisme avéré* », qui ne cessent de s'adapter aux mesures de sécurité mises en place par les établissements bancaires.

Un second exemple est celui du viol à distance - ou viol en ligne- , qui consiste à diffuser en direct un acte de viol, généralement commis sur un mineur, en échange d'une rémunération payée par un commanditaire. Une difficulté pratique tient au fait que dans la majorité des cas, ces violences sexuelles ne sont pas commises en France, mais à l'étranger et par des étrangers. Se pose alors un obstacle aux poursuites puisque, selon le droit français, le complice français d'une atteinte aux personnes réalisée à l'étranger ne peut être poursuivi de ce chef que si le crime a été constaté par une décision définitive de la juridiction étrangère. À ce titre, l'ancienne garde des Sceaux Nicole Belloubet a permis une satisfaisante évolution législative par la modification de l'article 222-26-1 du Code pénal[20], permettant désormais la poursuite des donneurs d'ordres français, y compris lorsque le viol est commis hors du territoire français par un étranger.

[20] "*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 viol, y compris hors du territoire national, est puni, lorsque ce crime n'a été ni commis, ni tenté, de dix ans d'emprisonnement et de 150 000 € d'amende.*"

§2. L'émergence de nouvelles infractions spécifiques

Au-delà de cette dématérialisation des infractions classiques, la cybercriminalité fait également référence à des incriminations inédites réprimant l'activité technique en tant que telle, selon que le système informatique constitue le moyen de commission de l'infraction, ou selon qu'il en est la cible. Dès lors, ce n'est pas la finalité lointaine qui est sanctionnée - telle que commettre une escroquerie-, mais le procédé même du cybercriminel.

En 1984, l'hebdomadaire *Le Canard enchaîné* publiait un article révélant par quel moyen des journalistes, sans connaissance technique ni aucun matériel, avaient pu avoir accès à des bases de données confidentielles à partir d'un minitel[21]. Au cours de la même décennie, les prémices de la cybercriminalité voyaient jour aux États-Unis avec les premières intrusions dans des réseaux protégés, opérées par de jeunes "*black hat*"[22]. Progressivement, la cybercriminalité s'est tournée en véritable chasse aux données confidentielles, notamment à des fins de ventes ou d'usurpation d'identité, avant de connaître l'extension considérable de ses mobiles comme précédemment cités. Aujourd'hui, la donnée est la grande cible des cybercriminels, et donc de façon causale la grande protégée des États[23], comme en témoignent les différentes interventions législatives de ces dernières années.

À jour de cette nouvelle menace, le législateur français est rapidement intervenu par la loi Godfrain du 5 janvier 1988 relative à la fraude informatique, réprimant pour la première fois la criminalité informatique, et notamment le piratage. Cette loi n'a été que quelque peu modifiée depuis son introduction en raison de sa capacité d'adaptation, permise par la volontaire rédaction des infractions en des termes généraux. A alors été institué un nouveau Chapitre III au sein du titre II du Livre III intitulé "*De certaines infractions en matière informatique*", composé de huit articles. Au cœur de cette loi, se trouve la notion de système de traitement automatisé de données (STAD), non défini par le texte, et figurant désormais comme objet du chapitre III renommé "*Des atteintes aux systèmes de traitement automatisé de données*".

---

[21] Minitel : terminal informatique -reconnu comme l'ancêtre de l'Internet- permettant d'accéder à des services en ligne tels que l'annuaire téléphonique ou des sites de rencontres.

[22] *Black hat* (en français "chapeau noir") fait référence à un pirate informatique mal intentionné par opposition aux "*white hat*", qui sont des hackers éthiques qui utilisent leurs compétences techniques afin de détecter les vulnérabilité d'un réseau informatique, et avertir sur ses failles.

[23] En France, la réglementation des traitements de données personnelles est régie par la loi Informatique et libertés du 6 janvier 1978

Cette notion mère, déjà introduite en droit français par la loi informatique et liberté du 6 janvier 1978, et reprise par la loi Godfrain, n'a jusqu'à présent jamais été définie. Il peut être supposé que cette absence de définition fut volontaire, afin de ne pas restreindre la portée des textes eu égard au caractère évolutif des technologies. En effet, alors que le Sénat avait proposé une définition des STAD lors de l'élaboration du nouveau Code pénal, le choix final a été de laisser à la jurisprudence la liberté de déterminer au cas par cas, ce qui constituait ou non un tel système. Il semblerait alors que les STAD soient conçus comme un tout hétérogène, qui ne peut faire l'objet d'une liste exhaustive, regroupant à la fois des éléments matériels tel qu'un disque dur[24], et des programmes immatériels tel qu'un logiciel. Très souvent, les juges du fond reprennent la définition issue des travaux parlementaires sur la loi Godfrain qui qualifie de STAD "*tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organe d'entrées-sorties et de liaisons qui concourent à un résultat déterminé*"[25].

S'agissant du contenu des incriminations, une summa divisio peut être opérée selon que l'incrimination protège l'intégrité du système ou l'intégrité des données qu'il contient. Les premières sanctionnent l'accès ou le maintien frauduleux dans un STAD, ainsi que le fait d'entraver ou de fausser son fonctionnement[26], tandis que les secondes sanctionnent l'introduction de données ou la manipulation des données qu'il contient[27]. Ainsi, il apparaît à la lecture de ces incriminations qu'elles suivent un ordre chronologique de commission, en ce qu'elles sanctionnent l'intrusion puis le maintien dans le STAD, l'atteinte à son fonctionnement et enfin l'atteinte à l'intégrité des données. Cependant, comme le souligne le Professeur Romain Ollard, " *à vouloir trop embrasser, en resserrant à l'excès le maillage répressif, le risque est de mal étreindre puisque, ce faisant, la loi pénale a créé de nombreuses situations de concours – de qualifications ou d'infractions –, parfois extrêmement délicates à résoudre.*".

[24] Cour d'appel de Douai, 7 oct. 1992
[25] Cour d'appel de Douai, 11 mai 2023, RG n° 15/06278
[26] Articles 323-1 et 323-2 du Code pénal
[27] Article 323-3 du Code Pénal "*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*"

Enfin, l'article 323-3-1 du Code pénal sanctionne "*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.*". L'objectif de cette disposition est donc de sanctionner le trafic de moyens informatiques cybercriminels, destinés à commettre les infractions précitées. Il s'agit donc d'une infraction obstacle, dont la portée préventive est affichée, puisque sont réprimés des actes précédents toute intrusion et entrave, et sans condition de résultat. Il est à noter que cette infraction a été inspirée de l'article 6 de la Convention de Budapest, qui au même titre que l'article 323-3-1, exclut la responsabilité dès lors que l'intention malveillante fait défaut, notamment afin de protéger les professionnels de la sécurité informatique[28].

En somme, ce qui est sanctionné par ces dispositions, c'est l'utilisation mal intentionnée des technologies numériques, ce qui témoigne de la prise en compte par le législateur de ce nouveau phénomène criminel.

Section 2. Une criminalité sans frontière

Non seulement la cybercriminalité trace ses propres frontières, mais au surplus, elle se désolidarise de toute frontière territoriale, complexifiant ainsi à la fois la conduite des enquêtes et des poursuites. La souveraineté territoriale est alors défiée et concurrencée par la souveraineté numérique, dès lors qu'au sein de nos sociétés contemporaines la puissance s'exerce désormais de manière dématérialisée, ouvrant la porte à une nouvelle forme de gouvernance. L'étymologie du préfixe *cyber*, issu du grec *Kubernêtikê* signifiant gouvernail, prend alors tout son sens.

[28] Notamment les whites hat

§1. L'atteinte à la souveraineté nationale

La cybercriminalité, en ce qu'elle défie la notion de territoire, entretient de façon causale une conflictualité avec le principe de souveraineté. En effet, la notion de souveraineté fait référence à l'exercice d'un pouvoir absolu sur une zone géographique donnée et sur la population qui s'y trouve, sans qu'aucun élément extérieur ne puisse interférer dans cette prérogative. Or, cette souveraineté est nécessairement mise à mal par la cybercriminalité, qui s'introduit sans limite dans tous les territoires, tout en portant atteinte aux intérêts des États et de leur population**.** En outre, le numérique constitue une véritable arme politique dont l'usage n'échappe pas aux dirigeants dans des contextes de tensions interétatiques.

A. L'affaiblissement de la souveraineté territoriale

L'atteinte à la souveraineté résulte en premier lieu de l'irrespect des frontières établies par les souverainetés étatiques. Internet, et plus généralement le numérique, échappent majoritairement au contrôle des États et permettent alors une ingérence sur leur territoire, et ce, sans présence physique du criminel. Le Maître de conférence Pauline Türk, fait ainsi référence à une "*fenêtre d'entrée sur le territoire étatique de données et d'informations de toute provenance, sur lesquelles un contrôle des autorités publiques serait aussi mal jugé qu'il est techniquement difficile. Internet permet à des intervenants extérieurs, aux statuts divers, de s'immiscer dans les affaires d'un État*"[29]. Par le jeu de ces frontières inexistantes, le cyber délinquant va également profiter d'une dislocation de l'infraction sur plusieurs États différents afin de brouiller les pistes et former ainsi des obstacles à la poursuite. Or, la localisation de l'infraction représente un enjeu majeur de la procédure pénale puisqu'elle emporte de nombreuses conséquences, notamment en termes de compétence juridictionnelle. Se dessine alors un schéma où les cybercriminels ainsi que leurs victimes se situent sur des territoires différents, avec une rupture de la concordance entre la présence du malfaiteur, de la victime et du lieu de commission de l'infraction. Les éléments constitutifs de l'infraction vont également être préalablement répartis entre différents États, grâce à l'immatérialité des flux numériques, constituant une énième difficulté à la poursuite.

[29] La souveraineté des États à l'épreuve d'internet, Pauline Türk, Revue du droit public - n°6 - page 1489

La cybercriminalité s'affranchissant de toute notion de territoire, l'application du critère de territorialité[30] dans la détermination des juridictions compétentes apparait alors inadaptée. Comme le souligne le Professeur Brigitte Pereira, "*même étendue, l'applicabilité du principe de territorialité souffre de certaines limites face à l'universalité d'Internet*". Elle ajoute que "*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*"[31]. De façon constante aujourd'hui, les États étendent leur compétence aux infractions réputées commises sur leur territoire dès lors qu'un des faits constitutifs a eu lieu sur le territoire. En ce sens, le législateur français conscient des possibilités qu'offre le numérique, a alors institué un article 113-2-1 au sein du code pénal qui dispose que "*tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République.*" Or, dès lors que par essence, plusieurs territoires sont impliqués, le risque est celui d'un conflit de compétences entre plusieurs juridictions nationales, aboutissant ainsi à un chevauchement des poursuites que la Convention de Budapest souhaitait pourtant éviter.

Cette difficulté procédurale, inhérente à la cybercriminalité, s'observe particulièrement à la lecture de la jurisprudence française, fluctuante et réservée, s'agissant du critère du *locus delicti*[32] pour déterminer la loi applicable. En effet, se pose la question de savoir s'il faut préférer le critère du lieu de l'émission de la menace numérique, ou celui de sa réception ? En outre, s'agissant des infractions de contenu, les juges du fond avaient à déterminer si le critère de l'accessibilité au contenu criminel était, en soi, suffisant pour établir la compétence des juridictions françaises. Il est certain que retenir un tel critère aurait eu pour malheureuse conséquence d'admettre la compétence de tous les États à partir desquels le contenu était accessible, ce qui explique pourquoi il était très largement discuté.

[30] Article 113-2 du code pénal "*La loi pénale française est applicable aux infractions commises sur le territoire de la République. 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.*"

[31] La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité, Brigitte Pereira dans Revue internationale de droit économique 2016/3 (t. XXX), pages 387 à 409

[32] Terme latin pour "lieu du délit"

Auparavant, le critère retenu dépendait de l'infraction en cause, en retenant le critère d'accessibilité pour les infractions de contenu[33], et le critère de la réception pour les infractions de nature économique. Aujourd'hui, et fort heureusement, la seule accessibilité au contenu ne suffit plus. En effet, les solutions semblent converger vers un seul critère plus restreint qui est celui de la focalisation[34], c'est-à-dire de l'orientation volontaire vers le public français. Désormais, "*la diffusion par le réseau internet depuis un territoire étranger de propos accessibles depuis la France ne caractérise pas à elle seule un acte de publicité sur le territoire de la République rendant le juge français compétent pour connaître de ce délit*". Les juges vont alors prendre en considération un certain nombre d'indices pour étendre leur compétence à raison de la focalisation du public français. Ainsi, s'agissant d'apologie publique d'acte de terrorisme, la chambre criminelle avait jugé que les propos étaient suffisamment rattachés au territoire français dès lors qu'ils "*ont été diffusés en langue française, certains accompagnés de photographies représentant la France, stigmatisée comme un pays de mécréance, opposé à l'organisation dite Etat Islamique, (...) et ce, alors que le territoire de la République a été frappé et reste frappé par le terrorisme islamiste*"[35].

B. La numérisation des conflits politiques

Le numérique est rapidement apparu comme une nouvelle ressource puissante à mobiliser par les États, notamment dans le cadre de conflictualités. L'ambivalence tient du fait que le cyberespace se trouve être à la fois un espace de puissance et un espace de vulnérabilité pour les États. La course à l'espace de la fin du XXème siècle a alors laissé place aujourd'hui, à une course au cyberespace dans laquelle l'État le plus victorieux est celui qui réussira à maîtriser au mieux cette nouvelle arène immatérielle. Se sont alors développées des discussions sur la notion de "*cyberguerre*" pour désigner les cyberattaques stratégiques menées par un État afin de déstabiliser, ou de causer un préjudice à un autre. Pour autant, il reste en pratique difficile d'identifier l'origine et les auteurs de ces attaques qui ne cessent de se multiplier et qui profitent de difficultés probatoires quant à leur attribution, souvent déduite des circonstances de fait.

[33] TGI Paris, référé, 22 mai 2000 s'agissant d'un site d'apologie du nazisme proposant à la vente des uniformes et insignes nazis
[34] Utilisé en matière de contrefaçon : Criminelle 9 septembre 2008, n° 07-87.281
[35] Chambre criminelle, 7 novembre 2023, 22-87.230

À ce titre, quelques exemples peuvent être cités, en commençant par la cyberattaque par déni de service[36] connue par l'Estonie le 27 avril 2007. Cette attaque a notamment été attribuée à la Russie par le gouvernement américain, en raison du fait qu'elle est survenue le lendemain du déplacement de la statue du Soldat de bronze - représentant un soldat en uniforme soviétique - du centre de la capitale vers un cimetière militaire. À cette date, alors que l'Estonie était l'un des États les plus dématérialisé du monde[37], l'auteur de l'attaque a su faire usage de cette "cyberdépendance" pour paralyser entièrement le pays en bloquant l'accès à de nombreux sites tels que celui du Parlement, des banques, des ministères et des journaux. Plus récemment, en 2020 et de façon inédite, l'ancien président américain Donald Trump avait révélé avoir organisé une cyberattaque contre l'organisation russe de diffusion de propagande sur Internet, *Internet Research Agency*, accusée d'avoir influencé l'élection présidentielle en 2016 dans l'affaire du Russiagate. Enfin, un exemple actuel de cyberguerre est celui de l'extension du conflit physique qui oppose l'Ukraine et la Russie au cyberespace, au sein duquel les deux États s'affrontent à coup d'attaques informatiques, et de campagnes de propagande et de désinformation en ligne.

En définitive, il apparaît que les armes numériques prennent aujourd'hui le dessus sur la souveraineté étatique, par la possibilité de déstabiliser et perturber le fonctionnement d'un État sans avoir à franchir ses frontières. Il ressort de ces exemples, que les grandes puissances du XXème siècle, et particulièrement la Russie, constituent aujourd'hui des "*cyber puissances*" du XXIème siècle, qui parviennent à mobiliser le numérique comme un nouvel outil stratégique, redoutable dans un monde interconnecté. Paradoxalement, il est intéressant de noter que la Russie fait régulièrement obstacle - pour des mobiles politiques notamment - aux poursuites étrangères contre les cybercriminels. Ainsi, il convient de voir pour finir, que la souveraineté constitue également une pierre d'achoppement dans la lutte contre la cybercriminalité.

[36] *Ddos* (ou attaque par déni de service) est une attaque informatique qui consiste à saturer un serveur afin de le rendre inaccessible.
[37] Il s'agit du premier État à avoir une administration totalement dématérialisée, d'où le jeu de mot souvent employé de "E-stonie" (la lettre E faisant référence à l'électronique).

§2. L'obstacle de la souveraineté nationale

La souveraineté nationale, autant qu'elle souffre de l'avènement de la cybercriminalité, constitue paradoxalement un obstacle à la lutte. En effet, en traçant ses frontières, l'État souverain trace également le champ d'application spatial de son droit national et plus généralement de son pouvoir de coercition. Dès lors, il s'affirme comme seul compétent pour traiter des affaires ayant eu lieu ou étant rattachés à son territoire. Concomitamment à la reconnaissance de cet obstacle procédural, la première convention de lutte contre la cybercriminalité a vu le jour le 23 novembre 2001 à Budapest, où se sont réunis des États désireux d'harmoniser leurs législations et de concentrer leurs moyens opératoires. Malgré cette ambition nourrie de bonne volonté, la convention s'est elle-même heurtée à ses propres limites tenant à la fois à l'insuffisance et à l'hétérogénéité des États signataires. Or, la lutte contre la cybercriminalité est elle-même dépendante de la coopération étatique, qui est tantôt refusée, tantôt freinée.

A. Le refus de coopération

Au vu du caractère transnational de cette criminalité, son traitement exige, par essence, une solide coopération des États. Or, certains États se montrent réticents et refusent, par faute de volonté ou de moyens, d'engager toute coopération étatique. Les cybercriminels vont alors s'accorder la faveur de localiser leurs infractions dans des "cyber paradis"[38], c'est-à-dire des États aux législations faibles, voire inexistantes ou simplement non coopératives.

a. Le manque de moyens

Tous les États ne sont pas également armés face au phénomène cybercriminel. En effet, l'avènement du numérique a eu pour effet de renforcer la fosse aux inégalités entre les États, à laquelle se greffent les difficultés sous-jacentes de l'accès inégal aux technologies d'une part, et l'insuffisance des moyens de lutte d'autre part. En effet, la lutte contre la cybercriminalité suppose en soit des moyens financiers et humains considérables, dont ne disposent pas ou peu les pays émergents et en développement.

[38] Terme utilisé par la magistrate spécialiste de la cybercriminalité, Myriam Quéméner

Dès lors, leur arsenal de lutte s'en trouve fragilisé, avec une cybersécurité rudimentaire et une législation inadaptée à ce nouveau risque. Ces pays se trouvent de ce fait en situation d'interdépendance vis-à-vis des grandes souverainetés numériques, constatée lors du sommet du G7 qui s'est tenu à Hiroshima du 19 au 21 mai 2023. C'est pourquoi le Japon, figurant parmi les pays les mieux dotés en termes de cybersécurité, s'est alors chargé de la formation de professionnels de la sécurité dans toute la région de l'ANASE[39], par le biais de l'Agence japonaise de coopération internationale (JICA). Toutefois, comme le souligne le spécialiste japonais Furukawa Masayuki, "*certains pays en développement manquent même des moyens humains et financiers pour pouvoir tirer pleinement parti de l'assistance offerte par divers pays et organisations*"[40]. En effet, les moyens de lutte contre la cybercriminalité sont très coûteux et supposent en tout état de cause, des moyens financiers dont ne disposent pas ces États cyber vulnérables.

b. Le manque de volonté

Très souvent la coopération internationale est refusée non pas par manque de moyen mais plutôt par un manque de volonté des États, généralement motivé par des différends politiques. Bien que le nombre de signataires de la Convention de Budapest accroît constamment, plus de la moitié des pays du monde n'en font pas partie, et représentent ainsi, un lieu privilégié de localisation de la cybercriminalité ou de ses fruits. La Russie, qui représente le premier bouclier contre les poursuites et qui abrite un nombre considérable de cybercriminels, refuse catégoriquement depuis 2001 d'intégrer la Convention de Budapest au motif qu'elle serait en contradiction avec la Constitution russe. En réalité, il semblerait que ce motif avancé serve uniquement à camoufler les réelles intentions de protection des cybercriminels russes, perçus comme le maillon fort dans la lutte menée contre l'Occident. Au-delà des motivations politiques, le refus de coopération est souvent justifié par un sentiment de méfiance nourri par la multiplication d'attaques silencieuses conduite par des États au détriment d'autres.

---

[39] ANASE (Association des Nations de l'Asie du Sud-Est) : Organisation intergouvernementale politique, culturelle et économique regroupant 10 États de l'Asie du Sud-Est dont la Thaïlande, les Philippines ou encore l'Indonésie.

[40] Article de la JICA [Spécial G7 - No 3] *Les cyber-vulnérabilités des pays en développement sont une menace pour tous*, 2023/05/18

Enfin, il est à noter que le cybercriminel désireux d'échapper à la répression, fait souvent le choix de recourir à la stratégie du "*forum shopping*"[41] en localisant les faits dans un État où ils ne sont pas constitutifs d'une infraction. De surcroît, les prestataires techniques font le choix, au même titre que les cybercriminels, de restreindre leur responsabilité en s'installant au sein d'États permissifs qui généralement n'imposent aucune collaboration de la part de ces entreprises. Dès lors, ce refus de coopération est double et provient tantôt des États, tantôt des opérateurs, tantôt des deux à la fois.

B. Les limites de la coopération

Bien que la coopération internationale soit nécessaire, celle-ci se trouve également être difficile à mettre en œuvre. Une première difficulté à la coopération, inhérente à cette forme de criminalité, tient à l'attribution de l'attaque qui est souvent disputée entre les États afin de se prévaloir de leur compétence juridictionnelle. Un énième obstacle juridique découle de la différence de législation entre les États concernant les règles régissant les investigations. En effet, quand bien même l'État ne s'opposerait pas aux investigations, sa législation nationale peut représenter à son tour un frein auquel il n'est pas possible de déroger en vertu de la souveraineté étatique. Ainsi, l'État requérant ne peut pas s'attendre à ce que les investigations se déroulent selon les règles de sa propre législation, et encore moins permettre à un de ses agents d'exercer lui-même les actes d'investigations, et donc d'exercer des prérogatives de puissances publiques en territoire étranger. Or, la recherche de preuve en matière de cybercriminalité suppose de recourir aux actes d'investigations les plus attentatoires aux libertés, et donc les plus difficiles à mettre en œuvre. Dès lors, les règles protectrices de l'État requis peuvent ralentir les investigations, de sorte que très souvent la coopération internationale est décriée. Cette limite s'observe particulièrement en matière de perquisition, pour laquelle les conditions sont très strictes lorsque la coopération est menée avec les États-Unis - premier pays d'où proviennent le plus grand nombre de cyberattaques - en raison de l'importance particulière accordée traditionnellement au droit de propriété.

[41] Terme utilisé par le magistrat David Bénichou afin de faire référence aux stratégies de paralysie de l'enquête

Cette disparité dans les législations, que la Convention de Budapest a tenté de résoudre, est une source de pesanteur pour les investigations qui trainent dans le temps alors même que la preuve numérique exige une rapidité d'action. L'intégration d'un premier protocole additionnel à la Convention[42], puis d'un second tenant à renforcer la coopération internationale en matière de preuves numériques[43], témoigne des divergences qui demeurent entre les États parties.

Un autre obstacle, d'ordre idéologique, tient à la différence de conception de la cyberdéfense entre les États. En effet, certains États -en particulier occidentaux- sont particulièrement attachés à la liberté que représente le numérique, et notamment Internet, de sorte qu'ils restreignent la répression aux formes les plus graves de criminalité. En revanche, d'autres perçoivent d'un mauvais œil cet espace de liberté, et y voient un espace d'anarchie qu'il faut absolument contrôler, et ce même au détriment des droits et libertés. Dès lors, la coopération entre ces États aux positions discordantes affecte l'enquête, dès lors que les uns comme les autres ne s'entendent pas sur quel comportement poursuivre ou non.

Enfin, une coopération effective suppose au préalable qu'il existe une relation de confiance entre les États, pierre angulaire des relations internationales. À ce titre, dans le rapport d'information du sénateur Jean Marie Bockel, celui-ci affirmait qu'il "*n'existe pas réellement d'alliées dans le cyberespace*"[44]. Or, ce manque de confiance mutuelle est en soit accentué par la difficulté d'identification des auteurs des cyberattaques - pouvant être les États eux-mêmes - , ce qui dissuade fortement les uns de partager aveuglément aux autres des informations sensibles et d'ouvrir ainsi, des failles dans leur propre sécurité.

[42] Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques du 28 janvier 2003
[43] Deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques du 29 mars 2022
[44] Rapport d'information du Sénat- La cyberdéfense : un enjeu mondial, une priorité nationale, p.53, 2012

TITRE 2. Une criminalité en rupture avec la procédure pénale classique

Section 1. La désuétude de la procédure pénale traditionnelle

§1. Une procédure inadaptée à l'immatérialité de la cybercriminalité

Avec l'émergence de cette nouvelle forme de criminalité, la procédure pénale traditionnelle a rapidement été confrontée à ses limites. En effet, classiquement, le crime -*lato sensu*- supposait une présence physique de l'auteur et de la victime de l'infraction, voire un contact entre ces derniers. De même, la criminalité traditionnelle impliquait généralement une proximité de lieu entre la victime et l'auteur. Désormais, par le jeu de l'immatériel, ce raisonnement par implication n'a plus lieu d'être et la procédure pénale perd ses repères. C'est en ce sens que le rapport "Protéger les internautes"[45] faisait justement état de "*l'impuissance des mécanismes classiques d'investigation, fondés sur un accès physique au suspect comme aux éléments de preuve*".

A. L'anonymat du cybercriminel

Hormis le cas où le suspect est en fuite et introuvable, la procédure pénale traditionnelle repose sur l'idée d'une mainmise de la justice sur le suspect, ce dernier étant arrêtable et à tout le moins identifiable. La garde à vue, les auditions et interrogatoires, ou encore les perquisitions sont autant d'actes d'enquête qui supposent un accès physique au suspect, généralement présent sur le territoire.

Par le jeu de l'immatérialité, la cybercriminalité bouleverse cette conception présentielle du délinquant qui va profiter des moyens d'anonymisation offerts par le numérique afin d'être non identifiable. En outre, l'absence de contact physique et direct entre le malfaiteur et sa victime constitue une perte considérable d'indices pour l'enquête. C'est d'ailleurs l'une des raisons les plus avancées pour expliquer l'absence de plainte des victimes, qui se sentent alors impuissantes et anticipent l'impunité de l'auteur.

[45] Rapport sur la cybercriminalité « Protéger les internautes », Groupe de travail interministériel sur la lutte contre la cybercriminalité, Février 2014

B. L'immatérialité des preuves

La seconde rupture majeure tient à l'immatérialité des preuves numériques, qui par nature, ne permettent pas un accès physique des enquêteurs mais supposent une manipulation informatique. Comme le souligne le magistrat Alexandre Rousselet-Magri, classiquement, les éléments de preuve de l'infraction devaient par nécessité délinquante être situés près du délinquant. Désormais, le délinquant peut avoir la mainmise sur l'instrument ou le produit du crime sans les détenir matériellement, et sans que ces derniers ne se trouvent sur le territoire français.

§2. L'évolution rapide et incontrôlée de la cybercriminalité

En établissant le constat de la désuétude de la procédure pénale traditionnelle, se pose la question de savoir si un tel constat n'est finalement pas une fatalité. Est-il réellement possible pour la procédure pénale, fruit d'un processus d'évolution lent et réfléchi, de s'adapter à la cybercriminalité, dont l'évolution est rapide et incontrôlée ? Finalement, cette lutte s'apparenterait à un véritable travail de Sisyphe, dès lors que chaque adaptation de la procédure serait suivie d'une innovation de la cybercriminalité.

En outre, plus les technologies s'améliorent et plus les malfaiteurs les utilisent en guise d'arme de destruction massive. Prenons l'exemple des logiciels malveillants, qui n'épargnent aujourd'hui personne et dont les conséquences sont démesurées et variables. Un logiciel malveillant, qualifié de malware[46] en anglais, est un logiciel nuisible comparable à un virus en ce qu'il infecte le système informatique de la victime sans son consentement. À l'origine, les premiers logiciels malveillants étaient utilisés à de simples fins telles que l'arrêt d'un ordinateur, ou encore la création de dysfonctionnements informatiques. Aujourd'hui, un logiciel peut constituer une véritable arme de destruction massive. À ce propos, le virus dénommé Stuxnet développé par la NSA est considéré comme le plus destructeur des logiciels malveillants en ce qu'il a été initialement conçu pour attaquer les centrales nucléaires iraniennes. Avec l'évolution de la technologie, ces logiciels malveillants deviennent de plus en plus difficiles à détecter et surtout de plus en plus difficiles à éradiquer.

[46] Pour "malicious software" c'est à dire logiciel malveillant

C’est par ailleurs cette évolution incontrôlable des technologies qui conduit le législateur à intervenir avec prudence afin de ne pas enserrer les articles dans un champ d’application qui deviendrait trop rapidement désuet. Or, l’évolution des technologies a pour corollaire l’évolution des formes de cybercriminalité : au départ réduite au piratage, la cybercriminalité devient de plus en plus sophistiquée et diversifiée. C’est pourquoi l’énumération des formes de cybercriminalité constitue en réalité une entreprise vaine, tant l’adaptation aux nouvelles technologies est constante et tant ses branches sont multiples.

Section 2. Les freins à la poursuite de la cybercriminalité

§1. La technicité de la matière

Le numérique, en tant que tel, renvoie à une matière technique et complexe, qui se compose d’un univers et d’un langage propre. Dès lors, cette technicité constitue le premier frein au traitement judiciaire de la cybercriminalité, d’où la priorité par les autorités nationales de former tant faire se peut le corps de la justice.

A. Un langage spécifique

Comme chaque science, l’informatique a son propre vocabulaire et ses propres codes que les profanes de la technologie numérique ignorent. Alors que les nouvelles technologies imprègnent notre quotidien, seule une fraction de la population parvient effectivement à maîtriser ces outils. L’informatique repose en effet sur des branches mathématiques complexes tels que l’algèbre, le calcul ou encore la géométrie. La création et l’utilisation de logiciels, par exemple, se font à partir d’algorithmes composés d’une suite d'instructions unique. De même, la cryptographie et les codes reposent sur une suite de chiffres précis afin de parvenir à un résultat déterminé. Les logiciels, les programmes informatiques, les sites webs, et tout ce qui a trait au numérique, sont eux-mêmes fondés sur une chaîne de texte inintelligible pour les novices. En outre, l’étude de la cybercriminalité et les présents développements témoignent de la difficulté inhérente à la compréhension de la matière issue de l’existence d’un jargon propre à l’informatique, très souvent conçu à partir de la langue anglaise.

B. Un matériel spécifique

En ayant recours aux nouvelles technologies, la cybercriminalité a bousculé les conceptions traditionnelles de "*l'arme du crime*". Par la mobilisation de moyens informatiques matériels (ordinateurs, téléphones, disques durs…) et de moyens informatiques immatériels (logiciels, fichiers informatiques…), la cybercriminalité engendre de nouveaux défis pour les enquêteurs dont la formation représente une nécessité évidente. En 2014, le groupe de travail interministériel sur la lutte contre la cybercriminalité établissait déjà le constat d'un "*traitement très inégal des procédures liées à la cybercriminalité, faute de bien saisir le fonctionnement des technologies de l'information et de la communication et de savoir manier aisément les preuves numériques*". Dès lors, la formation des enquêteurs est primordiale, d'une part en ce que ce matériel sert de support au cybercriminel, et d'autre part en ce qu'il sert de support aux techniques d'investigations numériques.

§2. La constitution de la preuve numérique

Le maître de conférence Sarah-Marie Cabon affirmait avec justesse que « *les investigations fondées sur un accès physique au suspect comme aux éléments de preuve semblent aujourd'hui dépassées* ». En effet, la dématérialisation de l'infraction emporte de manière causale, la dématérialisation de sa preuve. Ainsi, tantôt il s'agira de preuves classiques qui ont été numérisées - telle qu'une photographie - tantôt il s'agira de preuves numériques au sens strict du terme, en ce qu'elles ont été obtenues avec l'aide et par une technologie.

A. Le difficile accès à la preuve numérique

a. La localisation de la preuve

Comme en matière de criminalité classique, le préalable à tout recueil de preuves est celui de sa localisation. Or, la virtualité du cyberespace et l'immatérialité des preuves constituent de nouvelles sources de difficultés pour l'enquête. Dès lors, émergent deux problématiques : la première tenant à l'incapacité de localiser la preuve, et la seconde tenant à la délocalisation volontaire de la preuve à l'étranger.

Dans le premier cas de figure, le cybercriminel va employer des moyens techniques afin d'organiser l'intraçabilité des preuves. Ainsi, pour rendre leur identification d'autant plus délicate, les cybercriminels ont fréquemment recours à un service VPN[47] qui permet un accès privé et sécurisé à Internet. Tout comme la cryptologie, le VPN est un outil légal imaginé à l'origine à des fins sécuritaires légitimes, notamment afin de protéger les données des particuliers contre les procédés cybercriminels. Dès lors, la contradiction relève du fait que ces services sont également utilisés par les criminels afin de dissimuler leur activité, en profitant des fonctionnalités offertes par le VPN qui permettent de chiffrer la connexion, masquer l'adresse IP[48], ou encore camoufler la localisation de l'utilisateur. Non seulement le VPN permet de masquer la localisation réelle, mais il permet également à son utilisateur de changer la localisation virtuelle en utilisant l'adresse IP d'un serveur éloigné, généralement situé dans un autre pays. En plus du recours à ces VPN, les cybercriminels utilisent constamment la monnaie virtuelle qu'est la crypto monnaie, facilitant l'intracabilité des paiements en ligne, même transnationaux. En effet, la crypto monnaie est une monnaie électronique qui ne dépend d'aucun système bancaire, et échappe de ce fait au contrôle étatique. Son usage a alors la particularité de permettre d'effectuer des transactions financières, et ce, sans révéler des informations personnelles sur les parties. C'est pour ces raison qu'elle constitue la monnaie d'échange privilégiée par les cybercriminels, idéale pour commettre des infractions économiques et financières sans laisser de traces derrière soi.

Dans le second cas de figure - cumulable avec le premier -, le cybercriminel va délocaliser la preuve dans des serveurs étrangers, afin de contraindre les enquêteurs à la lourdeur de la coopération internationale, en espérant que celle-ci soit refusée. Cette difficulté a été particulièrement pointée s'agissant de l'usage de gestionnaires cloud[49], localisés généralement hors de l'Union européenne, et qui permettent de stocker, traiter et gérer des données au sein de serveurs informatiques à distance connectés à Internet. Le cloud permet alors aux utilisateurs d'accéder et de modifier son contenu à partir de n'importe quel appareil, et depuis n'importe quel territoire.

---

[47] VPN, de l'anglais *Virtual Private Network*, signifie "réseau privé virtuel".

[48] Adresse IP - *Internet Protocol* - : suite de chiffres unique attribuée à un appareil connecté à Internet, s'apparentant donc à une identité sur internet

[49] Cloud computing -en français "l'informatique en nuage" fait référence, sémantiquement, à des " systèmes informatiques fonctionnant par l'action conjointe d'éléments disparates réunis indépendamment de leur localisation géographique et de l'infrastructure sous-jacente", Wikipédia

Il est à noter que ces gestionnaires refusent généralement de collaborer avec les autorités étatiques, ce qui permet largement aux actes de cybercriminalité d'échapper aux poursuites. C'est pourquoi le droit français a ouvert une porte de secours pour les enquêteurs, dans le cas où les données stockées en cloud computing seraient accessibles depuis le domicile perquisitionné[50].

En définitive, force est de constater que les cybercriminels profitent des progrès issus de la technologie, et surtout de la combinaison de moyens légaux pour dissimuler les preuves et leur identité. Il faut noter que par précaution, ces derniers ne vont pas recourir à des moyens commercialisés publiquement, tel qu'un VPN proposé par une application mobile, mais vont préférer des services élaborés et commercialisés par leurs confrères qui opèrent au sein d'un circuit criminel finement élaboré.

b. Le cryptage de la preuve

Une autre difficulté, courante en matière de cybercriminalité, est celle issue du cryptage. Le cryptage est un procédé commun de chiffrement qui permet de sécuriser l'accès à un fichier ou à des données. Il faut alors distinguer la cryptographie au sens strict, qui consiste en un jeu de mots ou en une succession de mots, du chiffrement qui fait lui usage d'une clé de chiffrement composée de chiffres et de lettres. Le plus vieil exemple de cryptographie remonte au XVIème siècle avant Jésus Christ, en Mésopotamie, avec une tablette d'argile sur laquelle était gravée la recette secrète d'un potier qui avait modifié l'orthographe des mots et effacé des consonnes afin de la rendre illisible. Aujourd'hui, ce procédé se généralise et s'utilise - au-delà des fins malveillantes du cybercriminel- à des fins sécuritaires. En France, "*l'utilisation des moyens de cryptologie est libre*"[51]. Toutefois, le législateur conscient du risque de l'usage de la cryptologie à des fins malveillantes a prévu à l'article 132-79 du Code pénal, l'aggravation des sanctions dès lors que le moyen de cryptologie "*a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission*".

[50] Cf "Les perquisitions informatiques" p.51
[51] Article 30 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Dans le cadre de la recherche de preuve, il convient de distinguer selon que c'est la preuve en soit qui est crypté, ou selon que c'est le support dans lequel elle est contenu qui l'est. Ces différentes problématiques sont apparues notamment lors de deux fameuses affaires américaines, opposant le FBI et la NSA aux géants du Web Google et Apple. Dans l'affaire opposant la NSA à Google, l'agence de sécurité nationale affirmait que le chiffrement de la messagerie l'avait empêchée de détecter le projet d'attaque terroriste mené à Paris le 13 novembre 2015. Dans la seconde affaire opposant le FBI à Apple, c'était l'accès au téléphone chiffré d'un terroriste qui avait été refusé par la société. Ainsi, tantôt c'est le contenu qui est chiffré, et tantôt c'est le contenant qui l'est. Bien que ces deux affaires ne portent pas sur des cyber crimes, elles illustrent bien la difficulté pratique inhérente aux données cryptées, et l'obstacle que peuvent constituer les sociétés de communications généralement non coopératives.

En France, l'article 230-1 du Code de Procédure pénale permet au procureur de la République, au juge d'instruction ou encore aux juridictions de jugement d'ordonner le déchiffrement des données à toute personne physique ou morale qualifiée. Poussant encore plus loin le levier de la sévérité, le législateur a également imposé -au risque de sanctions- à quiconque ayant connaissance de la convention secrète de déchiffrement de la remettre aux autorités judiciaires[52]. À ce propos, la Cour de cassation avait renvoyé une question prioritaire de constitutionnalité sur le point de savoir si telle obligation valait également à l'égard du suspect, et le cas échéant, si cette obligation constituait une atteinte au droit de garder le silence et au droit de ne pas s'auto-incriminer. De façon inattendue, le Conseil constitutionnel a jugé que la disposition n'a pas pour objet l'obtention d'aveux, et n'emporte ni reconnaissance ni présomption de culpabilité en ce qu'elle permets seulement le déchiffrement des données cryptées[53]. Il est regrettable de constater que cette décision a été faiblement motivée, et ne semble pas répondre clairement à la question posée.

[52] Article 434-15-2 du Code pénal
[53] Conseil Constitutionnel, (QPC) n°2017-696 du 30 mars 2018

c. La destruction de la preuve

Enfin, il convient de formuler un dernier développement sur la volatilité de la preuve numérique. Contrairement à la preuve physique, la preuve numérique est quant à elle facilement accessible pour l'auteur de l'infraction dont la présence physique n'est pas nécessaire à sa destruction. En plus de cette possible destruction volontaire, intervient la difficulté inhérente aux preuves éphémères, destinées par nature à disparaître.

L'enquête pénale est alors confrontée à un impératif de rapidité, face à des preuves qui, contrairement aux preuves classiques, ne résistent pas ou très peu au temps. Or, une nouvelle difficulté émerge en raison de l'absence de règles communes s'agissant de la durée de conservation des données par les hébergeurs de contenus sur Internet. Certains États ont alors imposé à ces opérateurs un délai légal de conservation des données personnelles, sous réserve qu'elle soit limitée dans le temps et réponde à des finalités précises. Cette conservation est essentielle à l'enquête dès lors que ces données, particulièrement les données de connexion, sont le réceptacle des preuves de la cybercriminalité. Comme le souligne le rapport d'information déposé par le Sénat en 2023[54], "*les données de connexion constituent en cas d'infraction, autant de gisements de preuves qui ont le pouvoir de confirmer ou d'infirmer un alibi, de mettre au jour un mobile ou de rendre visible une complicité qu'un examen de preuves matérielles n'aurait pas rendue apparente*". Les données de connexion, également appelées "métadonnées", désignent un ensemble de données personnelles produites lors de la connexion d'un appareil à un réseau de communication électronique. Il s'agit pour les enquêteurs d'un précieux moyen d'identification du cybercriminel comprenant notamment l'adresse IP de l'utilisateur, son identifiant, ainsi que les dates et heures exactes de connexion. Leur accès est donc essentiel afin de retracer l'activité d'un criminel, voire de l'identifier.

[54] Rapport d'information n° 110 (2023-2024), déposé le 15 novembre 2023 "*Surveiller pour punir ? Pour une réforme de l'accès aux données de connexion dans l'enquête pénale*"

Toutefois, le droit de la protection des données à caractère personnel représente une muraille de Chine pour les enquêteurs en ce qu'il conditionne très strictement l'accès et la conservation de ces données sensibles. En France, pour les besoins de lutte contre la criminalité et la délinquance grave, les opérateurs sont tenus de conserver les données relatives aux connexions Internet jusqu'à l'expiration d'un délai d'un an[55]. Pour les besoins de l'enquête, les prestataires techniques sont tenus de divulguer ces données de connexion, notamment au regard de l'obligation générale d'apporter son concours à la justice. L'accès aux données ne se fait donc pas directement par les enquêteurs, et nécessite de recourir aux prestataires techniques en tant qu'intermédiaire. Pour autant, un frein sous-jacent tient au fait qu'en tout état de cause, il existe un décalage entre cette durée de conservation obligatoire d'un an et les délais d'exercice de l'action publique. En outre, seuls les hébergeurs français sont tenus à cette obligation alors même que ces données sont détenues essentiellement par des prestataires étrangers, ce qui a occasionné dans de nombreux cas, un blocage des investigations.

Enfin, il convient de s'intéresser au cas où la destruction de la preuve résulterait d'un acte positif du cybercriminel, qui tantôt profite du caractère éphémère des données, et tantôt les détruit volontairement. Aujourd'hui, une série d'applications de messagerie telles que Whatsapp ou encore Viber - nullement criminelles -, permettent l'envoi de messages et multimédias éphémères qui disparaissent automatiquement de la messagerie du destinataire après visualisation du contenu. L'utilisateur peut également lui-même configurer la durée de conservation de ces messages en un simple clic. Les sociétés propriétaires de ces applications ne cessent d'affirmer que la finalité de cette fonctionnalité est d'assurer la confidentialité de leurs utilisateurs. De ce fait, il est difficile voire impossible pour les enquêteurs de récupérer les messages supprimés automatiquement et donc de collecter des éléments probatoires. Pour finir, la seconde hypothèse est celle de la destruction volontaire de la preuve numérique. Alors qu'il peut être une lourde et difficile tâche pour le criminel d'effacer les traces physiques de son crime, cette destruction est facilitée par l'usage du numérique qui permet rapidement d'effacer une preuve, et ce même à distance. Il faut noter que dans ce cas, le recours au cloud computing est un réel avantage, en ce que la suppression du contenu sur un appareil emporte la suppression de ce même contenu sur tous les autres appareils connectés.

[55] Article L34-1 II bis, 3°du Code des postes et des communications électroniques

B. La difficile recevabilité de la preuve numérique

Le régime de la preuve numérique n'est pas dérogatoire à celui de la preuve classique de sorte qu'une fois collectée, se pose la question de savoir si elle sera recevable devant les tribunaux.

a. Le risque d'altération de la preuve numérique

Par nature, les preuves numériques sont fragiles et peuvent être facilement falsifiées ou altérées par leur seule manipulation. Lors des investigations, l'enquêteur ou l'expert doit de ce fait être extrêmement vigilant au moment de la manipulation de la preuve numérique afin d'en préserver l'intégrité et pouvoir ainsi, la produire en justice. En la matière, le principe d'échange développé en 1919 par Edmond Locard, selon lequel un transfert s'opère à chaque contact entre deux corps, est tout à fait transposable. D'après le maître de conférence Sophie Sontag Koenig, "*appliqué à l'informatique, ce principe illustre le fait que lorsqu'un enquêteur ou un utilisateur interagit avec un système en fonctionnement, des modifications sont apportées par ce dernier.*". Alors que la criminalité classique permet le placement sous scellé des preuves pour les authentifier, la cybercriminalité suppose quant à elle une opération de préservation informatique, complexe et délicate.

Les enquêteurs vont généralement procéder à une copie physique du support, à l'aide d'ordinateurs et de logiciels *forensics*[56], sans le manipuler directement afin de ne pas affecter son contenu et ses propriétés. Il s'agit dans ce cas d'un dead forensics, c'est-à-dire d'une analyse à froid. Le praticien va alors retirer le disque dur sans allumer l'ordinateur, afin de le connecter à un dispositif de blocage en écriture de données qui permet d'éviter toute modification. Les enquêteurs -ou experts- procèdent par la suite à une copie physique exacte du support original. Au lieu de connecter directement le disque à l'ordinateur du suspect, ils disposent d'un ordinateur forensic : le dispositif est donc relié à l'ordinateur forensic afin d'assurer qu'il n'y ait aucune modification. Cette méthode va permettre d'obtenir une image forensic qui est la copie conforme du contenu initial contrairement au copier-coller qui altère l'intégrité de la preuve, et notamment des dates.

[56] Forensic : investigation numérique sur un système d'information

Dans le cas où on ne pourrait pas retirer le disque dur, il existe une autre technique qui n'est pas sans risques : là encore, l'ordinateur est éteint. Une clé USB va être configurée à l'avance avec un logiciel Linux afin d'être connectée au support, et permettre ainsi l'accès au disque dur. Puis, une copie des données est réalisée sur un disque dur externe, avec encore une fois un blocage des données. Enfin, dans le cas où les deux techniques seraient impossibles, les enquêteurs seront contraints d'allumer l'ordinateur, puis de lancer des logiciels d'analyse et de récupération. Dans cette hypothèse, la modification des données est inévitable, ce qui en fait uniquement une solution de dernier recours.

b. La limite du principe de loyauté de la preuve

La recevabilité des preuves en justice est subordonnée au respect des règles d'administration de la preuve. Alors que le législateur érige la liberté de la preuve en principe du droit pénal à l'article 427 alinéa 1 du Code de procédure pénale, le champ particulier de la cybercriminalité invite à s'interroger sur la licéité des procédés en termes de recueil de ces preuves, notamment au regard du principe de loyauté. Tandis que les particuliers échappent à cette exigence, l'action de l'autorité publique demeure quant à elle strictement contrôlée par le juge. Étymologiquement, l'adjectif loyal dérive du latin « *legalis* » c'est-à-dire conforme à la loi. Alors que la langue française différencie nettement les termes loyal et légal, étymologiquement ces mots se rejoignent. C'est en ce sens que le droit français inclus dans l'exigence de loyauté de la preuve, d'une part le recours à des procédés légaux ou du moins à des procédés qui ne sont pas en contradiction avec la loi, et d'autre part l'honnêteté et la droiture de l'agent étatique qui administre cette preuve.

Le droit français dresse depuis plusieurs années une distinction entre la provocation à la preuve et la provocation à l'infraction. Tandis que la première est admise, la seconde est quant à elle constitutive d'une nullité de procédure. La différence tiendrait principalement au fait que dans le premier cas l'agent est passif et se contente de constater l'infraction commise ou qui se commets, alors que dans le second cas il outrepasse ses missions en adoptant un comportement actif consistant dans la mise en œuvre d'un stratagème ayant influencé le mis en cause à commettre l'infraction. Or, dans bien des cas, la mise en œuvre de cette distinction s'avère être délicate. En la matière, le respect de cette exigence de loyauté est rendu d'autant plus difficile pour les enquêteurs dans le cadre des investigations numériques, qui supposent fréquemment l'intervention de l'agent pour collecter des preuves.

Comme le remarque justement le Professeur Agathe Lepage, "*Internet facilite grandement certaines activités de délinquance mais, en retour, Internet offre aux enquêteurs des possibilités inédites de surveiller des suspects ou de confondre des auteurs d'infractions*"[57]. Dès lors, la tentation est grande pour les enquêteurs d'attirer les cybercriminels en recourant à diverses méthodes telles que la création de sites d'activités criminelles. Le juge va alors apprécier in concreto le procédé mis en œuvre par les enquêteurs, et ce même lorsqu'il a été exécuté à l'étranger par des agents étrangers, afin d'admettre ou non la preuve en justice. Ainsi, la Cour de cassation avait jugé que la création par les autorités américaines d'un site d'échange sur les techniques de fraude à la carte bancaire ne constituait pas une provocation à la commission d'infractions[58]. En l'espèce, la Cour avait retenu qu'aucun stratagème n'avait été mis en place, et que les autorités américaines s'étaient contenté de surveiller et d'enregistrer les échanges à l'insu des personnes concernées. Dès lors, la perquisition incidente autorisée au domicile d'un français impliqué et identifié grâce au site échappait également à la nullité. Dans cette espèce, les agents américains étaient loin d'être totalement passifs dès lors qu'ils ont créé eux-même un site permettant la vente et l'achat de numéros de cartes bancaires, et facilitant ainsi la rencontre des cybercriminels. Pour autant, dès lors qu'ils n'ont fait que surveiller les échanges délictueux, il ne pouvait leur être reproché d'avoir influencé la commission de l'infraction.

[57] Communication Commerce électronique n° 9, Septembre 2014, comm. 73 "La distinction entre provocation à la preuve et provocation à la commission d'une infraction à l'épreuve d'Internet", par Agathe LEPAGE
[58] Criminelle, 30 avril 2014, n°13-88.162

CONCLUSION DE LA PREMIÈRE PARTIE

Cette forme contemporaine de criminalité entraîne des défis uniques et aux multiples facettes pour les États du monde entier, qu'elle menace tant dans leur souveraineté que dans leur stabilité politique et financière. L'exploitation des technologies numériques va permettre d'une part de faciliter la commission d'une variété d'actes illicites, et d'autre part, de constituer des obstacles à l'enquête en complexifiant à la fois l'accès au cybercriminel et aux éléments de preuves. La nature transnationale des crimes, la volatilité des preuves numériques, la difficile identification du cybercriminel, ou encore l'évolution incontrôlée des technologies sont autant d'obstacles placés les uns après les autres, qui ralentissent voire paralysent totalement l'enquête pénale.

Dès lors, un traitement efficace contre cette nouvelle menace complexe et évolutive exige par nature, une approche globale et proactive des autorités avec le renforcement de la coopération internationale, de la collaboration avec les acteurs privés, et surtout des moyens techniques et humains de l'enquête pénale.

PARTIE 2. LA CONSTRUCTION D'UN ARSENAL PÉNAL DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Titre 1. La spécialisation des services d'enquête

Une telle criminalité, au regard de sa spécificité, de sa technicité et des difficultés qu'elle soulève, a fait apparaître l'impérieuse nécessité de recourir à des services spécialisés et formés, bénéficiant de moyens propres pour mettre en œuvre la poursuite et la répression de la cybercriminalité. Dans une recommandation du 11 septembre 1995, le Conseil de l'Europe avait déjà encouragé les États à créer de telles unités spécialisées. C'est alors qu'ont été créés successivement de multiples organes de lutte contre la cybercriminalité, tant au niveau national qu'international.

Section 1. Les organes de lutte nationaux

Il est à noter positivement que la France est l'un des pays pionnier dans la mise en place d'une structure de lutte contre la cybercriminalité. La création d'organes spécialisés s'est opérée dans deux cadres distincts : d'une part, ont été créées des unités spécialisées au sein de corps étatiques préexistants tels que la gendarmerie, et d'autre part, ont été créé de nouvelles institutions spécialement établies dans le cadre de la lutte contre la cybercriminalité. Il convient néanmoins de s'attarder uniquement sur les principales structures opérationnelles de lutte.

§1. Au sein de la gendarmerie

En 1998, a été institué au sein de la gendarmerie un département de lutte contre la cybercriminalité dénommé aujourd'hui Centre de lutte contre les criminalités numériques, dit C3N. Ce dernier est composé de 4 départements, dont le département investigations sur Internet (D2I) regroupant les enquêteurs sur Internet ou encore le département technique chargé de développer des outils d'analyses et d'investigations. Globalement, le C3N assure des missions d'investigation judiciaire, de renseignement criminel et d'appui opérationnel.

Les enquêteurs du C3N assurent par ailleurs une surveillance active du web grâce aux outils dont ils disposent, de leur propre initiative ou à la suite de plaintes ou encore de saisine par un magistrat. Dans le cadre de cette surveillance active, les membres du C3N sont alors chargés de détecter les infractions commises sur Internet et d'en collecter les preuves. Le département assure également des missions de renseignement criminel afin de prévenir, d'anticiper ou de suivre une activité cyber-criminelle en établissant notamment une typologie des auteurs et victimes, ou encore des modes opérationnels des criminels. Par ailleurs, le C3N intègre en son sein le Centre national d'analyse des images de pédopornographie (CNAIP) qui opère une centralisation des fichiers d'enquête, et participent à l'identification des auteurs et victimes de ce contenu. Enfin, le C3N assume une véritable mission de coordination des investigations à l'échelle nationale, en diffusant des outils et méthodes pour lutter contre la cybercriminalité.

§2. Au sein de la police

Consciente de la menace engendrée par la criminalité numérique, la France a rapidement créé, dès 1994 - au cours de la décennie du développement d'Internet - une brigade centrale de répression de la criminalité informatique (BCRCI), chargée de mener les enquêtes nationales voire internationales en coopération avec les organes internationaux. Cet organe a par la suite été remplacé en 2000, par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), à compétence nationale. Ce dernier intervient pour des enquêtes d'importance majeure au niveau national ou international, en procédant notamment à des actes d'enquête et d'investigations grâce à des moyens techniques spécialisés. L'office occupe un statut très important en ce qu'il constitue l'organe de contact avec les pays signataires de la convention de Budapest, et plus généralement avec le reste du monde notamment par le biais d'Interpol. Par ailleurs, l'office assure une coordination nationale des opérations de lutte contre les infractions liées aux technologies de l'information et de la communication. Enfin, il s'agit du point de contact des signalements d'activités illicites, et plus particulièrement de la pédophilie sur Internet qui occupe une large part du travail de l'office.

Puis, par arrêté du 29 avril 2014, a été créée au sein de la Direction centrale de la police judiciaire (DCPJ), une sous-direction en charge de la lutte contre la cybercriminalité (SDLC), intégrant en son sein l'OCLCTIC. La SDLC représente un organe important de formation des investigateurs spécialisés, et de gestion du réseau des référents cybermenace, dit RCM, qui occupe une mission de renseignement, de sensibilisation et d'accompagnement des acteurs sur le territoire français, notamment auprès des entreprises. En outre, la SDLC dispose de 16 laboratoires d'investigations numériques sur le territoire national, et aide les différents services de lutte contre la cybercriminalité à l'exploitation de supports numériques et à la conception d'outils d'investigations en la matière. Tout comme l'OCLCTIC, la SDLC met à disposition une plateforme de signalement en ligne pour les internautes. Elle constitue également un point d'information pour les enquêteurs, et de mise en contact avec les acteurs d'Internet. Enfin, la SDLC ne se résume pas à des missions d'aide et d'assistance, puisqu'elle se compose également de 3 brigades chargées de la répression des atteintes aux systèmes de traitement automatisé de données (STAD), des escroqueries commises sur Internet et des atteintes aux systèmes de paiement.

Par un décret récent du 23 novembre 2023[59], a été créé l'office anti-cybercriminalité (OFAC), se substituant à la sous-direction de la lutte contre la cybercriminalité (SDLC) et à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Cette combinaison avait notamment pour objectif de simplifier la communication entre les anciens services, afin "*de briser le fonctionnement en silos*", affirme Nicolas Guidoux, chef de l'office anti-cybercriminalité. En outre, l'office présente la particularité d'engager des ingénieurs spécialisés et contractuels, non membres du corps policier. L'office est composé de quatre pôles chargés de l'enquête, de l'appui opérationnel, du renseignement et enfin de la détection des menaces. Ce dernier pôle fonctionne à travers l'emploi des plateformes Thésée et Pharos, la première recueillant les plaintes en ligne des victimes d'une arnaque, et la seconde les signalements des contenus illicites sur les réseaux sociaux. Ces plateformes illustrent bien l'originalité de la lutte contre cette forme de délinquance, en ce que les particuliers et les entreprises participent activement à la collecte de preuves et à la dénonciation des actes criminels.

[59] Décret n° 2023-1083 du 23 nov. 2023 portant création de l'office anti-cybercriminalité

Pour finir, une légère parenthèse doit être consacrée à la dépendance des enquêteurs vis-à-vis de la contribution des opérateurs privés, et notamment des fournisseurs d'accès à Internet. Face à ce constat, le législateur a organisé la participation de ces derniers à l'enquête pénale, notamment en les obligeant à mettre à disposition une procédure de signalement auprès des internautes, et à informer les autorités compétentes de ces activités illégales signalées. Toutefois, lorsque ces opérateurs sont délocalisés, l'enquête pénale reste largement tributaire de la coopération internationale, d'où la nécessité de centraliser les investigations par le recours à des organes de luttes transnationaux.

Section 2. Les organes de lutte transnationaux

§1. À l'échelle européenne

L'Union européenne subit régulièrement des cyberattaques touchant soit directement à ses institutions, soit à ses États membres. En novembre 2022, le site du Parlement européen avait été la cible d'une attaque par déni de service, le rendant inaccessible pendant plusieurs heures. En mars 2023, des députés européens avaient été victimes d'un phishing par l'envoie d'un lien contenant un logiciel espion. La prise de conscience de l'Union Européenne s'agissant de la menace cyber et de la nécessité de mener une lutte coordonnée à l'échelle de la communauté a été précoce, et fait d'elle aujourd'hui, l'organisation internationale la plus avancée en ce domaine. Ainsi, dès 1996 avait été institué au sein de l'Union européenne un comité d'expert chargé de la cybercriminalité.

Aujourd'hui, la lutte contre la cybercriminalité constitue un axe prioritaire de l'agence européenne de police Europol, en tant qu'organe précieux de soutien des services de police des États membres pour la criminalité organisée et transnationale. S'agissant spécifiquement de la cybercriminalité, Europol a créé en 2013 le Centre européen de lutte contre la cybercriminalité, dit EC3, chargé de coordonner et d'appuyer les opérations policières. En outre, l'EC3 permet la centralisation des expertises et des informations, afin de garantir l'efficacité de l'action coopérative, et de promouvoir des solutions à l'échelle de l'Union. Toutefois, la cybercriminalité ne se cantonne pas au seul espace de l'Union européenne, de sorte que la coopération européenne ne peut se suffire à elle-même.

§2. À l'échelle internationale

À une échelle plus large, supra européenne, le soutien est apporté par l'Organisation internationale de police criminelle, Interpol, qui occupe généralement des missions similaires à l'EC3. Interpol a alors créé la Plateforme collaborative sur la cybercriminalité, chargée de la coordination des opérations internationales et de l'analyse de la cybercriminalité. Il s'agit d'un service à accès restreint, au sein duquel les acteurs de la lutte échangent des renseignements liés aux cybermenaces. Afin d'apprécier l'importance de ce point relais, il peut être intéressant de mettre en avant quelques exemples de coopération internationale à ssucès sous l'égide d'Interpol.

En 2021, l'opération Haechi II coordonnée par Interpol et à laquelle ont concouru une vingtaine de pays - dont la France - a permis d'arrêter plus d'un millier de personnes impliquées dans une criminalité financière en ligne. Cette opération de grande ampleur, qui a duré 3 mois, a permis la saisie de près de 27 millions de dollars américains provenant de fonds illicites. Cette explosion de la criminalité financière en ligne a notamment été facilitée par la pandémie du Covid-19 au cours de laquelle la dépendance à l'égard du numérique était démultipliée. Il s'agit de la première opération à retentissement mondial, réunissant des États provenant de chaque continent. Les résultats de l'opération ont en outre révélé le caractère grave, organisé et lucratif de cette criminalité qui est loin d'être une criminalité isolée et à faible enjeu. Comme le souligne le général Jorge Luis Vargas Valencia, Directeur général de la Police nationale colombienne, "*intercepter les produits illicites d'infractions financières en ligne avant qu'ils ne disparaissent dans les poches de « mules » est une course contre la montr*e". En effet, d'après les investigations, les groupes criminels organisés au sein de plusieurs pays utilisaient Internet pour soustraire de lourdes sommes d'argent avant de rapidement les transférer vers différents comptes bancaires au sein de plusieurs pays.

Quelques mois plus tard, de juin 2022 à novembre 2022, a été menée l'opération Haechi III, de plus grande ampleur que la précédente puisque près de 130 millions de dollars ont été interceptés. L'organisation internationale avait conclu à "*la résolution de 1600 affaires de phishing vocal, d'arnaques, d'extorsion, de fraudes et de blanchiment issu de jeux d'argent illicite, commis en ligne*". Lors de cette opération, Interpol a mis en œuvre le nouveau protocole d'intervention rapide anti blanchiment de fonds (en anglais Anti-Money Laundering Rapid Response Protocol ARRP) consistant en un mécanisme mondial de blocage des paiements. Ce protocole avait déjà fait l'objet d'un test lors de l'opération Haechi II, et avait permis l'interception de sommes provenant de fonds illicites.

Le succès de ces opérations, et surtout les enjeux de grande ampleur liés à ces affaires rendent compte de la primordiale nécessité de mener une action supra européenne, en combinant les ressources humaines, financières et techniques de chaque État.

TITRE 2. L'essor de l'investigation numérique

Face à une criminalité qui s'adapte constamment aux évolutions technologiques de la société, les méthodes d'investigations se sont adaptées de la même manière au numérique. À défaut de pouvoir parvenir à l'exhaustivité des techniques d'enquêtes utilisées lors des enquêtes, il sera fait mention des méthodes les plus effectives - en ce qu'elles sont les plus intrusives-, ainsi que des problématiques sous-jacentes à leur utilisation.

Section 1. La numérisation des techniques d'enquête

Répondre à un nouveau défi ne suppose pas nécessairement faire table rase des moyens habituels. Ainsi, les techniques d'investigations initialement conçues pour la criminalité classique et physique ont su trouver juste application dans le cadre de la criminalité numérique.

§1. L'enquête sous pseudonyme : une adaptation de l'infiltration

Dès 1991[60], le législateur avait permis aux enquêteurs français de s'immiscer au sein de réseaux de trafiquants de stupéfiants afin de surveiller les suspects et de permettre le démantèlement de ces réseaux. Étendu à la criminalité et à la délinquance organisée par la loi Perben II du 9 mars 2004, l'article 706-82 du code de procédure pénale organise l'irresponsabilité pénale des agents infiltrés par l'effet de l'autorisation de la loi. Il convient donc de voir en premier lieu la méthode d'infiltration classique avant de voir son adaptation à la cybercriminalité. L'infiltration classique consiste "*pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs*"[61]. L'agent est alors autorisé à faire usage d'une identité d'emprunt et à se comporter comme un délinquant afin de provoquer la preuve de l'infraction et si possible parvenir au démantèlement du réseau criminel.

[60] Loi n°91-1264 du 19 décembre 1991 relative au renforcement de la lutte contre le trafic de stupéfiants
[61] Article 706-81 du Code de procédure pénale

Cette technique d'enquête a été adaptée au numérique, par la loi du 5 mars 2007[62] ayant institué la procédure d'enquête sous pseudonyme dont l'objet est le même que celui de l'infiltration à la seule différence que cette infiltration est numérique et non physique. Initialement réduite à quelques infractions listées, le recours à ce type d'investigation a été généralisé[63] par la loi du 23 mars 2019[64] à tout crime et délit punis d'emprisonnement, dès lors qu'ils ont été commis par la voie des communications électroniques (article 230-46 alinéa 1 du code de procédure pénale). L'enquête sous pseudonyme peut être soit totalement à l'initiative de l'enquêteur, et dans ce cas, ce dernier va s'infiltrer au sein d'un réseau de cybercriminalité et participer à des échanges électroniques avec les suspects, soit l'enquêteur va faire usage du profil de la victime - après avoir recueilli son consentement - et communiquer avec le cybercriminel. De même que l'infiltration, le texte prévoit à peine de nullité, que les actes autorisés ne peuvent constituer une incitation à commettre l'infraction (article 230-46 alinéa 6 du code de procédure pénale). Dans le cas où l'infraction a déjà été commise, il n'y a pas de réelle difficulté à faire usage de cette technique en ce qu'elle aura pour finalité essentielle de constater et récolter les preuves de celle-ci. En revanche, la situation dans laquelle l'infraction n'a pas encore été commise est plus délicate, puisque l'agent anonyme devra s'assurer que son intervention ne constitue pas une incitation à commettre l'infraction afin d'échapper à la nullité de l'acte d'investigations et de ses actes subséquents, ainsi qu'à l'irrecevabilité des preuves récoltées.

§2. La perquisition informatique

Consacrées pour la première fois par la Convention de Budapest, les perquisitions informatiques consistent en la saisie de données informatiques nécessaires à la manifestation de la vérité. Dans une société en perpétuelle numérisation, cette forme inédite de perquisition apparaît comme un outil précieux dans les enquêtes portant sur des infractions commises ou non sur un support informatique. En effet, la digitalisation de la société a conduit à l'inscription d'une masse conséquente d'informations dans des fichiers numériques stockées sur des supports informatiques. Dès lors, et comme en matière d'enquête de droit commun, la perquisition demeure la grande technique d'investigation incontournable.

[62] La loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance
[63] Avant cette loi, la mesure d'enquête sous pseudonyme était limitée à une liste d'infraction précise, dont la traite des humains, le proxénétisme ou encore la prostitution de mineurs
[64] Loi de programmation 2018-2022 et de réforme pour la justice du 23 mars 2019 (n°2019-222)

Contrairement à la perquisition ordinaire, la perquisition informatique ne fait pas intervenir la notion de "domicile", à laquelle est substituée la notion de "système informatique", assimilée à un lieu clos. En effet, l'article 57-1 du code de procédure pénale[65] permet à des officiers de police judiciaire, ou sous leur responsabilité, à des agents de police judiciaire, d'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*."[66]. Pour simplifier, il est permis aux enquêteurs d'accéder à la fois à des données stockées dans un système informatique se trouvant sur les lieux de la perquisition "classique" et à ceux pouvant être accessibles à distance à partir de ce même système initial[67]. Se faisant, la portée d'une perquisition informatique est très large, et permet également de recueillir des données stockées dans un autre système informatique situé en dehors du territoire national, sous réserve du respect des règles prévues par les engagements internationaux[68]. Dans pareil cas, l'article 32 de la Convention de Budapest doit être appliqué : soit une demande d'entraide pénale internationale est formulée, soit l'accès est permis à raison du caractère public des données ou du consentement légal et volontaire de la personne concernée. Lorsque les données stockées sur le système distant demeurent sur le territoire national, l'extension de la perquisition n'est pas réellement problématique. En revanche, lorsque ce système distant est situé à l'étranger, interviennent les difficultés tirées de la territorialité et de la souveraineté étatique. En effet, admettre une telle extension de compétence reviendrait à admettre la possibilité pour un agent français de perquisitionner en territoire étranger. Cette problématique, inhérente même à l'immatérialité de cette criminalité, peut constituer un réel frein aux enquêtes puisque l'alinéa 3 de l'article conditionne l'accès au respect des engagements internationaux en vigueur.

[65] Issu de la loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure
[66] Article 76-3 du code de procédure pénale pour l'enquête préliminaire
[67] Extension préconisée par l'article 19.2 de la Convention de Budapest
[68] Article 57-1 alinéa 3 du code de procédure pénale

Initialement, la doctrine interprétait littéralement et strictement le texte de l'article : *« Mutatis mutandis en pénétrant dans un domicile, l'OPJ ne pourrait circuler que dans les pièces dont les portes sont ouvertes ("accessibles depuis le système initial"), quant aux autres, dont les portes sont fermées ("inaccessibles depuis le système initial"), il lui serait fait défense d'utiliser les services d'un serrurier pour les ouvrir (outrepasser les paramètres d'accès du système distant).*"[69]. C'est pourquoi la doctrine hostile à cette ouverture et les avocats désireux de faire annuler une telle perquisition, soutenaient bien souvent l'existence d'une analogie entre serveur distant et domicile distinct du domicile perquisitionné.

Par une décision du 6 novembre 2013[70], la chambre criminelle de la Cour de cassation avait retenu le critère de l'accessibilité aux données afin de valider l'accès aux données sur un serveur distant se trouvant aux États-Unis, réfutant toute nécessité de recourir à une demande d'entraide pénale. Selon le demandeur au pourvoi, cela équivalait à accéder à un nouvel espace privé et clos grâce à une clé trouvée au domicile perquisitionné, nécessitant soit le consentement exprès de l'intéressé soit une autorisation du juge des libertés et de la détention[71]. Le pourvoi soutenait qu'en tout état de cause, à raison de l'extranéité du serveur et en l'absence de procédure d'entraide, l'autorisation du JLD aurait été prise en violation des règles de compétences territoriales. Par cette décision, en refusant d'assimiler l'accès aux données stockées sur un serveur distant à une nouvelle perquisition, la chambre criminelle avait pour objectif de contourner la lourdeur de l'entraide pénale internationale. Cette décision illustre bien le malaise engendré par cette difficulté inhérente aux serveurs informatiques, majoritairement domiciliés à l'étranger. Se faisant, la chambre criminelle a totalement évité la question de la souveraineté de l'État étranger dans sa motivation, en se contentant d'affirmer de façon péremptoire que l'accès aux données n'est qu'un simple acte d'investigation pris dans le cadre de la perquisition. Finalement, il semblerait qu'à la fois le texte législatif et la jurisprudence inviteraient à ignorer l'extranéité du système distant, afin de ne pas paralyser l'enquête.

---

[69] D. Bénichou, Cybercriminalité, jouer d'un nouvel espace sans frontière, AJ pénal 2005, 225

[70] Criminelle, 6 novembre 2013, n° 12-87.130, s'agissant de la pénétration et de la recherche de données sur un site internet hébergé sur un serveur américain, à l'aide d'un code d'accès personnel obtenu dans le cadre d'une perquisition

[71] En l'espèce, le code d'accès personnel au site - hébergé sur un serveur américain- avait été obtenu dans le cadre de la perquisition initiale

Section 2. Les nouvelles technologies : nouvel instrument de l'enquête pénal

L'un des plus grands paradoxes dans la lutte contre la cybercriminalité tient au fait que l'arme de l'infraction se transforme quand il s'agit d'enquêter, en outil de l'enquêteur. Comme le souligne le magistrat David Bénichou, "*c'est la main de l'Homme qui donne à l'outil sa destination*". Ainsi, ces nouvelles technologies au service du cybercriminel le sont également vis-à -vis du cyber enquêteur, les deux protagonistes se distinguant finalement par l'existence ou non d'un motif légitime. Consciente de la force d'arme que représentent ces outils, la loi LOPMI du 24 janvier 2023 a prévu une hausse du budget de 15 milliards d'euros sur les cinq prochaines années, destinée à l'investissement dans le numérique.

§1. Le recours aux autres techniques spéciales d'enquêtes

Le recours à des dispositifs techniques et à des appareils au cours des investigations n'avait pas été envisagé à l'origine pour répondre spécialement et uniquement à la cybercriminalité. À ce titre, les techniques spéciales d'enquêtes instituées dans le cadre de la lutte contre la criminalité et la délinquance organisée, avaient vocation à s'appliquer initialement à des infractions classiques énumérées par l'article 706-73 du Code de procédure pénale dès lors qu'elles étaient commises en bande organisée. De l'interception de correspondances électroniques à la captation de données informatiques, l'utilisation des technologies est aujourd'hui familière pour les enquêteurs. Face à une criminalité discrète et dont les preuves sont fugaces, l'usage des techniques spéciales d'enquête « *dont la force de frappe réside dans leur déploiement à l'insu des suspects et le plus rapidement possible* »[72] est plus que nécessaire.

[72] Lumière sur un arsenal de lutte contre une délinquance tapie dans l'ombre, AJ Pénal 2017 p 312 , Marc Touillier

A. L’accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique

L’une des innovations majeures portée par la loi du 3 juin 2016, consiste dans la possibilité ouverte aux enquêteurs, d'accéder à distance et à l’insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d’un identifiant numérique. Contrairement à la perquisition informatique, cette technique d’investigation permet l’appréhension à distance de données, et cela même sans détenir matériellement le système ou le support de ces données. Dès lors, l’enquêteur pourra accéder au contenu des messageries électroniques, lui ouvrant la voie vers un véritable nid à preuves. Toutefois, une difficulté pratique pour cette méthode d’investigation tient à la méthode de la double authentification - ou vérification en deux étapes- qui conditionne l’accès à une confirmation de l’utilisateur, qui prend généralement la forme d’un code provisoire reçu par message ou par e-mail.

B. Le recueil de données techniques de connexion

Vivement décriée, la loi du 3 juin 2016 a importé en droit français la légalité du recours à des IMSI catcher, c'est-à-dire à un dispositif de surveillance de masse afin d’intercepter toutes les conversations passées par des téléphones portables dans un secteur donné. En se faisant passer pour une antenne relais, le dispositif électronique va permettre la connexion de tous les appareils mobiles à proximité. Selon la capacité d’espionnage de l’outil, au-delà de l’interception des connexions mobiles, il pourra être possible également d’accéder à leur contenu ou encore au trafic Internet mobile. En plus de permettre la surveillance des suspects et la collecte de preuves, l’IMSI catcher permet également de localiser ces derniers lorsqu’ils utilisent des réseaux mobiles pour opérer. Toutefois, une difficulté inhérente à son utilisation tient au fait que la puissance de l’appareil entraîne une interception de masse non ciblée, ce qui entraîne également l’interception de données d’innocents.

Comme évoqué plus tôt, les enquêteurs et les cybercriminels se partagent malgré eux les mêmes outils numériques, et l'IMSI catcher - outil précieux de l'enquête - n'échappe pas à ce constat. Ainsi, en février 2023, la police judiciaire avait arrêté une équipe agissant en bande organisée qui utilisait l'IMSI catcher à des fins d'escroqueries par l'envoi de 424 000 messages téléphoniques frauduleux sur les appareils détectés par l'outil. Par le jeu de l'imprévisible, une technique d'espionnage utilisée notamment pour lutter contre la cybercriminalité s'est retrouvée être une technique redoutable pour commettre un hameçonnage massif. Tel est le paradoxe de la lutte opposant les cyber enquêteurs aux cybercriminels, où les outils des uns deviennent les outils des autres.

§2. L'utilisation de logiciels informatiques

Introduite par la loi LOPPSI du 14 mars 2011[73], la captation de données informatiques permet "*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 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*."[74]. Comme pour les autres méthodes intrusives, son champ d'application est restreint aux infractions listées aux articles 706-73 et 706-73-1 du code de procédure pénale, et permets aux enquêteurs en cas de nécessité, d'accéder à ces données protégées sans le consentement de l'intéressé et surtout par l'usage de logiciels malveillants.S'agissant des données affichées sur l'écran et introduites par saisie de caractères, les enquêteurs vont recourir au *keylogger*, qui est un logiciel espion enregistrant toutes les frappes de clavier passées sur un système d'exploitation, mémorisant ainsi les données entrées. Encore une fois, il s'agit d'un outil fréquemment utilisé par les cybercriminels afin d'accéder à des informations personnelles telles que des identifiants et des codes d'accès. Cette méthode est utile pour retracer ce qui a été recherché sur le système, ou pour avoir accès à des mots de passe ou des clés de chiffrements.

[73] Loi n 2011-267 du 14 mars 2011 « d'orientation et de performance pour la sécurité intérieure »
[74] Article 706-102-1 du code de procédure pénale

Depuis la loi du 3 juin 2016[75], le champ de cette technique d'investigation a été étendu à toutes les données reçues ou émises par des périphériques, c'est-à-dire toutes les données contenues dans des dispositifs connectées au système informatique tels qu'un disque dur, ou une clé USB. Pour ce faire, les enquêteurs vont avoir recours généralement à un programme, qualifié de Cheval de Troie informatique, en ce que de la même manière que les soldats grecs, il prend l'apparence d'un logiciel légitime avant de prendre le contrôle du système informatique où il est installé. En pratique, cette technique est tellement complexe qu'elle est rarement pratiquée.

Enfin, à la fois pour la récolte et la préservation de la preuve numérique, les enquêteurs dépendent grandement des entreprises privées spécialisées dans le forensic auprès desquelles sont achetés les dispositifs et logiciels d'investigations numériques. À titre d'exemple, le logiciel d'investigations Magnet Axiom - développé par l'entreprise Magnet Forensics- est largement utilisé à travers le monde afin de récupérer des données supprimées. Kit Forensic permet quant à lui de récupérer des mots de passe divers, y compris cryptés. Il existe également FTK Imager, un outil puissant d'analyse d'images et de données, qui permet de préserver l'intégrité originale de la preuve sans affecter son état d'origine. Sans vouloir procéder à une énumération exhaustive, ces quelques exemples tendent à démontrer qu'il existe une large diversité de logiciels et de supports informatiques *forensic*[76] proposant des fonctionnalités différentes qui font d'eux des outils incontournables pour l'enquête.

[75] 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

[76] Forensic -ou digital forensic - est le terme anglais se référant au domaine de l'investigation numérique

Section 3. La limite des droits fondamentaux

De même que pour la criminalité classique, la recherche et la poursuite d'auteurs d'une infraction cybercriminelle suppose le respect de droits fondamentaux, et ce à tous les stades de la procédure. Or, ces droits fondamentaux sont d'autant plus défiés dans le cadre de la lutte contre la cybercriminalité en ce que l'enquête exige par nature, le recours aux moyens d'investigations les plus attentatoires. Au-delà du cas isolé des suspects, les techniques spéciales d'enquête sont également susceptibles d'atteindre des personnes totalement étrangères aux faits, de sorte que leur liberté est également atteinte par ricochet. Ainsi, les autorités étatiques doivent constamment s'assurer de la conciliation entre la sauvegarde de l'ordre public et les droits en présence, en démontrant la nécessité et la proportionnalité de la mesure. À ce titre, le rapport "*Protéger les internautes*" préconisait une adaptation de la réponse pénale, "*sans pour autant créer un droit d'exception insupportable au regard des libertés fondamentales*" . C'est pourquoi, la Convention de Budapest appelait les États à garder 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*".

§1. L'atteinte au droit à la vie privée

Parmi les droits les plus défiés par les investigations numériques, se trouve le droit au respect de la vie privée, qui représente également un frein considérable, spécialement dans le cadre de la collecte de preuves. Aujourd'hui, la vie privée est largement dématérialisée ce qui explique qu'elle est également devenue d'autant plus sensible. Comme le soutient le Professeur Jean Christophe Saint Pau, le droit à la vie privée implique des droits dérivés que sont le domicile, l'image, les paroles, les correspondances, les traitements de données et les fichiers d'informations personnelles. Or, ce sont ces mêmes éléments qui sont visés par les pouvoirs d'investigations qui permettent de voir, d'entendre, de lire, et de situer par des moyens audiovisuel, informatiques, et électroniques. À titre d'exemple, s'agissant de l'accès aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique, le législateur ne prévoit aucune limitation dans le temps de la mesure alors même que la Cour Européenne des Droits de l'Homme apprécie l'ingérence dans la vie privée au regard de la durée de la mesure.

Par ailleurs, le respect du droit à la vie privée constitue souvent le motif de refus de coopération des opérateurs privés, qui usent de cette protection accordée en guise d'argument commercial alors même qu'ils sont les premiers à s'approprier les données de leur clientèle à des fins mercantiles. Ces derniers font alors souvent le choix stratégique de s'implanter dans des États où la législation ne contraint pas à la contribution à l'enquête pénale contrairement à la France.

Désormais, depuis la loi du 23 mars 2019, l'article 706-95-18 du code de procédure pénale prévoit s'agissant des techniques spéciales d'enquête, que "*aucune séquence relative à la vie privée étrangère aux infractions visées dans les ordonnances autorisant la mesure ne peut être conservée dans le dossier de la procédure.*".

§2. L'atteinte au principe d'égalité

Dans le cadre de ces méthodes d'investigations intrusives se pose la question de savoir si la complexité de cette criminalité justifie en soit une différence de traitement des suspects, qui par principe sont égaux devant la loi. Bien qu'une différence de traitement avec les suspects de crimes de droit commun puisse se justifier par la nature grave et urgente de la cybercriminalité, une telle différence de traitement vis-à-vis des règles de la délinquance organisée - dérogatoires par nature - interroge quant à elle. Cette atteinte se vérifie principalement en termes d'enquête sous pseudonyme, qui comme le souligne le Maître Gabriel Dumesnil[77], n'est que quelque peu entourée de garanties pour la personne visée. Premièrement, avant la réforme issue de la loi du 23 mars 2019, et contrairement à la mesure d'infiltration, aucune autorisation préalable d'un magistrat n'était requise. Malgré la réforme, la participation à des échanges électroniques est toujours rendue possible sans autorisation préalable d'un magistrat, mais est soumise désormais au contrôle du procureur de la République. De plus, aucune motivation n'est requise pour recourir à cette technique, alors même que le texte impose une exigence de nécessité de la mesure. Enfin, l'enquête sous pseudonyme est nullement soumise par le texte à une limitation temporelle, alors que la mesure est d'autant plus attentatoire au respect de la vie privée, et que toutes les mesures d'enquêtes dérogatoires sont encadrées dans le temps.

[77] Droit pénal n° 9, Septembre 2018, étude 22 par Gabriel Dumenil "La nécessité urgente d'encadrer procéduralement la mesure de cyber-infiltration".

Cette problématique se retrouve également en matière de perquisition informatique, dont l'étendue considérable n'emporte pas le renforcement des libertés garanties par le régime des perquisitions classiques. Ainsi, le texte de loi permet d'accéder à des données stockées dans un système distant, accessibles depuis le système initial, sans requérir une autorisation du JLD ou de la personne perquisitionnée. Il apparaît donc que le régime des investigations numériques est doublement dérogatoire en ce qu'il ne s'accompagne pas toujours des garanties, déjà limitées, prévues pour la délinquance organisée.

§3. L'atteinte à la liberté de communication

Instituée à l'article premier de la loi Léotard du 30 septembre 1986, et reprise au même rang par la loi pour la confiance dans l'économie numérique du 21 juin 2004, la liberté de communication par voie électronique est très souvent invoquée par les pourfendeurs de la régulation d'Internet. Cette liberté, découlant de l'accession de la liberté d'expression au cyberespace, ne peut être limitée que dans les cas limitatifs prévus au troisième alinéa de ce même article parmi lesquels figure l'exigence de sauvegarde de l'ordre public. C'est notamment sur le fondement de cette exception qu'ont pu être justifiées des actions en régulation d'Internet destinées à garantir la licéité de son contenu.

En sus de cette régulation préventive, s'ajoutent les hypothèses de violation de cette liberté lors des enquêtes pénales fondées sur la lutte contre la cybercriminalité. Cette difficulté s'observe particulièrement dans le cadre des enquêtes sous pseudonymes dès lors que ces dernières permettent l'intrusion du contrôle étatique dans les communications électroniques, et ce à l'insu des concernés. De même pour la mesure d'interception des communications électroniques, qui porte par nature atteinte à la confidentialité des communications. Enfin, s'agissant de l'accès aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique, le législateur ne précise nullement la nature des correspondances pouvant être saisies, offrant alors une large marge de main d'oeuvre aux agents étatiques (article 706-95-1 du code de procédure pénale). Ces mesures aux garanties restreintes témoignent de l'équilibre délicat entre la sécurité nationale et la liberté de communication, dont l'exercice abusif est d'autant plus facilité par l'effet d'Internet.

CONCLUSION DE LA SECONDE PARTIE

La procédure pénale, anciennement désarmée face à ce nouveau phénomène, a su prendre appui sur sa panoplie traditionnelle ainsi que sur les nouvelles technologies pour résoudre les difficultés inhérentes à la cybercriminalité. En sus de ces moyens matériels, la France s'est dotée de réels moyens humains par la formation des forces de l'ordre et l'intégration d'experts informatiques, essentielle à l'efficacité des enquêtes. La spécialisation des acteurs de l'enquête pénale prend progressivement carrure, et s'accompagne progressivement d'une spécialisation complémentaire du corps judiciaire, tout autant essentielle. Alors que la section cyber du parquet de Paris - instituée en 2014 - était composée de seulement 2 représentantes du Ministère public en 2018, son effectif s'est renforcé et compte aujourd'hui 5 magistrats et une juriste assistante. L'arsenal de lutte contre la cybercriminalité ne cesse de s'enrichir, facilitant ainsi la détection et la collecte des preuves numériques, et ce parfois aux dépens des droits et libertés.

Cependant, face à une criminalité en constante évolution, il serait contre productif de se reposer sur ces acquis au risque de rétablir le constat de la désuétude de la procédure pénale. Les connaissances des forces de l'ordre, les outils législatifs et opérationnels doivent de ce fait être constamment mis à jour. C'est pourquoi, en sus de de cette adaptation amorcée, les autorités étatiques auraient tout intérêt à également anticiper les futures évolutions de la technologie, et de son utilisation potentielle par les cybercriminels, pour maintenir l'efficacité de l'enquête pénale.

CONCLUSION GÉNÉRALE

Le constat anciennement défaitiste de l'impuissance des États face à cette nouvelle forme inédite de criminalité est aujourd'hui dépassé. En effet, la France est parvenue à piocher dans ses réserves, en ayant recours à la fois aux incriminations classiques et aux moyens d'investigations existants pour pallier certaines difficultés nouvelles liées à la cybercriminalité. De surcroît, est en train de se développer un nouvel arsenal répressif contre la cybercriminalité composé d'un outillage technique révolutionnaire manié par une armée formée. Toutefois, face à cette criminalité transnationale menaçant l'équilibre institutionnel et financier des souverainetés étatiques, la problématique de l'auto insuffisance des États persiste, et appelle à une consolidation de la coopération internationale qui demeure lacunaire.

Par une approche prospective, la genèse de l'intelligence artificielle - fruit du paroxysme de l'innovation technologique - interroge sur l'avenir de la cybercriminalité. L'intelligence artificielle désigne le processus technique par lequel une technologie simule l'intelligence humaine à travers l'exécution d'algorithmes imitant les fonctions cognitives du cerveau. Les fonctionnalités de cette nouvelle discipline émerveillent autant qu'elles effraient, nourrissant la crainte que le slogan "*par l'homme et pour l'homme*" ne se convertisse en "*par l'homme et contre l'homme*". S'agissant particulièrement de son caractère criminogène, il est tout à fait clairvoyant d'appréhender l'appropriation de cette technologie par les cybercriminels, toujours à jour des innovations[78]. Pour autant, selon un expert de cyber malveillance.gouv.fr, "*si l'intelligence artificielle peut améliorer la productivité des cybercriminels et la sophistication de leurs modes opératoires, ceux-ci resteront sans doute, du moins encore un temps, très similaires dans leurs principes*"[79].

[78] Ainsi, dernièrement, l'usage de l'IA le plus dénoncé et recensé à l'international est celui du *deepfake* - hyper trucage en français-, qui consiste à créer des vidéos et audios falsifiés en récréant la voix et le physique de réel individus. Cette technologie permet alors de faire faire, et faire dire à n'importe qui, n'importe quoi. Son utilisation récente la plus fréquente visait à détourner l'image et la voix de personnalités publiques, telles que des célébrités afin de mener une escroquerie, ou encore de personnalités politiques afin de diffuser des informations mensongères dans le but de manipuler ou de tromper le public.

[79] L'intelligence artificielle (IA), entre menaces et opportunités, article paru le 6 mai 2024 sur cybermalveillance.gouv.fr

L'avènement de l'intelligence artificielle ne devrait donc pas, théoriquement, conduire à une réformation de l'arsenal répressif développé ces dernières années, dont la simple adaptation sera nécessaire. En revanche, tandis que la cybercriminalité *ante* intelligence artificielle était concentrée dans les mains d'individus maîtrisant les codes du monde virtuel, l'intelligence artificielle a pour redoutable conséquence de rendre cette criminalité accessible à des individus dotés de faibles compétences techniques. Dès lors, ce qui est à craindre ce n'est pas tant une révolution de la cybercriminalité mais une intensification de son étendue, avec d'une part une prolifération du nombre d'auteurs, et d'autre part une amélioration des performances criminelles, augmentant de façon causale et significative le nombre de cyberattaques.

BIBLIOGRAPHIE

REVUES ET ARTICLES

Sarah-Marie CABON, *Atteintes aux systèmes de traitement automatisé de données - L'influence du cyberespace sur la criminalité économique et financière* - Droit pénal n°3, Mars 2018

David Benichou, *Cybercriminalité : jouer d'un nouvel espace sans frontière* - AJ Pénal 2005 p 224

Christiane Féral-Schuhl, *Une procédure pénale adaptée à l'internet se dessine : entre « cyber-enquêteurs » et collaboration des fournisseurs et utilisateurs* - AJ Pénal 2005 p228

Éric Freyssinet, *Les données sont-elles devenues le premier enjeu de la cybercriminalité ?* - Annales des Mines - Réalités industrielles 2022/3 (Août 2022), pages 84 à 87

Pierre Berthelet, *Aperçus de la lutte contre la cybercriminalité dans l'Union européenne* - Revue de science criminelle et de droit pénal comparé 2018/1 (N° 1), pages 59 à 74

Myriam Quéméner, *Pour une lutte plus efficace contre la cybercriminalité* - Sécurité globale 2018/3 (N° 15), pages 5 à 16

Marc Touillier, *Lumière sur un arsenal de lutte contre une délinquance tapis dans l'ombre* - AJ Pénal 2017 p 312

Olivier Décima, *Du piratage informatique aux perquisitions et saisies numériques ?* - AJ Pénal 2017 p315

Jean-Christophe Saint-Pau, *Les investigations numériques et le droit au respect de la vie privée* - AJ Pénal 2017 p 321

Olivier Violeau, *Les techniques d'investigations numériques : entre insécurité juridique et limites pratiques* - AJ Pénal 2017 p324

Alexandre Rousselet-Magri, *Les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données* - Revue de science criminelle et de droit pénal comparé 2017/4 (N° 4), pages 659 à 676

Etienne Vergès, *La preuve numérique, entre continuité et changement de paradigme* - Justice Actualités n°21, Juin 2019

Pauline Türk, *La souveraineté des États à l'épreuve d'Internet* - RDP 2013, p. 1489, n° 6.

Imbert-Quaretta, *La plateforme nationale des interceptions judiciaires*, AJ pénal 2017. 318

Gabriel Dumenil, *La nécessité urgente d'encadrer procéduralement la mesure de cyber infiltration* - Droit pénal n°9 2018 p 10-14

Agathe Lepage, *La distinction entre provocation à la preuve et provocation à la commission d'une infraction à l'épreuve d'Internet* - Communication commerce électronique 2014, commentaire 73

Marc Robert, *Cybercriminalité : les nouvelles réponses législatives* - AJ Pénal, 2016 p.412

Sophie Sontag Koenig, *Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel* - AJ Pénal, 2016, p.238.

Frédérick Douzet, *La géopolitique pour comprendre le cyberespace* - Hérodote 2014/1-2 (n° 152-153)

Brigitte Pereira, *La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité* - Revue internationale de droit économique 2016/3 (t. XXX), pages 387 à 409

Alix Desforges, *La coopération internationale et bilatérale en matière de cybersécurité: enjeux et rivalités,* Laboratoire de l'IRSEM n°16 2013

Jean-François Renucci, *Loyauté des preuves et distinction entre « provocation à l'infraction » et « provocation à la preuve »,* Revue de science criminelle et de droit pénal comparé 2014/4 (N° 4), pages 843 à 847

RAPPORTS ET PROPOSITIONS

Rapport du CECyF et Cyberlex, La procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique : proposition pour une efficacité juridique renforcée, 24 janvier 2018

Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Rapport sur la cybercriminalité « Protéger les internautes »* , Février 2014

Proposition de résolution au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur la lutte contre la cybercriminalité, *Cybercriminalité : un défi à relever aux niveaux national et européen* - Rapport d'information n° 613 (2019-2020), déposé le 9 juillet 2020

Groupe de travail du club des juristes présidé par Bernard Spitz, *« Le droit pénal à l'épreuve des cyberattaques »* - mars 2021

TEXTES INTERNATIONAUX

Convention de Budapest sur la cybercriminalité, 23 novembre 2001

Rapport explicatif de la Convention sur la cybercriminalité, 23 juin 2001

Premier protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003

Second protocole additionnel à la Convention de Budapest relatif au renforcement de la coopération et de la divulgation de preuves électroniques, 17 novembre 2021

THÈSE

Jean-Nicolas Robin, *La matière pénale à l'épreuve du numérique* 2017

TABLE DES MATIÈRES

PARTIE 2. LA CONSTRUCTION D'UN ARSENAL PÉNAL DE LUTTE CONTRE LA CYBERCRIMINALITÉ