**Année académique 2020/2021**

**Master 2 Droit pénal international et européen**

*Mémoire de stage*

---

# *La preuve numérique à l'épreuve de la cybercriminalité*

**Par** : Mahougnon Franc KAI

**Sous la supervision de** :

- Monsieur Baptiste NICAUD, Enseignant référent
- Monsieur François TESSIER, Tuteur de stage au Parquet de la Cour d'Appel de Limoges
- Madame Alexia DUDOGNON, Tutrice de stage à la DTPJ de Limoges

# Remerciement

Je tiens à adresser ces quelques mots de remerciements à des personnes sans lesquelles ce travail serait une dure épreuve. Il s'agit de :

- Monsieur François TESSIER, substitut au procureur et secrétaire général du parquet de la Cour d'Appel de Limoges, et de l'équipe de juristes assistants (Julien MIALLON, Justine DELRIEU, Gabrielle GOULET, Kévin BIHANNIC, Clara CORDIER), pour m'avoir très bien accueilli, fait découvrir la cour et son fonctionnement, et m'avoir donné quelques orientations fructueuses sur mon thème.
- Madame Alexia DUDIGNON, actuelle directrice adjointe de la DTPJ de Limoges ainsi que toute son équipe, notamment Catherine NONCLERCQ, Isabelle MALEYRAT-BEY, Olivier et Cyrille, Gilles-Etienne, pour m'avoir bien accueilli dans leurs locaux, planifié, exécuté, enrichi et coordonné le déroulement de mon stage.
- Monsieur Rémy MARCILLAUD, Chef de la Brigade mobile de recherche, avec son équipe pour m'avoir fait découvrir leur unité et donné quelques formations en matière de fraude documentaire
- Monsieur Christophe Roland, Commandant de la section de recherche de Limoges, pour son accueil et pour m'avoir permis d'assister à la recherche de cadavre.
- Monsieur Marc PETER, Chef du groupe interministériel de recherche Limousin, avec son adjointe, madame DOMINIGUEZ Laure, pour leur accueil et pour m'avoir permis d'assister à une perquisition domiciliaire
- Monsieur Christophe MORMINA, actuel chef de la division des douanes, et toute son équipe pour leur accueil et sympathie, et pour avoir nourri ma curiosité sur les réelles missions des services de douane.
- Monsieur Mohammed ED DARDI, actuel directeur de la maison d'arrêt de Limoges, pour m'avoir accueilli pour un stage de découverte de cinq jours au sein de ladite maison.
- Ma famille pour s'être montrée toujours un soutien infaillible à mon égard depuis mon enfance.
- Ma compagne, Firmine GNANGNON, pour son soutien quotidien.

Evidemment, je tiens particulièrement à remercier monsieur Baptiste NICAUD pour m'avoir permis de vivre ces expériences, été d'une source de référence importante pour l'organisation de ces travaux et pour avoir compris et soutenu notre promotion qui traversé des saisons éprouvantes à cause de la crise sanitaire.

## Les abréviations principales

- Adresse IP *:* Internet Protocol
- CPP Code de procédure pénale
- CP Code pénal
- CEDH Cour Européenne des Droits de l'Homme
- La Convention. Convention de Budapest du 23 novembre 2001
- C-NTECH Correspondant en investigation numérique
- DTPJ Direction territoriale de la Police judiciaire ou la Police judiciaire
- DOS Disk operating system
- ICANN International Corporation for Assignated Names and Numbers
- ICC Investigateurs en cybercriminalité
- JLD Juge des libertés et de la détention
- LOPPSI *2* Loi d'orientation et de programmation pour la performance de la Sécurité intérieure 2
- MLAT Traité d'assistance judiciaire mutuelle (Mutuel legal assistance treaty)
- NTECH Enquêteurs en nouvelle technologie
- OCLCTIC Office central de la lutte contre les atteintes aux technologies de L'information et de la communication
- OPJ Officier de Police Judiciaire
- SDLC Sous-direction de la lutte contre la cybercriminalité
- STAD Système de traitement automatisé de données
- TFUE Traité pour le fonctionnement de l'UE
- TIC Technologie de l'information et des communications
- UE Union Européenne.

# Table des matières

# Introduction

Le passage de l'analogique au numérique a provoqué un nouvel âge de la technologie dont les conséquences juridiques, multiples, ne laissent pas indifférentes sur la question de la procédure pénale notamment celle de la preuve pénale numérique, qui reste à nos jours un enjeu crucial en matière de lutte contre la cybercriminalité. A en croire Josef Moser, ministre autrichien, « Les preuves numériques deviennent un élément crucial des procédures pénales. Aujourd'hui, les délinquants recourent à des technologies de pointe rapides qui ne s'arrêtent pas aux frontières... »[1]. Raison peut être accordée à cette pensée de l'auteur lorsqu'on observe aujourd'hui les difficultés que provoquent la fraude informatique au Pass sanitaire, lesquelles exigent de la part des services d'enquête judiciaire une infaillibilité dans la traçabilité, la constitution des éléments de fraude et l'identification univoque des auteurs.

La question soulevée par la preuve pénale numérique dans le cyberespace tient principalement à sa constitution, sa fiabilité plutôt qu'à sa légalité. C'est pourquoi, pour emprunter les termes d'Etienne Verges, l'on s'intéresse à l'épineuse problématique de savoir si la réunion de la preuve numérique a pu bouleverser la physionomie du droit de la preuve et la pratique juridictionnelle ? [2]

Mes stages effectués consécutivement à la Direction Territoriale de la Police Judiciaire et au parquet général de la Cour d'Appel de Limoges, dans le cadre de mon master 2 droit pénal international et européen, m'ont permis d'étudier plusieurs facettes de la question. Le choix de ces deux organismes se justifie notamment au regard de la mission principale qui est la leur à savoir : réunir les preuves d'une infraction, rechercher le ou les auteurs et complices, et exercer, le cas échéant, l'action publique.

***La Police judiciaire***

Créée en 1907 par Georges Clemenceau alors Président du Conseil et ministre de l'intérieur, la Police Judiciaire jadis connue sous le nom de brigade mobile ou brigades du « Tigre »[3] était en effet conçue comme le seul véritable apanage susceptible de faire face à une période gangrénée par une sulfureuse délinquance, laquelle, transgressant toutes les valeurs tant chères à l'ordre républicain français, n'avait de limite que l'impuissance de ces hommes qui en étaient les promoteurs[4]. Ce dispositif, à la différence de la police locale dont les pouvoirs furent limités à une délinquance zonale, a été doté pendant cette période de turbulence d'une

[1] Communiqué de presse du 7 décembre 2018, Conseil de l'UE, https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

[2] Le traitement de la preuve numérique dans les procédures judiciaires civiles et pénales, Etienne VERGES, justice actualité n°21, 2019, p1

[3] Cette appellation renvoie au pseudonyme de monsieur G. Clemenceau

[4] Histoire de la police judiciaire, 10 octobre 2011, https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Histoire-de-la-police-judiciaire

compétence étendue à l'ensemble du territoire avec à l'appui, d'importants matériels pour contenir et éradiquer l'ampleur des actes criminels[5].

Aujourd'hui, d'un point vue organisationnel, la Police judiciaire (PJ) relève du ministère de l'Intérieur, représenté au plan national par la Direction Générale de la Police Nationale, de laquelle relève la Direction Centrale de la PJ. Cette dernière a sous sa responsabilité les Directions Zonales dont celle de Bordeaux Sud-Ouest, qui chapeaute la Direction Territoriale de la PJ de Limoges, actuellement dirigé par Monsieur Anthony DE FREIAS MEIRA assistée de Madame Alexia DUDOGNON. Ayant sur ses épaules le Service Régional de la Police Judicaire de Poitiers, la compétence de cette Direction couvre la région de la Nouvelle-Aquitaine (née de la fusion des anciennes régions Aquitaines, Limousin et Poitou-Charentes). Ce dispositif a été doté au fil du temps et de l'évolution de la criminalité dans cette région d'un ensemble de services, lesquels interviennent selon leur domaine et leur mission afin de réunir tout élément de preuve susceptible de concourir à l'établissement de la vérité dans le cadre d'une procédure judiciaire. Ainsi, par exemple, pour enquêter sur la cybercriminalité, la PJ de Limoges est composée d'une diversité de services techniques (le service en charge de la criminalistique numérique, un ICC, un NTECH), des acteurs du renseignement (Service d'Information, de Renseignement et d'Analyse Stratégique de la Criminalité Organisée), des services partenaires de la gendarmerie, des personnes qualifiées et aussi des acteurs relevant des coopérations internationales.

***Le parquet général de la Cour d'appel***

Le Parquet de la Cour d'Appel, quant à lui, est l'organe chargé de conduire au second degré juridictionnel l'action publique. Il est également compétent pour connaitre de certaines actions transversales à savoir par exemple : étudier au plan local l'impact de la politique pénale du gouvernement sur la justice de proximité, régler les problèmes liés au refus de désignation d'avocat au profit des bénéficiaires de l'aide juridictionnelle, etc. Le parquet général de la Cour d'Appel de Limoges est actuellement dirigé par Madame le Procureur Générale Anne KOSTOMAROFF, assistée d'un Secrétaire Général en la personne de Monsieur François TESSIER, d'une équipe d'Avocats et Substituts généraux, de magistrats placés, de juristes assistants et d'un assistant de justice.

Outre sa casquette de Secrétaire général et Substitut, Monsieur TESSIER est aussi un référent cyber. En effet, depuis 2019, il existe dans le ressort de chaque Cour d'appel un référent cyber. Celui-ci est un magistrat qui est formé à la théorie générale de la cybercriminalité[6]. Contrairement aux magistrats de la section J3 du parquet de Paris et à ceux du pôle d'instruction du tribunal de Paris, les référents cybers des parquets locaux et interrégionaux ne sont pas spécialisés dans ce domaine. Toutefois, leur connaissance générale de la matière leur permet d'aider leur juridiction respective à traiter des dossiers de cybercriminalité de moindre ampleur. Aussi assistent-ils à des réunions de cybers référents organisées périodiquement afin d'être au courant des affaires cybercriminelles importantes, des

[5] Ibid.
[6] Cybercriminalité : un défi à relever au niveau national et européen, site de la Sénat, http://www.senat.fr/rap/r19-613/r19-6134.html

enjeux qu'elles posent pour le droit pénal et les nouvelles politiques prises pour les contrecarrer.

***La cybercriminalité***

La cybercriminalité n'a pas reçu une définition unanime tant à l'échelle nationale qu'internationale. Ce défaut de consensus sur la notion serait en effet à l'origine d'une kyrielle de définitions proposées de toute part par les Etats et les organisations internationales officielles, lesquelles confrontent plusieurs intérêts et systèmes. Classiquement, lesdites définitions limitent la cybercriminalité au modus operandi des cybers-délinquants ou à l'objet de l'infraction. C'est le cas entre autres de la définition élaborée par l'Organisation de Coopération et de Développement Economique (OCDE) qui, faisant allusion au traitement ou à la sécurité des données, conçoit la cybercriminalité comme « *tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne le traitement automatique de données et/ou de transmission de données* »[7]. Au même titre, l'Organisation des Nations Unies limite aussi la cybercriminalité aux atteintes à la sécurité des systèmes informatiques[8]. D'autres définitions, notamment celles des Etats-Unis et du Royaume-Uni se limitent uniquement à l'accès frauduleux d'un système informatique, ce qui exclut indubitablement une partie importante du spectre infractionnel de la cybercriminalité à savoir, toutes les infractions qui peuvent être commises via un système[9].

En France, la cybercriminalité n'a pas été définie ni dans le Code pénal ni dans aucun autre texte, même si dans le Code de procédure pénale a été mentionné de bout en bout ce terme, notamment au niveau de certaines dispositions relatives à la coopération policière et judiciaire de l'Union[10]. Cependant, le 30 juin 2014, une ébauche de définition a été élaborée dans un rapport sur la cybercriminalité rédigé conjointement par le Procureur Général près la Cour d'Appel de Riom, Monsieur Marc Robert, et les Ministres Bernard Cazeneuve, Christiane Taubira et Axelle Lemaire. Ce rapport précise que « *la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen de système d'information et de communication, principalement Internet*[11] *»*[12]. Comme il peut être observé, la définition produite par ce rapport a l'écueil d'être hiérarchisant, en ce sens qu'elle conçoit la cybercriminalité comme une criminalité commise via Internet ; pour autant, la cybercriminalité n'a pas fait son apparition avec Internet. Ce choix définitionnel du rapport pourrait néanmoins être compréhensible d'un point de vue statistique. En effet, selon un rapport annuel de la société

[7] « Protéger les internautes », rapport sur la cybercriminalité, groupe interministériel sur la lutte contre la cybercriminalité, février 2014, p.11
[8] Ibid.
[9] Ibid.
[10] Article 694-32-11° du Code de procédure pénale, Article 695-8-2-i du CPP, Article 695-23 du CPP et S.
[11] Internet, avec un « I », est un réseau informatique mondial accessible au public, à communication de paquets, sans centre névralgique, composé de millions de réseaux aussi bien publics que privés, universitaire, commerciaux et gouvernementaux, eux-mêmes regroupés en réseaux autonomes ». Il puise son origine dans Arpanet, qui est l'acronyme du premier réseau transfert de paquets de données conçu aux USA en 1969 par DARPA (Defense Advenced Research Project Agency). ; initiation au fonctionnement de l'Internet et aux enjeux de la gouvernance Internet, l'OCLCTIC, DACG, juin 2021
[12] « Protéger les internautes », rapport sur la cybercriminalité, groupe interministériel sur la lutte contre la cybercriminalité, février 2014, P.12

de sécurité informatique Symantec[13], le taux d'activité malveillante sur Internet est estimé à 71%[14], ce qui confirme le rôle principal joué par Internet dans la cybercriminalité.

Quoiqu'il en soit, la cybercriminalité est une notion protéiforme qui s'analyse généralement sous deux acceptions[15]. Littéralement composée de deux mots, « cyber » qui vient du latin « ***kubernan*** », c'est-à-dire gouverner ou piloter, et de « criminalité » qui constitue l'ensemble des actes criminels commis à une période donnée dans une société, la cybercriminalité, au sens strict, englobe la cyberattaque, laquelle correspondant aux atteintes aux systèmes de traitement automatique de données grâce aux virus ou malwares. Cette forme de criminalité réprimée au niveau des articles 323-1 et suivants du CP sous l'angle de piratage, cible en effet les ordinateurs, les téléphones, les serveurs reliés à Internet, les équipements périphériques comme les imprimantes, etc. La cyberattaque se manifeste sous plusieurs formes, lesquelles sont généralement connu sous une appellation anglaise : le *phishing*[16] ou hameçonnage, le *pharming*[17], le *jackpoting*[18], le *sniffing*[19], etc.

Ensuite, au sens large, la cybercriminalité regroupe certaines infractions classiques du droit commun avec la circonstance qu'elles sont commises via les réseaux de communication en ligne. Certains auteurs conçoivent ce type de criminalité comme les « *infractions commises dans l'environnement numérique*" » (Féral-Schuhl, 2010). A ce titre, il peut s'agir de la E-escroquerie, de la haine ou la discrimination en ligne, le cyber-harcèlement, la pédopornographie en ligne, etc. Statiquement, c'est la forme de cybercriminalité la plus répandue.

Réprimée pour la première fois en 1971[20], la cybercriminalité a connu une recrudescence assez inquiétante à partir de 2000, période marquée par la création du réseau Internet, lequel a permis la propagation de programmes malveillants tels que les virus « *I love you* », « *Joke* »[21], l'augmentation du nombre de prédateurs financiers et sexuels, de cyber espions et des logiciels de piratage ou *rançongiciels* [22] dont les plus récents sont *Egregor*[23] , *Lockergoga*[24], *Petya*[25] et *Wannacry*. D'ailleurs, cette question de rançongiciel a été récemment

[13] http://www.symantec.com/fr/fr/business/theme.jsp?themeid=threatreport
[14] Sécurité et stratégie, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », Myriam Quéméner, cairn, 2011, P.59, https://www.cairn.info/revue-securite-et-strategie-2011-1-page-56.htm#re12no12
[15] *Ibid. P.56*
[16] C'est une technique qui consiste à envoyer des mails en trompant le destinataire du message afin que celui-ci divulgue des informations personnelles, visite un faux site afin de qu'il fournisse des données ou qu'un logiciel malveillant s'installe à son insu sur son ordinateur.
[17] https://fr.wikipedia.org/wiki/Pharming
[18] Ce mode opératoire, réalisé surtout par des groupes originaires de l'Europe de l'Est, consiste à démonter une partie d'un distributeur automatique de billet pour y introduire un virus informatique qui générera gratuitement le retrait des billets de banques
[19] C'est une technique de piratage qui consiste à introduire dans un serveur un programme informatique spécifique qualifié de « renifleur », lequel va capturer des données
[20] D'où vient la cybercriminalité ? : Origines et évolution. | Le VPN (le-vpn.com)
[21] « La fraude informatique », Abdoulaye Salifou, 2016, P2
[22] Ibid.
[23]https://www.leparisien.fr/high-tech/cybersecurite-enquete-sur-le-rancongiciel-egregor-cauchemar-absolu-des-entreprises-02-12-2020-8411844.php
[24]https://www.cyberveille-sante.gouv.fr/cyberveille/1166-le-ransomware-lockergoga-identifie-lors-dune-attaque-contre-altran-2019-02-01
[25] https://fr.wikipedia.org/wiki/Petya

au cœur d'un bras de fer politique entre les Etats unis et la Russie à la suite de l'attaque informatique d'un géant réseau d'oléoduc situé sur le *Colonal Pipeline* aux USA, attaque qui a empêché l'approvisionnement en essence et une hausse du prix du carburant. L'administration Biden a ainsi soupçonnée la Russie d'être instigatrice de cette attaque informatique. Également en France, entre le 8 et le 15 février 2021, dans un contexte tendu de crise sanitaire, les hôpitaux de Dax et de Villefranche-sur-Saône, ont été victimes d'une attaque informatique sur leur réseau. Cela a paralysé l'ensemble de leurs appareils, empêchant la prise en charge des patients. Toutes ces situations semblent en effet donner crédit aux prédictions contenues dans le livre blanc sur la sécurité et la défense nationale de 2008, qui annonçaient que « *dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur* ». La doctrine qualifie cette situation de « *cyberguerre* »[26].

***La preuve pénale numérique***

La preuve s'entend de la démonstration de la réalité d'un fait ou d'un droit. La doctrine la conçoit comme « *ce qui persuade l'esprit d'une vérité* »[27]. Elle est présente dans toutes les matières juridiques, y compris le droit pénal où elle consiste précisément à établir la constitution d'une infraction et à rechercher l'auteur. A la différence du droit civil qui inscrit la constitution de la preuve dans un ensemble d'obligations légales et contractuelles[28], le droit pénal consacre à travers l'article 427 du code de procédure pénale une liberté relative de la production de la preuve, c'est à dire que la preuve d'un fait ou d'un droit, en matière pénale, "*peut être apportée par tout moyen, sans qu'une preuve ne prévale sur l'autre ou que le juge ne soit lié à l'une plutôt qu'à l'autre*"[29]. C'est pourquoi l'on découvre dans l'histoire du droit pénal plusieurs modes de preuve variant des preuves rationnelles (l'aveu, le témoignage et l'écrit) aux preuves irrationnelles, lesquelles ayant été largement pratiquées dans les anciennes sociétés dans le cadre de la justice sacrée, ont fini par disparaitre. Il s'agit en l'occurrence du duel judiciaire et des ordalies[30]. Aujourd'hui, avec le marché du numérique, est apparue une nouvelle forme de preuve, la preuve dite numérique.

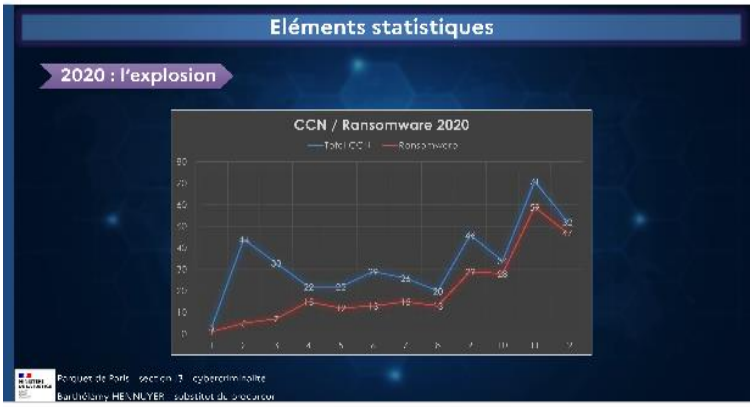
***L'enjeu de la preuve pénale numérique en matière de cybercriminalité***

La révolution technologique marquée par la montée en puissance des nouvelles technologies d'informations et de communications a favorisé le passage de l'analogique au numérique ainsi que la démocratisation de l'Internet. Ainsi, a-t-on observé la possibilité pour chaque individu, internaute en l'occurrence, de se connecter à titre personnel sur le réseau Internet. Cela a rendu facile la communication, la commercialisation, etc[31]. De sorte que l'être humain est aujourd'hui devenu ultra dépendant du numérique. En 2011, on dénombre plus de

[26] Cf. note de bas de page 11, P.60
[27] J. Domat, "Les lois civiles dans leur ordre naturel", Paris, éd. Cavelier, t.1, 1771, p. 204.
[28] Article 9 du code de procédure civile
[29] La preuve pénale, Grunvald S. et Danet J., UNJF
[30] Une forme de justice moyenâgeuse qui consiste à soumettre une personne accusée d'un crime à une épreuve douloureuse dans dont seul un dieu peut l'aider à réussir si elle était innocente.
[31] « la preuve numérique, un défi pour l'enquête criminelle au 21e siècle », Eric Ok, https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

deux (02) milliards d'individus utilisateurs d'Internet[32]. Selon le Secrétaire Général d'INTERPOL, M. Jürgen Stock, ce nombre s'est aujourd'hui accru pour atteindre les 4,5 milliards d'utilisateurs, à cause de la pandémie de Covid19 qui a contraint au télétravail et au commerce électronique et la communication à distance[33]. C'est-à-dire que, le numérique fait indéniablement aujourd'hui partie intégrante de la vie de l'*Homo numericus,* car grâce à lui, il est capable de presque tout faire (commercer, divertir, travailler, enregistrer son mémoire, communiquer, s'informer, acheter, faire des rencontres, se déplacer...).

Toutefois, cette dépendance ou corrélation humain-internet, bien que favorisant l'activité humaine, aura des conséquences négatives tant à l'égard de l'économie mondiales qu'à la vie privée et professionnelle des usagers de ce réseau, car elle causera l'explosion du taux de la cybercriminalité. Selon Symantec, la cybercriminalité coûte chaque année, en termes de préjudice mondial, environ 82,8 milliards d'euros, soit près de dix (10) fois plus que le cout des Jeux Olympiques de 2012 à Londres. Cette somme a augmenté de façon astronomique en 2008 (environ 1000 milliards de dollars) selon une étude de la société informatique McAfee[34]. Avec la crise sanitaire depuis fin 2019, l'activité des rançongiciels n'a cessé d'augmenter portant ainsi la barre des préjudices à un niveau plus critique.




Graphique tiré d'une étude du ministère de l'Intérieur

Cependant, la justice pénale tirera avantage de cette révolution technologique et, à l'instar des empreintes papillaires ou d'ADN utilisées dans le cadre de la criminalistique conventionnelle, les traces numériques laissées par les cybercriminels pourront aider à retrouver les auteurs et reconstituer éventuellement les actes. D'où l'utilité de la preuve numérique dans le cadre d'une procédure de cybercriminalité.

[32] Sécurité et stratégie, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », Miriam Quéméner, cairn, 2011, P.56, https://www.cairn.info/revue-securite-et-strategie-2011-1-page-56.htm#re12no12

[33] 8ème Conférence INTERPOL-Europol sur la cybercriminalité : « Plus de la moitié de l'humanité court un risque », 2020, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/8eme-Conference-INTERPOL-Europol-sur-la-cybercriminalite-Plus-de-la-moitie-de-l-humanite-court-un-risque

[34] http://resources.mcafee.com/content/NAUnsecuredEconomiesReportwww.lemonde.fr/web/depeches/0,14-0,39-38313716@7-37,0.html

Cette question de la preuve numérique intéresse aujourd'hui à plusieurs égards nombre d'Etats, surtout ceux qui sont régulièrement ciblés par les attaques cybercriminelles d'envergure internationale. Ceux-ci ont été convaincus de l'idée qu'une coopération aboutissant à la création d'un cadre juridique pourrait permettre de faciliter la collecte des traces numériques dans le cadre d'une enquête pénale. C'est pourquoi, réunis à Budapest, les Etats engagés dans la lutte contre la cybercriminalité ont voté le texte international de référence en matière de lutte contre la cybercriminalité. Le texte qui permet donc de faciliter la collecte de la preuve numérique est aujourd'hui la convention de Budapest du 23 novembre 2001 avec son premier Protocole additionnel du 28 janvier 2003. Rédigé par le Conseil Européen avec la participation fructueuse des Etats comme le Canada, la Chine et le Japon, ce texte a été ratifié par soixante-cinq (65) Etats[35]. Il a été transcrit dans l'ordre interne français par une loi du 19 mai 2005[36], loi qui a reçu son application grâce aux décrets d'applications n° 2006-580 et 2006-597.

Concrètement, cette convention traduit la volonté des Etats parties à délimiter le spectre infractionnel de la cybercriminalité, instaurer un nouveau réseau d'échange pour la conservation de données informatiques de connexion et d'identification et inviter les pays du Conseil Européen à définir les limites de leur juridiction. Le rapport « Protéger les internautes » susmentionné ajoutait à ce titre que la convention se voulait être pour les Etats membres un instrument susceptible de leur permettre de collecter efficacement les éléments de preuves des cyber-infractions transfrontalières[37]. Pour autant, ce texte présente des lacunes sur les éléments numériques susceptibles de constituer ce type de preuve et sur leur méthode de collecte. Aussi, l'ensemble de son contenu a-t-il été rédigé en des termes généraux, laissant tirer à travers son article 14-2-c la conclusion que seuls les pays membres ont eux-mêmes la responsabilité de mettre en place, de façon personnelle, leur propre stratégie quant à la collecte de la preuve numérique en cybercriminalité. Or, avant cette convention, en 1995, le Conseil de l'Europe avait déjà, dans une recommandation, invité les Etats à définir eux-mêmes leur propre stratégie visant à créer des unités spécialisées en vue de la répression des cyber-infractions[38]. Sur cette base, il y avait eu en France une anticipation à la collecte de la preuve numérique notamment avec une première loi relative à la fraude informatique, la loi Godfrain[39]. Elle définit la responsabilité pénale des cyber-délinquants. Portant le nom de son concepteur, cette loi se retrouve actuellement dans le code pénal au niveau son livre III, titre II, chapitre III.

Aujourd'hui, sous l'impulsion de la convention de Budapest et des nombreux textes de l'Union européenne sur la cybercriminalité et la preuve numérique, le système français tend à renforcer son arsenal juridique quant à la collecte de la preuve numérique. Pratiquement, les méthodes de collecte de preuves dans ce domaine ne sont pas différentes des autres, et cela

[35] Convention sur la cybercriminalité — Wikipédia (wikipedia.org)
[36] Loi n° 2005-493 du 19 mai 2005 parue au JO n° 116 du 20 mai 2005, autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques
[37] « Protéger les internautes », rapport sur la cybercriminalité, groupe interministériel sur la lutte contre la cybercriminalité, février 2014, P.90
[38] « La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique », CNEJITA, Colloque, 13 avril 2010, P.13
[39] Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique

amène certains auteurs à conclure que la preuve numérique est loin d'être originale[40]. Néanmoins, la nouvelle technologie permettra de constater un sérieux retard du droit pénal sur elle, et amènera les autorités françaises à revoir certaines pratiques juridictionnelles et d'enquête. En claire, si par exemple il est facile de retrouver les traces des échanges de menace de mort ou de conversation à caractère pédopornographique entre un auteur et sa victime concomitamment sur leurs comptes sociaux ou dans leur téléphones lorsque ceux-ci peuvent être facilement accessibles, dans certains cas, cela ne va pas être simple lorsqu'on sait que l'information numérique de nature fragile, fugace et volatile peut être, grâce à la nouvelle technologie, modifiée, supprimée ou *obfusquée* c'est-à-dire, être noyée dans une masse de données et ce, dans plusieurs serveurs répandus à travers les quatre points du globe, rendant ainsi complexe son accessibilité. Dans ce contexte, le défaut de coopération de l'Etat sur le territoire duquel les informations ont été dissimulées peut constituer un frein à l'enquête, conduisant parfois à une cristallisation des procédures en cours.

De plus, même en cas d'accord politique entre deux Etats, la coopération peut parfois se révéler inutile lorsque le système pénal du pays étranger n'offre pas une meilleure garantie permettant de réunir les éléments de preuve et de retrouver les délinquants. C'est le cas par exemple en Afrique où la majorité des cyber-escrocs utilisent des cybers café pour commettre leur forfait. La difficulté dans cette situation est que les adresses IP générées par ces ordinateurs ne permettent pas d'identifier les auteurs malgré la volonté affichée de certains Etats africains de coopérer. Il n'est pas aussi rare de constater que certains éléments recueillis soient déjà détruits par les délinquants au moyen d'outils informatiques sophistiqués ou que, lors de l'exploitation du contenu de la preuve, les enquêteurs n'eussent pas pris les précautions adéquates afin de sécuriser la preuve, de sorte que l'authenticité de l'information numérique contenue dans une mémoire de stockage soit déjà compromise avant même sa présentation au juge.

Quant au juge pénal, lorsque celui-ci se retrouve en possession des informations numériques d'une procédure, il lui faudra aussi s'assurer que la procédure ayant abouti à la collecte des éléments respecte les exigences de loyauté et de proportionnalité. En effet, il n'est pas sans constater que, pour certaines infractions pour lesquelles la preuve pénale numérique peut s'avérer difficile à constituer, quelques enquêteurs s'adonnent à toute sorte de pratique pouvant parfois être qualifiées de détournements de procédure. Il incombe donc au juge de vérifier la mise en œuvre de la procédure d'enquête dans les règles de la loyauté de la preuve. C'est sur cette question que s'est récemment penchée la Cour de Strasbourg le 25 mai dans deux affaires emblématiques. Il s'agit des affaires Brother Watch c. Royaume-Uni et Centrum För Rättvisa c. Suède relatives à l'interception de masse des données de communication à l'échelle internationale. En effet, depuis les révélations du lanceur d'alerte américain Edouard Snowden sur la mise sur la mise sur écoute de l'UE par les services américains, de nombreux Etats ont mis en place un système de sécurité permettant d'intercepter les communications entre les individus. Si de telles mesures sont justifiées selon la Cour EDH par le devoir des Etats de protéger leurs citoyens et de renforcer leur souveraineté, elles soulèvent néanmoins un

[40] Le traitement de la preuve numérique dans les procédures judiciaires civiles et pénales, Etienne VERGES, justice actualité n°21, 2019, p1

sérieux débat sur la protection des droits des individus constitutionnellement et conventionnellement garantis dans un Etat qui se veut démocratique ; parce que, lorsque de telles surveillances électroniques ne sont pas ciblées, c'est-à-dire diligentée dans le cadre d'une enquête pénale, le risque de compromission d'une procédure pénale par usage de données obtenues dans le cadre d'une mission de police administrative est non négligeable et par là, interpelle sur la loyauté des enquêteurs.

Cet état des lieux, loin d'être exhaustif, dresse le défi du droit pénal face à une forme particulière de criminalité dont la preuve comporte plusieurs défis. En effet, tout en s'érigeant en police du cyberespace, il est vrai que la justice pénale a la légitimité de collecter les éléments de preuve au moyen de la technologie. Cependant, il doit aussi se garder de trop faire confiance aux informations fournies par celles-ci de peur de condamner injustement. C'est d'ailleurs en occurrence dans ce contexte que Mélanie Clément-fontaine, lors d'un colloque organisé par la compagnie nationale des experts de justice en informatique et technique associée **(CNEJITA)** sur la preuve numérique, soulignait que « *le droit s'adapte pour accueillir ces modes de preuve tout en gardant une distance avec le présupposé du tout scientifique »*[41].

***Le choix du sujet***

C'est donc l'étude de cette adaptation du droit pénal à cette nouvelle forme de preuve pénale, avec toutes les implications juridiques et techniques que cela peut présenter tant à l'égard des acteurs judiciaires (police, magistrats, experts de justice), que des auteurs ainsi que des victimes, qui a été au cœur de mes recherches dans le cadre de mes stages. Au contact des personnes que j'ai rencontré, j'ai pu comprendre comment les différents acteurs interviennent dans l'établissement de la preuve numérique en cybercriminalité, parviennent à réunir les éléments numériques en lien avec différentes formes de cybercriminalité et à en assurer leur fiabilité. Dans mes recherches, il m'est aussi apparu nécessaire de découvrir les problématiques nouvelles auxquelles sont confrontés ces différents acteurs dont la plupart ne sont pas formés pour comprendre les subtilités de la technologie numérique. J'ai pu également étudier quelques jurisprudences qui traitent de la preuve en cybercriminalité et les attentes des magistrats en termes de constitution de preuve. Ont enfin été au cœur de mes attentions, les enjeux relatifs aux atteintes à la vie privée des individus que peuvent constituer la mise en œuvre de la collecte des données numériques, le cas échéant de l'interception de masses des informations.

De ces analyses, je suis parvenu à formuler mon sujet de mémoire de la manière suivante : « **La preuve numérique à l'épreuve de la cybercriminalité** »

Le but ici est, étant donné que le concept de la preuve numérique apparait encore flou, de s'y intéresser principalement, le comprendre, c'est à dire l'identifier, étudier dans quelle mesure elle peut prétendre avoir une valeur probante, et enfin, découvrir le défi auquel sa constitution soumet les acteurs judiciaires dans le cadre de son établissement.

Cela suppose donc d'abord de comprendre le concept de la preuve numérique au sens du droit pénal, de découvrir son cadre juridique et opérationnel (**chapitre** I), et ensuite de

[41] Ibid, P10

comprendre son mode de collecte dans le cadre d'une cyber-investigation, et d'exploitation par les magistrats sans oublier les limites liées à sa constitution (**chapitre** II).

## <u>Chapitre 1</u> : La preuve pénale numérique : définition, cadre juridique et opérationnel en matière cybercriminelle

Lorsqu'on évoque la question de la preuve, l'on s'intéresse habituellement à son objet, les personnes qui en ont la charge et à la modalité de sa constitution[42]. Toutefois, sous cette rubrique, seront en priorité mis en exergue la définition du concept de la preuve numérique **(section 1**) ainsi que son régime juridique et opérationnel **(section 2).**

### <u>Section 1</u> : Du concept de la preuve numérique en droit pénal

S'il a fallu une loi du 13 mars 2000[43], transposant une directive du Conseil de l'Europe[44], pour consacrer la signature électronique comme preuve en droit civil, au pénal, cette consécration ne semble pas avoir posé de difficulté, principalement à cause du principe de la liberté de la preuve pénale qui voudrait que tout moyen soit accepté comme mode de preuve. Cela n'empêche pas néanmoins de faire le constat que le concept de la preuve numérique au sens du droit pénal est encore flou et pose quelques difficultés de qualité **(paragraphe 1),** même si les dispositions relatives à son régime et au statut des personnes qui en ont la charge dans le cadre précis d'une cybercriminalité sont connues **(paragraphe 2).**

#### § 1 : <u>Un concept au contours non précis</u>

L'imprécision tient au fait que nulle part dans le droit pénal interne ou international une définition de la preuve numérique n'a été apportée. Deux conceptions existent : une qui limite la preuve à son contenu, c'est à dire aux informations numériques (**A**), l'autre qui fait le tri en entre les informations en cherchant lesquelles peuvent réellement une valeur probante (**B).**

##### *A. <u>La conception limitant la preuve numérique à son contenu</u>*

L'expression « preuve numérique » n'a pas explicitement été utilisée par le législateur français, en tout cas pas dans les codes pénal et de procédure pénale, ni en jurisprudence[45]. Le constat en est que, en évoquant les éléments de preuve, le législateur utilise souvent l'expression « données informatiques ». Cette appellation revient à plusieurs reprises et l'on la retrouve par exemple au niveau des articles 57-1 du CPP relatif à la perquisition d'un système

---

[42] "Le rôle du juge pénal dans la recherche de la preuve" in Mélanges en l'honneur de G. Giudicelli-Delage, Humanisme et Justice, Dalloz, 2016

[43] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

[44] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, **Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques - Légifrance (legifrance.gouv.fr)**

[45] La preuve numérique, entre continuité et changement de paradigme, Etienne VERGES, éd. Justice actualité n°21, juin 2019, P.1

informatique, 323-1 et suivants du Code pénal qui traitent des atteintes aux STAD[46]. La convention de Budapest sur la lutte contre la cybercriminalité fait aussi usage de ce terme [47].

Le terme « donnée numérique », en effet, renvoie à la traduction anglaise de « *Digital data* ». Il a fait son apparition à la fin des années 1960 avec les premiers moyens de communications et d'informations électroniques à savoir, la messagerie instantanée et le courrier électronique, puis après grâce à la diffusion de l'ordinateur personnel. A partir de l'année 2000, la révolution technologique a provoqué une exploitation nouvelle du calcul, ce qui a eu pour conséquence l'émergence d'un commerce numérique approuvé par une masse populaire impressionnante. C'est à partir de cet instant qu'informatique et Internet ont pris une telle importance dans la vie de l'Homme contemporain à tel enseigne que tout son quotidien, enfin presque, se résume au numérique[48]; qu'il s'agisse de travailler, regarder un film, faire une photographie, commercer, faire une réservation, se divertir, faire des rencontres, s'instruire, etc. ainsi, même s'il n'a qu'une conscience diffuse que toutes ses activités sont faites au moyen du numérique, toutes les données laissent des informations sur son statut et ses empreintes sur Internet.

A ce jour, les données numériques sont définies comme toutes informations contenues dans un système de traitement automatisé de données. Selon la Cour de cassation, la notion de donnée doit être considérée dans son acception la plus étendue comme la représentation d'une information, la forme et non la substance d'un élément de connaissance quelconque[49]. Cette conception vient en effet s'accommoder avec celle des rédacteurs de la convention de Budapest qui eux-mêmes conçoivent les données informatiques comme « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction* »[50]. Aussi, dans une récente étude réalisée sur le numérique, le Conseil d'Etat a-t-il partagé cette même conception du numérique. Ce dernier définit une donnée numérique comme « *la représentation de l'information ou de grandeurs physiques (par ex. images, sons) par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1 »*[51].

A la différence d'un écrit papier, une donnée numérique présente plusieurs caractères spécifiques. Elle peut être facilement copiable, riche quantitativement et qualitativement, vulnérable, dépendant de son environnement, effaçable, non statique ou modifiable[52]. Ainsi, dans une enquête de cybercriminalité, les enquêteurs de la PJ ou les experts traiteront une quantité parfois illimitée et diversifiée de données, de sorte qu'on en arrive à la conclusion que seules les informations constituent la preuve pénale numérique. Il peut donc être question des

[46] Livre III (« Des crimes et délits contre les biens »), titre II (« Des autres atteintes aux biens »), chap. III : « Des atteintes aux systèmes de traitement automatisé de données », Code pénal, P675 et S.
[47] Article 16 et S. de la convention de Budapest
[48] Adjectif substantivé utilisé parfois pour désigner la technologie numérique
[49] Crim., 19 mars 2014, Bull 1193, n° 12-87-416
[50] Article 1-b de la Convention de Budapest
[51] Conseil d'État, *Étude annuelle 2014 – Le numérique et les droits fondamentaux*. 2014, v. : https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000541.pdf, p. 35, Note de page 4
[52] « La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique », CNEJITA, Colloque, 13 avril 2010, P.19

traces d'identité numériques d'une personne, des données relatives à ses activités sur Internet lorsqu'elle est connectée à un serveur fournissant les services internet, de sa localisation, des informations sur sa vie privée, sa profession, ses avoirs et transactions bancaires, des échanges de messages ou de mail, etc. Le plus souvent, ces données sont logées dans un environnement qui empêche leur accès ou interprétation immédiate par les sens. A ce titre, David BENICHOU, magistrat instructeur au Tribunal de Grande Instance de Nanterre conçoit « *la preuve numérique ou électronique (comme)* ***toute information contenue dans un objet que l'homme n'est pas en mesure d'examiner avec l'usage de ses sens directs (ex : contenu d'une clé USB, d'un disque dur ou d'une carte à puce, code source d'un site web****…)* »[53]. Il ajoute également que « *la preuve numérique couvre aussi ce qu'une personne normalement sensée ne peut interpréter en raison de son caractère technique* »[54]

Toutefois, bien que présentant l'ensemble de ces caractères précédemment cité, toutes les données numériques ne sont pas forcément constitutives de preuve pénale numérique. Autrement dit, pour qu'une donnée numérique soit érigée au rang de preuve pénale numérique, il ne suffit pas seulement qu'elle soit aperçue avec les sens ou représentée de manière binaire par une suite de chiffres ou de lettres, copiable, riche quantitativement et qualitativement, effaçable, statique, accessible sur un mémoire de stockage ou renseignant quelques informations sur un internaute. Il est en effet aussi prépondérant qu'elle présente véritablement les garanties d'une preuve pénale.

### B. ***De l'information numérique à la preuve pénale numérique***

Pour avoir une valeur probante, l'information numérique doit présenter des garanties de fiabilité qui correspondent à deux groupes de conditions : les conditions générales et les conditions spécifiques.

Les conditions générales incluent l'idée que l'information numérique, comme tout élément de preuve, soit recevable et en lien direct avec les faits en l'étude. Une information numérique est recevable devant une juridiction pénale lorsqu'elle a été recueillie dans les conditions de légalité, c'est-à-dire lorsque les principes de dignité, de loyauté, de proportionnalité et/ou de nécessité ont été rigoureusement observés par les enquêteurs.

Pour rappel, le principe de dignité renvoie à l'absence d'emploi de la violence par les agents enquêteurs au moment de la collecte des éléments de preuve. La jurisprudence française est intransigeante sur cette question de dignité. Dans une décision de 2010 portant sur une question prioritaire de constitutionnalité, le Conseil constitutionnel a notamment rappelé cette valeur constitutionnelle. Il a précisé que « la protection des droits et libertés constitutionnellement garantis, au nombre desquels figurent le respect de la vie privée, protégé par l'article 2 de la Déclaration de 1789, le respect de la présomption d'innocence, le principe de dignité de la personne humaine, ainsi que la liberté individuelle que l'article 66 place sous la protection de l'autorité judiciaire »[55]. La chambre criminelle s'inscrit également dans la même logique vis-à-

[53] « La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique », CNEJITA, Colloque, 13 avril 2010, P.58
[54] Ibid.
[55] Conseil constitutionnel, 16 septembre 2010, QPC 2010-25

vis de ce principe. Dans une affaire liée à une garde à vue qui se serait déroulée dans une atmosphère de tension, où le gardé à vue aurait subi une privation de liberté inhumaine[56], si elle n'a pas censuré les juges du fond, elle a néanmoins tenu à rappeler l'évidence du respect du principe de la dignité de la personne humaine. La Cour européenne des droits de l'homme, de son côté, tient un regard de veille rigoureux sur le respect de ce principe par le biais de l'article 3 de la convention européenne, lequel interdit la torture et le traitement inhumain et dégradant.[57]

La loyauté, quant à elle, est la conformité aux règles de la procédure. Dans le cadre d'une enquête judiciaire, elle consiste pour les enquêteurs à ne pas provoquer à la commission de l'infraction. La doctrine la conçoit comme « u*ne manière d'être de la recherche de la preuve conforme au respect des droits de l'individu et à la dignité de la justice* »[58]. Ce principe de loyauté de la preuve est valable tant pour les enquêteurs que pour les magistrats[59]. Il a été rappelé plusieurs fois par la Cour de cassation notamment dans l'arrêt *Schuller* en 1996, dans lequel elle a solennellement affirmé que n'était pas admissible une preuve procédant d'une "*machination de nature à déterminer les agissements délictueux et que, par ce stratagème, qui a vicié la recherche et l'établissement de la vérité, il a été porté atteinte au principe de la loyauté des preuves*" [60]. Toutefois, si son fondement a été principalement d'interdire la provocation à la commission de l'infraction, ce principe n'interdit pas la provocation ou l'incitation à la preuve par les autorités publiques. En effet, de nouvelles législations sont venues assouplies ce principe en instaurant des dispositions dérogatoires à l'égard de la criminalité transfrontalière dont les preuves sont souvent difficiles à collecter. C'est le cas de la loi dite Perben II du 09 mars 2004 qui a étendu le régime de l'infiltration d'agents dans les organisations afin d'inciter à la preuve. Il y a également la loi LOPPSI 2 qui intervient dans ce domaine. En revanche, à la faveur des particuliers ou les justiciables, contrairement à la jurisprudence de la chambre civile qui maintient une position constante sur le refus de productions des preuves recueillies illicitement, la déloyauté dans la collecte de la preuve en droit pénal est admise à la condition que ces preuves seront débattues et que l'exercice du droit de la défense sera pleinement respecté[61]. Le principe de proportionnalité implique que les moyens de preuve employés ne sont pas en disproportion avec l'infraction poursuivie, afin de

[56] Cass. crim., 26 février 1991, Bull. n° 97.

[57] CEDH, 28 juillet 1999, Selmouni c/ France « *La Cour rappelle que l'article 3 consacre l'une des valeurs fondamentales des sociétés démocratiques. Même dans les circonstances les plus difficiles, telle la lutte contre le terrorisme et le crime organisé, la Convention prohibe en termes absolus la torture et les peines ou traitements inhumains ou dégradants… En tout état de cause, la Cour rappelle qu'à l'égard d'une personne privée de sa liberté l'usage de la force physique qui n'est pas rendu strictement nécessaire par le comportement de ladite personne porte atteinte à la dignité humaine et constitue, en principe, une violation du droit garanti par l'article 3 »*

[58] P. Bouzat, "La loyauté dans la recherche des preuves", Mélanges Hugueney, 1964, p. 155

[59] Cass. crim., 12 juin 1952, Bull. n° 153

[60] Cass. crim., 27 fév. 1996, bull. crim., n° 93 , Voir aussi Cass., crim., 4 juin 2008, Bull. crim. n°41 et Cass. crim., 11 juillet 2017, n° 17-80313

[61] Cass. crim., 15 juin 1993, Bull. 210 : « ... *la circonstance que des documents ou des enregistrements remis par une partie ou un témoin aient été obtenus par des procédés déloyaux ne permet pas au juge d'instruction de refuser de les joindre à la procédure, dès lors qu'ils ne constituent que des moyens de preuve qui peuvent être discutés contradictoirement ; que la transcription de ces enregistrements, qui a pour seul objet d'en matérialiser le contenu, ne peut davantage donner lieu à annulation »*

protéger la vie privée des personnes. A défaut du respect de ces principes, les éléments de preuves recueillis seront frappés de nullité.

En outre, toujours au titre des conditions générales, il apparait également important que les indices de preuve recueillis soient en lien direct avec les faits sur lesquels porte une poursuite. Une telle évidence se justifie au regard notamment d'une bonne administration de la justice. Ce critère de lien direct est formulé de diverses manières tant en droit interne que dans la convention. La convention de Budapest parle de **« données relatives au trafic[62]** », qu'elle désigne par « *toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent* ». A l'analyse, l'usage du terme « trafic » est embarrassant dans la mesure où il n'éclore pas précisément le lien direct avec une enquête de cybercriminalité. Littéralement, cette formule utilisée par les rédacteurs de la Convention met en lumière les informations relatives à une communication enregistrée dans le cadre d'une mesure de surveillance électronique[63]. En revanche, la formule utilisée par le législateur français laisse entrevoir une meilleure perception de ce critère. Il parle par exemple de **« donnée intéressant l'enquête[64]** » ou de **« donnée utile à l'enquête** ». Dans la pratique, lorsque les OPJ ou les magistrats, conformément à l'article 159 du CPP, sont amenés à solliciter une expertise en vue de l'extraction des données d'un appareil, les consignes données par ceux-ci laissent transparaitre de façon claire l'intérêt du lien direct. A titre d'exemple, dans un dossier dans lequel un individu a comparu devant la Cour d'appel de Limoges pour les faits qualifiés d'exhibition sexuelle, de corruption de mineurs de moins de 15 ans et de pédopornographie[65], commis au moyen des réseaux de communication au public, un technicien de la police scientifique et technique de Limoges a été requis aux fins d'extraire les données ayant un rapport avec les chefs d'accusations. Les instructions contenues dans la réquisition ordonnée par le magistrat en charge de la procédure se présentaient de la façon suivante :

« *Nous X (le magistrat)*

*Prions, et au besoin, requérons Y (l'expert)*

*A l'effet de procéder aux actes ci-après :*

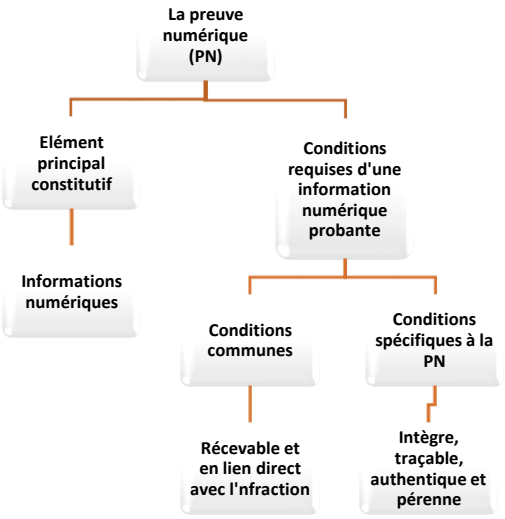
- *Prendre en charge le scellé contenant l'appareil ou le support de stockage appartenant à Z (le mis examen)*
- *Briser le scellé*
- ***Procéder à l'analyse de cet appareil ou du support et indiquer tout renseignement utile à l'enquête en cours, tous échanges entre Z et des adolescents, échanges à caractère sexuel.***
- ***Vérifier si cette personne détient des images des adolescents nus »[66].***

De plus, l'information numérique pour avoir une valeur probante, doit présenter des garanties spécifiques telles que l'intégrité, la traçabilité et l'authenticité. L'intégrité renferme

[62] Article 16 de la convention de Budapest
[63] Article 1 de la convention :
[64] Article 57-1 du CPP
[65] Affaire audiencé devant le TJ de Limoges le 11 juillet 2019
[66] *Ibid.*

l'hypothèse où le contenu de l'information n'a pas été modifié. L'authenticité tient à la fiabilité de l'origine de l'information, et la traçabilité met en exergue le fait que le procédé technique de la collecte des données doit permettre d'établir les différentes opérations techniques qui ont pu être réalisées jusqu'à la conservation des éléments de preuve. Certains auteurs ajoutent un autre critère qui est celui de la pérennité de l'information, mettant ainsi en lumière la qualité de la preuve dans le temps.

Le but de ces critères est de permettre la validité des éléments de preuve numérique et aussi d'éviter à la partie qui les produit d'être confrontée à une contestation du camp adverse. Cependant, il ne s'agit pas de critères posés ni par dans la Convention ni par le droit interne. Ils sont observés et pratiqués quotidiennement par les enquêteurs et experts spécialisés en cybercriminalité, et appréciés au moment de l'instruction ou du procès par les magistrats selon leur intime conviction.




## § 2 : <u>Typologie de données numériques et de leur support de stockage</u>

Dans le cadre d'une enquête de cybercriminalité, les enquêteurs traiteront plusieurs données numériques (**A**), lesquelles peuvent être stockées au moyen de divers supports (**B**).

### *A. <u>Typologie de données numériques</u>*

Généralement, les enquêteurs s'intéressent à un panel de données dont la plupart sont liées à l'identité numérique de la personne suspectée d'avoir commis une cyber infraction, sa localisation dans l'espace, ou le fonctionnement d'un programme malveillant (virus) grâce auquel une personne commis son action. Au titre des données liées à l'identité numérique, il y a les données à caractère personnel. On entend par donnée personnelle, les données pouvant permettre d'identifier ou de rendre identifiable une personne, directement ou non[67]. Il peut donc

[67] Article 4 al. 1 Règlement général de la protection des données personnelles, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

s'agir, dans le cadre d'une identification directe, des données relatives à l'état civil de la personne (nom, prénom, date et lieu de naissance), et dans le cadre d'une identification indirecte, des données comme par exemple des photos, l'adresse postale, le numéro de sécurité sociale ou numéro matricule, des adresses mail ou IP[68], la messagerie électronique, des données de recherches sur Internet, l'historique d'appel et les durées d'appel, des données multimédias, le code de chiffrement, des fichiers bureautiques (tableurs, documents divers, présentations, notes), des messages vocaux, des avatars de mondes virtuels[69], des données relatives à l'identité domaniale dans le cadre d'un usage frauduleux du nom patronymique d'autres personnes dans le but d'en tirer un bénéfice indu, des données de localisation, bref un panier de données tel que fixé au niveau de l'article 10-13, I du code des postes et des communications[70].

Aussi, pour localiser une personne suspectée, les enquêteurs s'intéressent aux coordonnées géographiques fournies par le GPS du téléphone ou de l'ordinateur de la personne, la date, l'horaire, sa carte de crédit. A ce titre Visa a développé en partenariat avec la startup Finsphere un programme dénommée « *Mobil Location confirmation* » visant à recouper la position de l'utilisateur d'une carte et du commerçant.[71] Concrètement, lors d'un paiement, l'utilisateur entrera son code de carte de crédit, il y aura ensuite une transformation de son GPS en adresse postale du commerçant que Finsphere vérifiera avant de confirmer la demande.

Les données liées à un programme malveillant sont en réalité les données concernant le fonctionnement et la finalité de ce programme. Sous ce canevas, les enquêteurs s'intéressent aux modes d'opération du délinquant à savoir par exemple, dans le cas d'un *phishing*, à l'envoi d'un URL (une adresse électronique) qui a pour fonction de rediriger l'internaute vers un autre site où un programme malveillant s'incrustera dans l'espace privé de cet internaute pour y aspirer ses informations. En outre, il y les métadonnées, lesquelles constituent les schémas de classification qui permettent de structurer un fichier numérique.

La plupart de ces éléments de preuve ne constituent pas en soi une nouveauté parce qu'ils furent connus par le passé sous une forme analogique et sont aujourd'hui numérisés. C'est le cas entre autres des vidéos, des photographies, des bandes-son qui étaient gravées sur des supports analogiques à savoir des bandes magnétiques, disques, vinyles, etc. Sont retrouvés également des procédés qui ont subi une profonde transformation sous l'emprise de la technologie, mais dont la finalité ne diffère pas. En effet, la localisation d'un individu pouvait se faire par le biais d'une filature, d'un témoignage ou d'une géolocalisation par le biais d'un radar. Mais la technologie permet désormais de localiser un individu en suivant les traces de

---

[68] C'est un numéro d'identification adressé de façon permanente ou provisoire à chaque périphérique relié à un réseau qui utilise l'Internet Protocol. Sur le plan mondial, une adresse IP est attribuée par l'organisme ICANN (*Internet Corporation for assignated Names and numbers*) pour ce qui concerne les périphériques relevant du public. Elle existe sous deux formes, l'adresse IPv4 et l'adresse IPv6., initiation au fonctionnement de l'Internet et aux enjeux de la gouvernance Internet, l'OCLCTIC, DACG, juin 2021
[68] *Ibid. P.56*

[69] Les avatars du monde virtuel sont des programmes robots (personnage fictif) qui sont créés pour accéder et exécuter dans le monde virtuel des fonctions données. Ils permettent de suivre les intérêts des internautes, leur désir, etc.
[70] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006466369/2010-09-22/
[71] La géolocalisation : nouvelle arme de visa ?, Jérémy, https://www.paymon.fr/2015/03/12/la-geolocalisation-nouvelle-arme-de-visa-pour-lutter-contre-la-fraude/ , 2015

son téléphone portable ou de sa carte de crédit. On retrouve le même raisonnement pour les courriels, la mise sur écoute, le portrait-robot génétique qui a la même fonction que le portrait-robot dessiné.

Par ailleurs, l'on ne peut citer ces données numériques indépendamment de leur support qui constituent l'espace sécurisé de leur stockage.

### *B. Les types de supports de stockage*

Les enquêteurs et les experts s'intéressent dans leur recherche à plusieurs supports de stockage lesquels sont d'accès direct ou indirect. Sont d'accès directs, les supports détenus directement par les personnes suspectées ou auprès des opérateurs logés sur le territoire français. C'est le cas entre autres des supports physiques comme le téléphone, l'ordinateur portable ou de bureau, les supports amovibles (clé USB, disque dur), la console d'administration de vidéo de protection, et les autres supports comme les serveurs (archives, stockage, hébergement), le GPS (dans un véhicule ou non), la console de jeux vidéo et la box internet, et les serveurs conservés par les opérateurs internes (Orange, Free, Bouygues et SFR).

Quant aux supports d'accès indirect, allusion est faite notamment aux bases de données détenues auprès des hébergeurs de sites étrangers dont les géants sont Facebook, Amazone, Microsoft, Google et les autres opérateurs externes. On rencontre à cet effet, la base de données Cloud qui est un serveur notoire existant sous plusieurs formes : les serveurs de données chez OVH, serveur de mail chez Google, les comptes GPS (TOM-TOM, Two nav…).

En outre, certaines bases de données détenues ou contrôlées par les services de l'Union européenne dans le cadre de la coopération judiciaire et policière entre ses Etats membres sont restent un facteur utile pour une enquête de cybercriminalité. En fait, dans le cadre de la Convention de Schengen, l'UE détient une base de données dénommée le *Système d'Information Schengen*. Mis en service depuis 1995, ce système permet concrètement d'avoir des informations précises sur une personne suspectée, disparue, signalée, ou sur la circulation de faux billets, documents détournés, etc. Il relie les Etats membres et son accès dans le cadre d'une procédure d'interrogation automatisée diligentée par les autorités (Douane, Police judiciaire et Gendarmes) est direct. Pour avoir enregistré plus de 70 millions de signalement depuis sa création, le SIS est aujourd'hui la plus grande base de données au monde. Cette base permet également la détection et l'arrestation des djihadistes en partance pour des zones de guerre ou en revenant, si ceux-ci font l'objet d'une alerte. Récemment, par exemple, il a permis d'identifier à la frontière bulgare un homme partant faire le djihad en Syrie en emmenant son jeune enfant que sa compagne avait signalé en France. De l'autre côté, il y a aussi le Système *Prüm* issu du Traité de Prüm que certains appellent Schengen+. Ce traité établi pour renforcer la coopération policière et judiciaire dans le cadre du troisième pilier de l'UE, permet

principalement l'échange de données relatives aux empreintes génétiques, digitales et à caractère personnel entre les Etats[72].

Quant au système de donnée PNR (Passager Name Record), son accès aux autorités étatiques, dans le cadre de la lutte contre la criminalité transfrontière, a longtemps animé les débats surtout à la suite des attentats du 11 septembre. Nombre d'Etats était réticent contre un accord consistant pour les compagnies à fournir des informations contenues dans cette base aux autorités étatiques pour des raisons tenant à leur politique interne ou à cause des modalités de fonctionnement de ce système, sans oublier son enjeu à l'égard de la protection des droits fondamentaux. Certes, il y a eu des accords externes sur la question, mais au sein même de l'Union, la résilience à l'accord régnait en puissance. Les attentats contre le magazine de presse Charlie hebdo en France ont quelque peu permis de surmonter les difficultés. Cela a permis d'aboutir à un accord d'échange d'informations et de données relatives au dossier personnel des passagers. La France a transposé cet accord dans sa législation grâce à une loi antiterroriste d'octobre 2017 permettant la fin de l'état d'urgence. Ainsi, les services de police peuvent avoir accès aux données renseignant sur les passagers, leur identité, leur moyen de paiement, leur activité, leur destination, etc. En France, ce système s'appelle API-PNR France et permet de renseigner à la fois sur les données de réservation (PNR) et celles d'embarquement (API, *Advance Passager Information*)[73].

En somme, la technologie numérique offre la possibilité aux enquêteurs de prendre en compte un ensemble de données numériques dans le cadre de la constitution de la preuve. Ces données existent sur maints supports parmi lesquels les serveurs distants qui sont, pour la majorité, logé aux USA. Toutefois, si certains sont connus et accessibles, d'autres ne le sont pas et constituent de ce fait une niche parfaite où la cybercriminalité s'épanouit sans crainte. C'est le cas par exemple, et on y reviendra, des serveurs du *darkweb ou le web profond.*

## **Section 2 : Le cadre juridique et institutionnel de la preuve numérique en matière d'investigation cybernétique**

La complexité de la cybercriminalité est aujourd'hui un point de vue quasi unanime. En effet, il serait très surprenant pour un Etat, aussi puissant qu'il soit, d'affirmer sans l'ombre d'un doute qu'il se trouve à l'abri de ce phénomène. Les dernières actualités relatives aux différentes attaques informatiques commises sur des infrastructures américaines montre que même la première puissance mondiale est loin d'être non vulnérable sur le plan de cyberattaque. Aujourd'hui, les Etats conjuguent toutes les occasions possibles, tant en au plan local qu'international, pour lutter contre ce phénomène. Il s'observe une course contre la montre dans le processus de législation des normes anti-cybercriminalité. Des normes dont la plupart des dispositions traitent de la preuve numérique (**paragraphe 1**) et qui permettent aussi de créer, en plus des acteurs existant, d'autres types d'acteurs qui sont dotés de compétence renforcées en matière de la collecte des traces numériques **(paragraphe 2).**

[72] https://fr.wikipedia.org/wiki/Trait%C3%A9_de_Pr%C3%BCm_(2005)
[73] Le système API-PNR France, CNIL, 2016, https://www.cnil.fr/fr/le-systeme-api-pnr-france

## § 1 : L'arsenal juridique de la preuve numérique

Le droit pénal étant une prérogative de la puissance publique, il va de soi que la constitution de la preuve numérique ne peut se faire en dehors du cadre légal ou conventionnel. C'est alors que les dispositions qui traitent de la preuve numérique trouvent leur fondement dans deux ordres juridiques : l'ordre juridique interne (**A**) et l'ordre international **(B).**

### *A. Les dispositions juridiques internes*

D'abord, dans l'ordre juridique français notamment en droit pénal, la preuve est régie à l'article 427 et suivants du Code de procédure pénale. Cet article précise que, *« hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout moyen de preuve et le juge décide d'après son intime conviction* ». Toutefois, d'autres dispositions de ce code renchérissent la question de la preuve pénale. C'est le cas notamment de l'article 57-1 issue de la loi du 18 mars 2003 relative à la sécurité intérieure, qui traite de la perquisition des systèmes informatiques. Cet article précise que dans le cadre d'une perquisition effectuée lors d'une enquête de flagrance, les enquêteurs peuvent accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données utiles à l'enquête en cours et stockées dans ledit système ou dans un autre, à condition que les données en question sont accessibles à partir du système initial. Dans le cas où les données sont dissimulées dans un système situé à l'étranger et lorsque l'OPJ en est informé, l'accès à ces données est fait dans le respect des engagements internationaux de la France[74]. Les dispositions de cet article sont mises en œuvre normalement dans le cadre d'une enquête de flagrance conformément à l'article 53 alinéa 1er du CPP[75], mais, dans le cadre d'une enquête préliminaire, elles peuvent être appliquée lorsque les exigences de consentement de la personne mise ne cause sont respectées, comme c'est prévu à l'article 76 du même Code. De plus, les dispositions relatives aux réquisitions informatiques ou télématiques de l'article 60-2 du code de procédure pénale issue de la loi n° 2003-239 du 18 mars 2003, donnent pouvoir aux différents enquêteurs, sur autorisation du procureur de la République[76], de demander aux organismes publics ou personnes morales de droit privé, à l'exception des églises ou des groupements à caractère religieux, philosophique, politique ou syndical ainsi que des organismes de presse audiovisuelle, de mettre à leur disposition les informations utiles à la manifestation de la vérité contenues dans le ou les systèmes de données nominatives, à l'exception de celles protégées par un secret prévu par la loi[77]. Cette disposition n'est applicable que dans le contexte d'une enquête préliminaire, mais peut l'être aussi pour l'instruction[78] et pour l'enquête de flagrance, uniquement sur commission rogatoire pour une enquête de flagrance, à la condition de respecter les conditions de l'article 53 du CPP.

[74] Article 57-1 alinéa 3 du CPP
[75] Article 53 du CPP « Est qualifié crime ou délit flagrant le crime ou le délit qui se commet actuellement, ou qui vient de se commettre. Il y a aussi crime ou délit flagrant lorsque, dans un temps très voisin de l'action, la personne soupçonnée est poursuivie par la clameur publique, ou est trouvée en possession d'objets, ou présente des traces ou indices, laissant penser qu'elle a participé au crime ou au délit. »
[76] Article 77-1 du CPP
[77] « Prévenir des actes de cybercriminalité dans un contexte professionnel », Martine Exposito, UNJF, P.39
[78] Ibid.

Par ailleurs, l'on retrouve aussi les dispositions liées au déchiffrement ou décryptage de données, issues de la loi du 15 novembre 2001 pour la sécurité quotidienne[79]. Insérée dans le CPP au niveau de son article 230-1, cette loi précise que, lorsqu'il apparait que les données saisies dans le cadre d'une enquête ou instruction ont subi un codage empêchant leur exploitation, toute personne qualifiée peut être désignée à cette fin[80]. A cela s'ajoute aussi les dispositions relatives à l'obligation de conservation des données et l'infiltration d'agents de police. Le principe de la conservation des données, une dérogation au principe d'effacement des données dès la fin de la communication, a été introduit dans le code des postes et des communications au niveau de son article L. 34-1-1[81] et de l'article 6-II de la loi du 21 juin 2004, par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Ces dispositions vont dans le sens qu'une directive de l'Union qui impose aux Etats l'obligation de conservation de données générées ou traitées dans le cadre de la fourniture de services de communications en ligne[82].

Sur l'infiltration, certaines dispositions issues de la loi dite Perben II autorisent des mesures d'enquête dérogatoire utiles à la lutte contre la cybercriminalité, notamment dans le cadre des réseaux de trafic d'être humain, du proxénétisme, de blanchiment, bref, les infractions dont la commission peut être facilitée par la technologie. L'initiative de cette mesure réside, selon certains auteurs, dans l'inefficacité des autres mesures existantes pour pouvoir identifier les auteurs de criminalité organisée[83]. Les dispositions sur l'infiltrations se retrouvent au niveau de l'article 706-81 et suivantes du CPP. La loi du 5 mars 2007 relative à la prévention de la délinquance étend le recours à cette mesure aux infractions sexuelles sur mineurs afin de faciliter également la preuve dans ce domaine, lorsque de telles infractions ont été faites au moyen de la technologie.

Enfin, les dispositions issues du code des postes et des communications, du code de la protection des données personnelles et du code monétaire constituent un enjeu important à la constitution de la preuve numérique. Elles n'ont pas forcément un lien direct avec la cybercriminalité mais peuvent aider à identifier l'utilisateur d'un réseau internet grâce à ses données personnelles, dans la limite légale. C'est le cas entre autres des dispositions de l'article 10-13, I du code des postes et des communications, déjà cité[84], qui traitent de la conservation des données.

---

[79] Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000222052/

[80] Article 230-1 du CPP

[81] Article L.34-1-1 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006465794/2010-09-22/

[82] Directive 2006/24/ CE *du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*

[83] Quemeur et Ferry, op. cit. P. 248

[84] *Cf. note de bas de page 52*

| Les dispositions du code de procédure pénale | les dispositions du code pénale | Les dispositions des autres codes |
|---|---|---|
| • Article 427 relatif au principe de la liberté de production de preuve<br>• Article 57-1 relatif à la perquisition informatique<br>• Article 60-2 relatif aux réquisitions télématiques et informatiques<br>• Article 76 relatif au consentement à la perquisition de la personne mise en cause<br>• Article 230-1 et suivants du CPP relatif au déchiffrement des données<br>• Article 706-81 relatif à l'infiltration | • Article 323-1 et Suivants relatifs aux atteintes aux STADs<br>• Les dispostions concernanant les infractions classiques commises au moyen du TIC | • Article L. 34-1-1 du code des postes et des communications<br>• Article R 10-13, I du même code<br>• Les dispositions du code monétaire<br>• code de la protection des données personnelles |

Tableau récapitulatif

### B. ***Les dispositions tirées des conventions et traités***

En premier lieu, au niveau régional, la volonté de l'Union d'instaurer un espace de sécurité, de liberté et de justice l'a amené à créer une coopération policière et judiciaire en matière pénale[85]. Basée sur le principe fondamental de reconnaissance mutuelle des décisions et jugements entre les Etats membres, cette coopération assurer la facilité entre les Etats. Grâce à elle, l'Union s'est dotée de la possibilité d'établir des règles minimales relative entre autres à l'admissibilité des preuves entre les Etats membre dans le cadre de la répression de la criminalité organisée[86], la criminalité informatique y compris[87]. A ce titre, l'article 87 du traité du fonctionnement de l'Union européenne pris en son alinéa 2-a précise que « *le Parlement européen et le Conseil, dans le cadre d'une procédure législative ordinaire, peuvent établir des mesures sur la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes* ». Cette volonté a été concrétisée et renforcée par la mise en place de plusieurs textes dont par exemple la directive d'enquête européenne du 03 avril 2014 qui a pour objectif d'exiger d'un Etat le transfert des éléments de preuves électroniques vers un Etat demandeur dans le cadre d'un mandat européen[88]. Ladite directive fait suite à deux décision-cadres européenne, l'une en date de 2003[89] sur le gel de bien et des éléments de preuves et l'autre de 2008 sur le mandat européen d'obtention de preuve visant à recueillir des documents, des

[85] Article 82-2-a du TFUE
[86] Ibid.
[87] Article 83-1 du TFUE
[88] Directive 2014/41/UE du Parlement et du Conseil du 03 avril 2014 concernant la décision d'enquête européenne en matière pénale
[89] Décision-cadre 2003/577/JAI du Conseil du 22 juillet 2003 relative à l'exécution dans l'Union européenne des décisions de gel de biens ou d'éléments de preuve (JO L 196 du 2.8.2003, p. 45).

données dans le cadre d'une procédure pénale[90]. Plusieurs dispositions de cette directive traitent de la question de la preuve numérique. L'article 13 par exemple donne plus de précisions sur les modalités de transfert de données entre les Etats[91]. Au niveau de l'article 12, l'Union a fait le choix de résoudre le problème du délai de traitement des demandes de transfert. Dans un premier temps, elle avait pu réduire ce délai à 120 jours[92], marquant une avancée louable par rapport au délai de 10 mois que prennent classiquement une procédure d'entraide dans le cadre du traité d'assistance judiciaire (MLAT)[93]. Tous les Etats membres participent à cette directive sauf le Danemark et l'Irlande qui fonctionnent sous le régime d'entraide pénale[94].

En outre, en 2013, l'Union a pris une directive[95] en remplacement de la décision-cadre 2005/222/ JAI, afin de rapprocher le droit pénal des Etats en matière de lutte contre des attaques contre les systèmes informatiques. Cette direction a apporté par exemple quelques éléments de

[90] Décision-cadre 2008/978/JAI du Conseil du 18 décembre 2008 relative au mandat européen d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédures pénales (JO L 350 du 30.12.2008, p. 72

[91] Article 13 de la directive d'enquête européenne : " 1. *L'autorité d'exécution transfère sans retard indu à l'État d'émission les éléments de preuve obtenus ou déjà en la possession des autorités compétentes de l'État d'exécution à la suite de l'exécution de la décision d'enquête européenne. Lorsque cela est demandé dans la décision d'enquête européenne, et dans la mesure du possible en vertu du droit de l'État d'exécution, les éléments de preuve sont transférés immédiatement aux autorités compétentes de l'État d'émission qui prêtent assistance dans le cadre de l'exécution de la décision d'enquête européenne conformément à l'article 9, paragraphe 4. 2. Le transfert des éléments de preuve peut être suspendu, dans l'attente d'une décision concernant un recours, à moins que la décision d'enquête européenne n'indique des motifs suffisants pour considérer qu'un transfert immédiat est indispensable au bon déroulement de son enquête ou à la préservation de droits individuels. Toutefois, le transfert des éléments de preuve est suspendu dans le cas où il causerait un préjudice grave et irréversible à la personne concernée. 3. Lors du transfert des éléments de preuve obtenus, l'autorité d'exécution précise si elle exige le renvoi des éléments de preuve à l'État d'exécution dès qu'ils ne sont plus nécessaires à l'État d'émission. 4. Lorsque les objets, documents ou données concernés sont déjà pertinents pour d'autres procédures, l'autorité d'exécution peut, à la demande expresse de l'autorité d'émission et après consultation de celle-ci, transférer temporairement ces éléments de preuve, à condition qu'ils soient renvoyés à l'État d'exécution dès qu'ils ne sont plus nécessaires à l'État d'émission ou à tout autre moment ou toute autre occasion convenus entre les autorités compétentes."*

[92] **Article 12-3 et Suivants** : " 3. *L'autorité d'exécution prend la décision relative à la reconnaissance ou à l'exécution de la décision d'enquête européenne dès que possible et, sans préjudice du paragraphe 5, au plus tard 30 jours après la réception de la décision d'enquête européenne par l'autorité d'exécution compétente. 4. Sauf s'il existe des motifs de report au titre de l'article 15 ou si l'État d'exécution est déjà en possession des éléments de preuve mentionnés dans la mesure d'enquête visée par la décision d'enquête européenne, l'autorité d'exécution exécute la mesure d'enquête sans tarder et sans préjudice du paragraphe 5, au plus tard 90 jours suivant la date à laquelle la décision visée au paragraphe 3 a été prise. 5. S'il n'est pas possible, dans un cas spécifique, pour l'autorité d'exécution compétente de respecter le délai indiqué au paragraphe 3 ou la date spécifique indiquée au paragraphe 2, elle en informe sans tarder l'autorité compétente de l'État d'émission par tout moyen disponible, en indiquant les raisons du retard et une estimation du temps nécessaire pour prendre une décision. Dans ce cas, le délai visé au paragraphe 3 peut être prorogé de 30 jours maximum"*

[93] Daskal, Jennifer, A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right , février 2016

[94] Par exemple, l' acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l' Union européenne , la convention d'entraide judiciaire en matière pénale entre les États membres de l'Union européenne ; Convention européenne d'entraide judiciaire en matière pénale (STCE n°030) ; et d'autres accords bilatéraux ou multilatéraux.

[95] Directive 2013/40 du Parlement et d Conseil relative aux attaques contre les systèmes informatiques remplaçant la décision-cadre 2005/222/JAI, https://cdre.eu/82-documentation-en-ligne/justice/droit-penal-materiel/1080-directive-2013-40-ue-du-parlement-europeen-et-du-conseil-du-12-aout-2013-relative-aux-attaques-contre-les-systemes-d-information-et-remplacant-la-decision-cadre-2005-222-jai-du-conseil

définitions sur les données informatiques[96], un système informatique[97], l'atteinte illégale à l'intégrité d'une donnée[98], etc. Cette directive précise également au niveau du paragraphe 24 de son préambule la nécessité pour les Etats membres de « transmettre à Europol et à son Centre européen de lutte contre la cybercriminalité des informations sur le mode opératoire des auteurs d'infractions, afin que ces agences puissent établir des évaluations de la menace et des analyses stratégiques en matière de cybercriminalité »[99].

Il existe certains textes qui n'ont pas un lien étroit avec la collecte des éléments de preuve électronique dans le cadre de la cybercriminalité, mais qui y contribuent. C'est le cas entre autres du Règlement européen pour la protection des données à caractère personnel, dont le chapitre V traite du transfert à l'étranger des données personnelles[100].

L'Union conclue également des accords bilatéraux avec ses partenaires extérieurs. Se trouve en premier plan, le traité d'assistance judiciaire (*mutual legal assistance treaty,* MLAT) qui permet de faire une demande aux fournisseurs de services des USA afin que ceux-ci mettent à disposition des services et agences de l'Union des informations nécessaires à la poursuite d'une action qui relève du champ de compétence de cette organisation. L'exécution de ce traité est souvent lente, c'est ce qui a poussé le conseil de l'Union, à la suite d'une importante affaire[101] qui a conduit au vote du *Cloud Act* aux Etats unis, a mandaté en 2018 la Commission européenne à négocier un accord avec ce pays afin de permettre un traitement accéléré des

[96] Article 2 de la directive 2013/40 relative aux attaques contre les systèmes informatiques
[97] Ibid., article 3
[98] Ibid., article 5
[99] Paragraphe 24 de la directive suscitée « *Il est nécessaire de recueillir des données comparables sur les infractions prévues dans la présente directive. Des données pertinentes devraient être mises à la disposition des agences et organes spécialisés compétents de l'Union, comme Europol et ENISA, en fonction de leurs missions et de leurs besoins en information, afin d'avoir une vision plus complète du problème de la cybercriminalité et du niveau de sécurité des réseaux et de l'information au niveau de l'Union et de permettre ainsi de formuler une réponse plus efficace. Les États membres devraient transmettre à Europol et à son Centre européen de lutte contre la cybercriminalité des informations sur le mode opératoire des auteurs d'infractions, afin que ces agences puissent établir des évaluations de la menace et des analyses stratégiques en matière de cybercriminalité, conformément à la décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol). La communication d'informations peut aider à mieux comprendre les menaces actuelles et futures et contribuer ainsi à ce que des décisions plus appropriées et mieux ciblées soient prises pour combattre et prévenir les attaques contre les systèmes d'information*. »
[100] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
[101] Affaire Miscrosoft : il s'agit d'une affaire de trafic de stupéfiant. Un juge américain a en effet ordonné en 2013 à la société Microsoft de lui livrer les emails d'un suspect, situés dans le *cloud*, le serveur étant en Irlande. Microsoft s'y est toutefois refusée, car la loi américaine de 1986 fondant l'injonction du juge (*Stored Communications Act*, SCA) n'avait pas d'effet extraterritorial selon elle. La Cour d'appel a confirmé ce point de vue, estimant que la loi SCA ne s'appliquait qu'aux données stockées sur le territoire des États-Unis. Le gouvernement américain a alors saisi la Cour Suprême en octobre 2017, cette dernière étant censée rendre son jugement en juin 2018. Entre temps, le Président américain Donald Trump a pris toutefois le juge de vitesse, en incluant le *Cloud Act* (*clarifying lawful overseas use of data act*) dans le projet de loi fédérale sur le budget 2018, soit 32 pages noyées dans plus de 2000 pages … Le Congrès avait déjà tenté à deux reprises de modifier la loi SCA de 1986, mais sans succès (projets de « Loi sur l'accès aux données stockées à l'étranger », LEADS Act, de 2015 et loi sur la protection des communications internationales, ICPA, en 2017). Cette importante loi a ainsi été adoptée sans examen spécifique, profitant de l'adoption globale de la loi de finances

échanges d'informations entre les deux systèmes. C'est exactement le fondement du projet *E-evidence* qui est actuellement en cours de négociation entre les deux puissances[102].

D'un autre côté, l'Union établit actuellement un projet de règlement visant à faciliter l'accès à des données sur injonction européenne[103]. Les règles de ce nouveau projet qui ont été rendues publiques dans un instrument d'orientation générale du 11 juin 2019[104] affichent un besoin utilitaire pour l'Union de créer une injonction européenne de préservation et de conservation dans le cadre de l'établissement d'une preuve électronique, peu importe le lieu de localisation des données recherchées. Ces données peuvent être de toutes catégories et donc concernées les données d'accès relatives aux abonnées, aux transactions et au contenu. Il est exigé dans ce texte une liste de conditions de fond et de forme d'émission et d'exécution de cette injonction[105], un peu comme c'est le cas dans le cadre d'une demande d'extradition classique. Ce projet qui est à l'image d'une loi américaine de 1986 fondant l'injonction du juge (*Stored Communiactions Act,* SCA), a la particularité de fixer le seuil d'exécution d'une injonction européenne à 10 jours, délai record qui peut être réduit à 6 heures dans les cas d'extrême urgence[106]. De plus, les entreprises visées par une injonction européenne qui s'opposeront à son exécution se verront sanctionner jusqu'à 2% de leur chiffre d'affaires annuel mondial pour l'exercice précédent[107].

Enfin, concernant les traités multilatéraux, il est primordial de compter les dispositions de la Convention de Budapest sur la cybercriminalité, qui est un texte de référence en matière de lutte contre la cybercriminalité à l'échelle internationale. Ces dispositions évoquent les axes d'orientations voulus par les Etats membres dans le cadre de la politique de collecte des éléments de preuve pour la lutte contre la cybercriminalité transfrontalière. Ont été mises en lumières, les dispositions des articles 16 à 18 qui traitent de la conservation des données stockées, la conservation et la divulgation rapide des données relatives au trafic, de l'article 19 relatif à la perquisition des systèmes et la saisie de donnée informatique et les dispositions des articles 20 et 21 qui traitent de la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu. Les dispositions des articles 23 à 34 de cette convention invitent les Etats à agir, par le biais de leurs autorités judiciaires et services de police, dans un but coopératif, afin de permettre à établir la preuve électronique, sans toutefois mener d'enquêtes et de perquisitions transfrontalières. Les informations obtenues doivent être rapidement communiquées. L'article 35 de cette Convention instaure un réseau de contacts H24/7 afin de prêter une assistance immédiate et permanente aux investigations en cours.

---

[102] https://ec.europa.eu/info/sites/default/files/placeholder.pdf

[103] Règlement relatif à l'accès transfrontière aux preuves numériques : le conseil arrête sa position, Veronica Huertas Cerdeira, https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/, 7 décembre 2018

[104] https://data.consilium.europa.eu/doc/document/ST-10206-2019-INIT/en/pdf

[105] Articles 5, 6 et Suivants du règlement relatif à l'injonction européenne de préservation et européenne

[106] Règlement relatif à l'accès transfrontière aux preuves numériques : le conseil arrête sa position, Veronica Huertas Cerdeira, https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/, 7 décembre 2018

[107] *Ibid.*

Par ailleurs, cette convention a été complétée par un premier protocole additionnel ouvert à la signature le 28 janvier 2003 à Strasbourg, et dont le but était de réprimer les actes racistes et xénophobes commis en ligne[108]. Ce protocole prévoit en son article 8-2, les mêmes mesures quant à la collecte des informations telle que prévue dans la convention[109]. Ayant pour objectif le renforcement de la coopération, le Conseil de l'Europe a en outre autorisé la commission à négocier avec le gouvernement américain un deuxième protocole[110]. La rédaction de ce projet a été clôturée et approuvée le 28 mai 2021 par le Comité de la convention sur la cybercriminalité (T-CY) à l'issu de sa 24e session plénière[111]. Au niveau de son chapitre 2, les acteurs de ce projet exhibent plusieurs mesures dont notamment le fait de donner effet dans les meilleurs délais aux injonctions d'une partie ordonnant la communication accélérée des informations sur un abonné ou un trafic, de divulguer les informations stockées en cas d'urgence, etc.

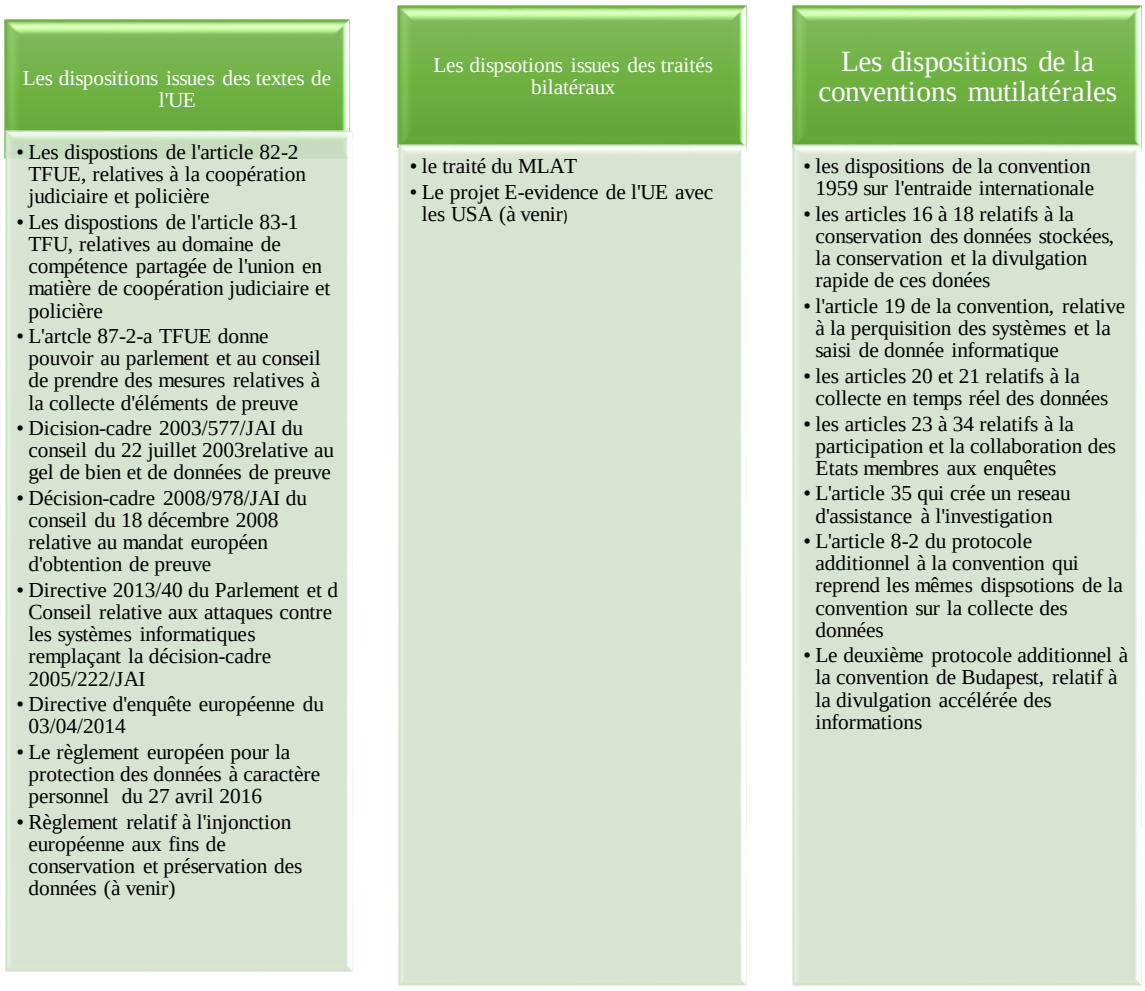
OBJ

[108]Protocol additionnel, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2014/09/protocole_de_strasbourg_du_28_janvier_2003_additionnel_a_la_convention_de_budapest_du_23_novembre_2001_-_incrimation_dactes_raciste_et_xenophobe_commis_par_le_biais_de_systemes_informatiques.pdf

[109] Article 8-2 les Parties étendent le champ d'application des mesures définies aux articles 14 à 21 et 23 à 35 de la Convention, aux articles 2 à 7 de ce Protocole.

[110] https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/pdf

[111] https://rm.coe.int/t-cy-2020-7-fr-pdp-protocol-v3t-approuve-par-le-tcy-/1680a2bb10




## § 2 : <u>La charge de la preuve d'une cybercriminalité</u>

En matière pénale, la présomption d'innocence voudrait que toute personne poursuivie pour une infraction soit innocente jusqu'au moment où sa culpabilité est établie devant une juridiction compétente et équitable[112]. Ce principe consacré par les philosophes des lumières a pour corolaire le fait que la charge de la preuve incombe à la partie poursuivante. En conséquence, la répression d'une quelconque forme de cybercriminalité mobilisera l'office de l'autorité judiciaire de poursuite (le parquet) qui sera appuyée par plusieurs services

[112] Article préliminaire du CPP issu de la loi du 15 juin 2000,
Article 11 déclaration universelle des droits de l'homme et du citoyen

opérationnels internes et externes (**A**), lesquels utilisent pour cette mission différentes ressources informatiques mises à leur disposition (**B**).

### *A. Les acteurs*

Deux catégories d'acteurs interviennent dans la constitution de la preuve d'une infraction cyber : les intervenants internes (**1**) et ceux relevant de la coopération internationale (**2**).

#### 1) Les intervenants internes

On retrouve au premier plan les magistrats cybers référents du parquet et de l'instruction des juridictions interrégionales, et les magistrats spécialisés de la section J3 du parquet de Paris, du pôle d'instruction du Tribunal de Grande Instance et de la Cour d'Appel de Paris. Ayant une connaissance générale de la matière, les magistrats référents cybers assurent la coordination, le suivi, la veille juridique et dans certains parquets, la centralisation dans les procédures mises en œuvre dans le domaine de la cybercriminalité[113]. Par ailleurs, le Tribunal de Paris bénéfice depuis le 3 juin 2016 d'une compétence concurrente nationale en matière d'atteintes aux STAD et crime de sabotage informatique[114]. Les effectifs de la section J3 sont très limités. Elle est aminée par deux magistrats, un assistant spécialisé et un greffier

Les autorités judiciaires ordonnent et suivent dans la légalité l'exécution des moyens de preuves, et leur bras opérationnel est la Police judiciaire, la Gendarmerie et les instituts spécialisés dans les attaques informatiques. En effet, la répression de la cybercriminalité est loin d'être une affaire simple lorsqu'elle nécessite par exemple d'extraire les preuves électroniques d'un outil informatique codé ou de s'assurer de leur fiabilité et leur intégrité. Seuls les techniciens, experts, enquêteurs ou personnes qualifiées ont pareille compétence. Ainsi, il existe au sein de la Police judiciaire et de la Gendarmerie nationale une kyrielle d'entités opérationnelles dont les missions sont incontournables dans le domaine de la constitution de la preuve numérique en cybercriminalité. On y trouve :

- *La SDLC*

Cette une unité de police importante de la lutte contre la cybercriminalité en France. Elle assure non seulement les missions de prévention et de répression mais aussi constitue un lieu de définition des stratégies à mettre en œuvre dans les domaines de l'opérationnel, de la

[113] Rapport « protéger les internautes », 2016, P.116

[114] Article 706-72-1 C du Code de procédure pénale

formation et de la prévention au profit du grand public et du tissu économique. Elle est composée d'un bureau de coordination stratégique, d'un bureau de l'internet, d'un bureau de la formation à la lutte contre la cybercriminalité, de l'office central de lutte contre les infractions liées aux technologies de l'information et de la communication (OCLCTIC), ainsi que d'une division de l'anticipation et de l'analyse. La SDLC a par exemple joué un rôle de premier plan dans le démantèlement d'un réseau de trafic sur internet dans l'espace francophone. Appelé « French Deep Web market » ou la main noire, ce réseau assure la mise en relation entre vendeurs de produits et services illicites sur Internet. Il peut s'agit des produits stupéfiants, des armes, des faux documents, des données bancaires frauduleusement captées, outils de piratage informatique, etc. En 2019, les services de la SDLC et de la cyber-douane ont ciblé ce réseau et les recherches ont amenées à Nice, Bordeaux, Lisieux et Metz, et aboutissaient à l'interpellation de deux modérateurs (encore appelés des *escrows* dans le jargon des internautes du marché noir), lesquels ont été mis sous contrôle judiciaire[115].

- *L'Office Central de la Lutte Contre les infractions commises contre les TIC*

Cet office est chargé d'animer et de coordonner la mise en œuvre opérationnelle de la lutte contre la cybercriminalité. Elle est animée par une section internet, une section opérationnelle, une section d'assistance technique de recherche et développement et une section relation internationale. Cet office a récemment contribué à l'arrestation de plusieurs délinquants à la suite du piratage d'une plateforme d'échange de cryptomonnaie de la société *Gatehub.* En effet, les délinquants ont exploité les failles de sécurité du système et ont pris le contrôle de plusieurs portefeuilles appartenant aux clients de cette entreprise. Le préjudice était évalué à 8 millions d'euros. Saisi de l'affaire par la police slovène, les services de l'OCLCTIC ont donc sûr analyser les données des *wallets*[116] et découvrir les personnes qui ont contribué à l'écriture du script utilisé pour opérer le piratage[117].

- *La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI)*

La brigade d'enquêtes sur les fraudes aux technologies de l'information a été créée en 1994 et comprend des groupes d'enquêtes et un groupe d'assistance. Elle a pour mission d'élucider les crimes et délits informatiques. Sa compétence territoriale comprend Paris et les départements de la petite Couronne (92, 93 et 94). Cette entité ne traite pas des escroqueries mais enquête sur les atteintes aux STAD, la contrefaçon, les réseaux téléphoniques, la captation frauduleuse de programme TV payants, le défaut de sécurisation des données personnelles.

- *Le Service Central de l'Information et des Traces Technologiques **(SCITT)***

[115] Rapport annuel sur la cybercriminalité organisée en France, Direction générale de la PN, et de gendarmerie nationale, Sirasco, éd., 2019

[116] Portefeuille en anglais, en cryptomonnaie, il s'agit d'un procédé de stockage sécurisé physique ou numérique de cryptomonnaie

[117] Rapport annuel sur la cybercriminalité organisée en France, Direction générale de la PN, et de gendarmerie nationale, Sirasco, éd., 2019

Le service central de l'information et des traces technologiques (SCITT) de la police technique et scientifique est une composante de la police scientifique et technique de la PJ. Animée par des techniciens n'ayant pas le statut d'enquêteur, ce service a été créé en 2001 en remplacement du laboratoire d'analyse et du traitement du signal. Il assure le suivi et la gestion de l'activité des services territoriaux dans le domaine de l'informatique et des traces technologiques. Il consulte, exploite ou extraire le contenu des appareils numérique réquisitionnés dans le cadre d'une enquête pénale. A la PJ de Limoges, ce service est animé par un personnel très limité en nombre mais avec des compétences qualifiées en l'informatique.

- *Le réseau des Investigateurs en cybercriminalité (ICC)*

Le réseau d'ICC a été créé en 2005 en remplacement à son ancêtre l'ESCI (Enquêteurs Spécialisés en Criminalité Informatique), créé en 1999. Les investigateurs en cybercriminalité de la Police nationale (PN), actuellement au nombre de 451 repartis sur l'ensemble du territoire national au sein des directions de la PN, ont des compétences pour analyser et catégoriser les infractions pénales liées à la cybercriminalité, réaliser des copies et des analyses de supports numériques dans le respect de la préservation et de l'intégrité de la preuve, procéder à des constatations techniques et diligenter des enquêtes dans le domaine des technologies de l'information et de la communication. Sur une scène de crime, les ICC sont relayés par les primo intervenants. Ces policiers sont en première ligne et confrontés aux actes courants d'enquêtes en milieu numérique. Au sein de la PJ de Limoges, il n'existe qu'un seul ICC lequel est spécialisé uniquement dans les fraudes bancaires.

- *Le centre Technique d'Assistance (CTA)*

C'est une unité de police dont la mission est de mettre au clair les données ayant subi une transformation particulière rendant complexe leur intelligibilité. Ce centre a été créé par le décret n°2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance. Selon l'article 2, ce centre est l'organe visé au niveau de l'article 203-2 et suivants du code de procédure pénale, relatif au déchiffrement. Ses interventions sont couvertes par le secret de la défense nationale[118].

- *Le Centre de lutte Contre les Criminalités Numériques (C3N)*

C'est une unité du pôle judiciaire de la gendarmerie nationale qui a pour vocation de traiter directement les questions en rapport avec la cybercriminalité et les analyses numériques. Ce centre contient un département de prospective et d'animation territoriale composé d'un guichet unique (GUTI) qui assure une assistance hotline H24 aux unités territoriales, d'un centre national d'analyse des images de pédopornographie dont la mission est d'identifier les victimes et auteurs des contenus à caractère pédopornographique. Les enquêteurs de ce centre sont

[118] Article 3 du décret

formés à l'enquête sous pseudonyme sur Internet. Le centre s'appuie également sur les enquêteurs locaux (cyber référents) et les spécialistes départementaux (les cyber Ntech)[119].

- *Les correspondants en technologie numérique (C-NTECH)*

Ce service a été créé par une Circulaire du 16 février 2008[120] et repartie dans les brigades de recherche de la gendarmerie. Les enquêteurs de ce service ont pour missions de recevoir, dans leurs localités respectives, les plaintes des victimes, effectuer des actes techniques simples (perquisition, mesures conservatoires et examens) grâce aux outils qu'ils disposent et mener avec l'assistance systématique des Ntech des actes d'enquêtes. La formation des C-NTECH dure trois (03) jours et est organisée au niveau des régions. En effet, ils reçoivent une formation de base dans le domaine informatique (théorie générale, micro-ordinateurs, supports), juridique (un cours d'introduction au droit, la perquisition informatique, recherche en source ouverte, escroquerie sur Internet, la fraude bancaire) et dans le domaine de la téléphonie (téléphone mobile, analyse de la carte SIM).

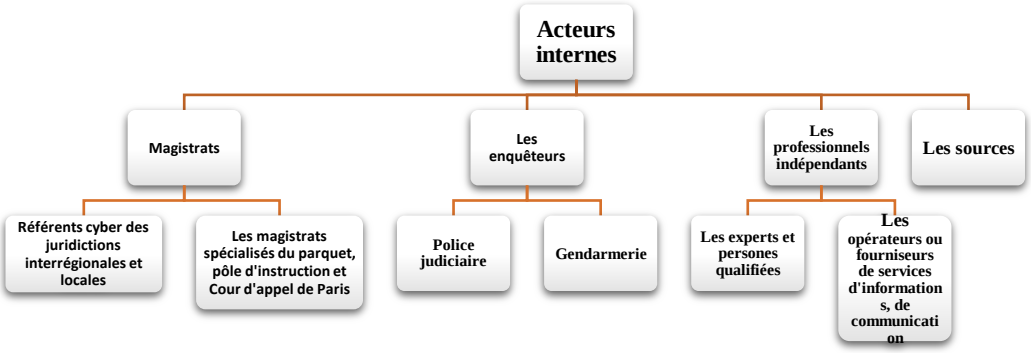
- *Les enquêteurs en technologie numérique (NTECH)*

Cette mission a été créée en 2001 et repartie dans plusieurs secteurs d'enquête de la gendarmerie. Leur mission consiste entre autres à animer le réseau des C-NTECH, effectuer des investigations ciblées sur Internet, administrer la base nationale des contenues pédopornographiques issus des enquêtes de la police et de la gendarmerie, en lien avec INTERPOL et les partenaires étrangers, et surveiller principalement les sites internet en vue de détecter et caractériser les cybers infractions, etc[121].

A côté des autorités policières et judiciaire, viennent apporter aussi leur concours à l'enquête les partenaires internes du secteur privé. Ce sont généralement les fournisseurs de services d'informations et de communications qui ont d'ailleurs une obligation, à la demande des autorités judiciaires, de fournir les informations relatives au trafic de leurs abonnés. Le règlement européen sur la protection des données personnelles oblige les entreprises à informer dans un délai de 72 heures l'autorité indépendante (CNIL en France) lorsqu'elles ont fait l'objet d'une attaque informatique. Sont également retrouvés les experts[122] en l'informatique assermentées dont les interventions sont capitales face à des cas complexes de cybercriminalité.

[119] Le centre de lutte contre les criminalités numériques, SCRCGN, gendarmerie.interieur.gouv.fr
[120] Circulaire n° 16000/DEF/GEND/OE/SDPJ/PJ du 16 février 2008
[121] Ibid.
[122] L'expert est une personne désignée par ordonnance du juge d'instruction ou toute juridiction de jugement afin de répondre à une question d'ordre technique. Son régime est assuré au niveau des articles 156 et suivants du CPP. Il est choisi sur une liste disponible dans les cours d'appel et de cassations, sauf décision motivée du magistrat. Dans ce dernier cas, il doit prêter serment.

Par ailleurs, il existe au sein de la police et même de la gendarmerie, une catégorie privilégiée de personnes dont les missions aident plus ou moins à l'enquête. Il s'agit des « sources ». Ce sont des individus qui n'ont aucun statut officie mais qui, en raison de leur parcours de délinquance, ont acquis certaines connaissances ou sont affiliés à certains réseaux dont l'accès est le plus souvent difficile aux enquêteurs. Ainsi, lorsque ces personnes sont par exemple condamnées pour avoir commis des agissements pénaux, elles négocient leur liberté contre une mise à disposition des autorités des informations pouvant servir à démanteler, le cas échéant, un réseau de cyber-délinquants. Lorsqu'elles sont hors du champ de poursuite judiciaire, ces personnes peuvent continuer à travailler sous anonymat avec les enquêteurs moyennant une certaine rémunération.




### 2) Les intervenants relevant de la coopération internationale

En raison du caractère intrinsèquement transfrontière de la cybercriminalité, la sollicitation de la coopération internationale en vue de la collecte des éléments numériques s'avère une utilité incontestable. La seule condition fondamentale pour un aboutissement d'une demande de collaboration ou d'entraide à l'enquête est l'existence préalable d'un accord entre les pays avec de surcroit, au sein de l'UE, d'une décision d'enquête[123]. A ce titre, l'Union européenne, ayant compétence pour intervenir dans le domaine de la criminalité informatique, met à la disposition des Etats membres son arsenal opérationnel dans le cadre de cette lutte contre la criminalité organisée. On retrouve notamment les deux principales agences de l'UE (Europol et Eurojust), le réseau judiciaire, les équipes d'enquêtes communes et les magistrats de liaison.

Eurojust, est une agence européenne créée dans le cadre du troisième pilier de l'union (Justice et Affaire intérieure)[124], dont la mission est d'appuyer et renforcer la coordination et la coopération entre les Etats dans le cadre de poursuites pour une criminalité transfrontalière affectant plusieurs Etats[125]. Dans un récent rapport du Conseil sur cette agence, publié au

[123] Article 694-15 et 694-16 du CPP
[124] Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust, modifiée en dernier lieu par la décision 2003/659/JAI du Conseil du18 juin 2003
[125] Article 85 du TFUE

journal officiel le 09 décembre 2019, au niveau du paragraphe 10, il a été conclu que cette agence devait veiller à l'amélioration de l'échange des informations et assurer l'interopérabilité entre les systèmes d'information de l'Union européenne dans le plein respect des exigences en matière de protection des données, dans le but de renforcer l'échange rapide, fiable et sécurisé d'informations et d'éléments de preuve entre les agences et les organes tels qu'Europol, l'OLAF[126], Frontex[127] et le Parquet européen. Eurojust a en effet un rôle essentiel à jouer pour faire en sorte que les données nationales puissent faire l'objet de références croisées, afin de permettre une liaison entre différentes enquêtes pénales. C'est pourquoi le Conseil soutient qu'il était nécessaire de veiller à ce que les membres nationaux d'Eurojust aient accès au système d'échange de preuves numériques établi par la Commission et exploité par les États membres[128]. Ce Conseil invite par cette occasion Eurojust à mettre en œuvre tout son pouvoir afin d'assurer l'échange d'informations sensibles entre les Etats membres à travers le réseau des magistrats de liaison[129]. L'implication de cette agence en vue de faciliter l'obtention des traces numériques susceptibles de constituer une preuve pénale était très une importante au regard de son efficacité.

Quant à l'Europol, cette agence a été créée par une convention dans le cadre du troisième pilier en 1995, mais a subi plusieurs réformes jusqu'à un règlement de 2016, règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs,[130] lequel constitue désormais son fondement juridique. Organe répressif de l'Union, il intervient dans la constitution des éléments de preuves numérique de par sa mission principale de développer la coopération policière de l'Union en aidant à faciliter les mesures d'enquêtes entre les Etats (article 87-2-a du TFUE). L'une de ses principales bases de données est le système d'information Europol, lequel constitue source d'informations sur les infractions et les délinquants. Ce système alimente plusieurs autres systèmes des Etats et permet aussi une consultation directe par les autorités en charge des enquêtes dans chaque pays membre. En outre, le règlement de 2016 est venu renforcer l'obligation de transmission des informations des Etats membres vers les agences européennes. Pour les besoins de ses missions et notamment afin d'être plus réactive face aux menaces, Europol a créé des unités spécialisées. Par exemple, elle a créé un centre européen de lutte contre la cybercriminalité (EC3) en 2013[131] dont la mission est entre autres d'apporter son soutien aux services d'enquête dans la lutte contre la fraude bancaire, la pédopornographie et les escroqueries financières en ligne, et les attaques contre les systèmes. Ce centre a accueilli en son sein en 2014 une nouvelle unité dénommée J-CAT (Joint Cybercrime Action Taskforce), dont la mise en place consiste à

[126] L'office européen de lutte antifraude
[127] Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des Etats membres de l'Union européenne
[128] Conclusions du Conseil sur Eurojust: l'unité de coopération judiciaire de l'union européenne à l'ère numérique2019/C 412/04ST/12285/2019/INIT, https://eurlex.europa.eu/legalcontent/FR/TXT/?uri=CELEX%3A52019XG1209%2802%29&qid=1625574487088, paragraphe 10
[129] *Ibid*., paragraphe 11
[130] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), https://eur-lex.europa.eu/eli/reg/2016/794/oj
[131] https://fr.wikipedia.org/wiki/Centre_europ%C3%A9en_de_lutte_contre_la_cybercriminalit%C3%A9

renforcer la lutter par la facilité d'échange d'informations. Les enquêteurs de cette unité surveillent les nouvelles méthodes inventées par les cybercriminels. Il y a une priorité sur les réseaux de machin zombies. Il est également prévu d'intégrer des procureurs à cette cellule pour accélérer les échanges d'information. Europol est également appuyé pour leur savoir-faire dans le domaine de la collecte de la preuve numérique, par l'agence européenne de la sécurité informatique des réseaux (ENISA), le CERT[132] de l'Union européenne et le Collège Européen de Police (CEPOL)[133] qui fait figure de formateur des enquêteurs de l'Europol.

Le Réseau Judiciaire de l'Union européenne constitue un autre bras opérationnel de l'Union dont les missions contribuent effacement au renseignement sur la criminalité organisée qui relève du champ de cette organisation. Ce réseau est principalement composé d'autorités judiciaires mais aussi d'autres autorités ayant des compétences spécifiques. Le but de ce réseau est d'identifier un interlocuteur direct et privilégié dans chaque pays membre afin de faciliter l'échange d'informations. Ainsi, en matière de cybercriminalité organisée, ce réseau servira d'appui technique à la mise en place d'une demande d'entraide pénale. En matière policière, il existe aussi un réseau judiciaire des officiers de police de liaison, détachés des autorités répressives des Etats membres.

Les équipes communes d'enquête, elles ont été instituées dans le cadre d'une décision-cadre de 2002 qui a fait l'objet de transposition dans l'ordre interne par la loi Perben II de 2004. Une équipe commune d'enquête peut être créée par une autorité judiciaire compétente avec l'accord du ministre de la Justice et celui des autres Etats membres lorsqu'il y a lieu d'effectuer une enquête d'envergure internationale sur des infractions exigeant une action coordonnée et concertée entre les Etats[134].

Enfin, l'autre acteur européen qui joue aussi un rôle partiel dans la collecte des éléments de preuve dans toute procédure pénale d'envergure internationale, est le magistrat de liaison. Le magistrat est une autorité judiciaire détachée par un Etat sur le territoire d'un autre, dans le but d'assurer une liaison entre les deux Etats. Le mécanisme de magistrat de liaison a été instauré par une Action commune de 1996 dans le cadre du troisième pilier. En cybercriminalité organisée, ce magistrat permet d'assurer un échange d'information sur le système coopératif des Etats non-membres de l'Union. Il constitue concrètement un point d'attache crucial pour assurer l'information des enquêteurs nationaux ou européens sur toutes les questions d'ordre juridique relatives, par exemple, à l'accès aux données numériques à caractère personnel de son pays d'accueil, au mode opératoire d'une forme particulière de cybercriminalité, etc.

En dehors de l'Union, la coopération internationale en matière de lutte contre la cybercriminalité implique aussi la participation de plusieurs autres organes diversifiés de par

[132] Computer Emergency Response Team : c'est un centre spécialisé dans la demande et le traitement des attaques contre les systèmes informatiques, https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/
[133] Le CEPOL contribue à créer une Europe plus sûre en facilitant la coopération et en permettant l'échange de connaissances entre les agents des services répressifs des États membres de l'UE et, dans une certaine mesure, de pays tiers, sur des questions découlant des priorités de l'Union dans le domaine de la sécurité, en particulier du cycle politique de l'UE sur la grande criminalité et la criminalité organisée.
[134] Article 695-2 et S. CPP

leur compétence. C'est le cas d'Interpol qui fait figure de police internationale et dont les missions consistent à assister les Etats dans le cadre des enquêtes pénales à dimension internationale. Dernièrement, lors de la 8e conférence Interpol-Europol qui a réuni plusieurs Etats autour des risques de la cybercriminalité liée au Covid19, Interpol a suggéré d'agréger les informations nationales su la cybercriminalité au niveau international afin de renforcer la coopération dans ce domaine. Il s'est même proposé pour conduire cette politique.

Ensuite, la corporation ICANN (*International corporation for assignated names and numbers)* constitue un autre acteur très important dont les bases de données sont d'une utilité capitale pour les enquêteurs, notamment dans le cadre de la gestion des domaines de connexion et d'attribution des adresses IP. En effet, les missions d'ICANN consiste principalement à gérer Internet dans le monde entier. Elle coordonne l'affectation et l'attribution dans la zone racine du système de noms des domaines, assure l'enregistrement des noms de domaine de second niveau dans les domaines génériques de premier niveau, facilite la mise en marche et l'évolution du système des serveurs du nom des racines du DNS, coordonne l'allocation au plus haut niveau des adresses IP et des numéros pour les systèmes autonomes et enfin, coopère avec d'autres organismes afin de mener à bien ses missions. L'ICANN détient une base de données dénommée WHOIS qui rassemble les informations sur les domaines enregistrés, y compris les informations sur leurs titulaires[135].

Enfin, la recherche des traces numériques dans le cadre d'une cybercriminalité connait aussi le concours de associations internationales. C'est le cas notamment de l'association *Pishing Initiative* qui réunit les grands groupes tels que Microsoft, PayPal et le Certlexsi. Cette association se donne pour mission d'aider à se prémunir contre les tentatives d'hameçonnage, les attaques informatiques. Pour ce fait, elle met à la disposition de leurs clientèles la possibilité de signaler les URL, c'est-à-dire les adresses électroniques qui dirigent vers les sites malveillants.

### ***B. Les outils disponibles***

La recherche des éléments de preuve numérique fait appel à l'usage de plusieurs outils informatiques, lesquels peuvent différer selon le type de cyber infraction ou de la nature de l'opération à effectuer. A ce titre, on rencontre les outils de signalement qui servent à dénoncer les publications à contenu illicite. Telle est par exemple la vocation de la plateforme d'harmonisation, d'analyse, de recoupement, d'orientation des signalement (PHAROS). Cet outil permet aux enquêteurs alertés d'un fait illicite commis en ligne (escroquerie, apologie au terrorisme) d'enregistrer les faits dénoncés et si possible de rechercher les auteurs grâce aux données d'identification indirecte (adresse IP, avatar…). En 2017, cette plateforme a enregistré plus de 180.000 dénonciations[136], en 2019 ce chiffre est porté à 228.000 signalements majoritairement liés à l'escroquerie en ligne. Ensuite, la plateforme de plainte THESEE (traitement harmonisé des enquêtes et des signalements pour les E-escroqueries) lancée dans le dernier trimestre de 2020 a permis de réorienter Pharos afin de mieux recouper les

[135] L'ICANN et les problématiques d'abus de DNS, séminaire cyber référents, Laurent Ferrali, 112 juin 2021
[136] https://www.loi1901.com/intranet/a_news/index_news.php?Id=2630

informations et lancer les enquêtes d'envergure[137]. Concrètement, cette plateforme permet la prise en ligne des plaintes, elle facilite l'identification des auteurs des infractions et de leurs victimes associées, grâce à l'analyse par des experts de la police judiciaire et à la coopération internationale judiciaire indispensable dans ce domaine délictuel[138].

Ensuite, l'investigation numérique en matière de cybercriminalité nécessite l'usage de logiciels de performance, afin d'extraire des données numériques. Dès lors, dans le domaine de l'informatique, les experts utilisent les logiciels comme Xways, Encase, Forensic explorer ou Axiom[139].

Xways est un logiciel dont les fonctionnalités sont souvent sollicitées en matière d'extraction de données de tout type mémoire et de visualisation d'images sur l'écran. Ce logiciel est utilisé par les enquêteurs de la SDLC, les ICC, les techniciens de la criminalistique de la police scientifique afin d'analyser la structure complète de l'arborescences à l'intérieur d'une image, même lorsqu'elle est segmentée, visualiser et faire la copie physique d'une mémoires RAM et de la mémoire virtuelle des processus lancées[140]. Il a également la puissance technique de reconstruire les données détruites ou supprimées. Il partage les mêmes fonctionnalités de sécurité que les logiciels *Encase*, *forensic explorer* et *axiom*. C'est le cas par exemple de la conservation des données à l'état brut ainsi que de la gestion de la métadonnée.

En matière de téléphonie, l'investigation numérique amène également les enquêteurs à utiliser certains logiciels adaptés. C'est le cas en occurrence du logiciel *Ufed* de la société Cellebrite et de *XRY* du startup MSAB. Ces logiciels permettent l'exploitation des mémoires des téléphones afin d'y découvrir toute sorte de données pouvant permettre aux enquêteurs de découvrir des informations utiles à une enquête. Ces logiciels ont également le potentiel de reconstituer les données supprimées d'un appareil téléphonique. Dans le cadre de mon stage à la Police judiciaire, j'ai pu assister à l'extraction des données d'une carte à puce grâce à ces deux logiciels. Concrètement, sur une carte SIM dont la norme résulte des travaux de l'Institut européen des standards de télécommunication (IEST), il est possible de lire grâce au XRY les données comme le nom de l'opérateur (SPN[141]), le numéro du mobile de l'abonné (MSISDN[142]), de série de la carte (ICCID[143]), le numéro identifiant de l'abonnement du mobile (IMSI[144]), le répertoire téléphonique, les messages textes effacés ou non, le journal des appels, les informations réseaux mémorisées sur la carte, etc. La difficulté reste le volume des données que le logiciel n'est pas capable de trier de façon à permettre de rendre un résultat dans un délai trop court.

Ensuite dans le domaine de la cryptomonnaie, *Chainalysis* et *Neutrino* sont les logiciels de main courante des experts qui leur permettent de détecter toute intrusion frauduleuse dans le système portefeuilles des clients. L'investigation sur le Darknet est, quant à elle, possible

[137] Lutte contre la cybercriminalité, DCPJ
[138] Lancement de THESEE, DCPJ, 2020
[139] Informations reçues d'un enquêteur de la SDLC, Monsieur Dominique Renard,
[140] https://www.tracip.fr/nos-produits/logiciels/x-ways-forensics/
[141] Service Provider Name
[142] Mobil Station International Subscriber Directory Number
[143] Integrated Circuit Card ID
[144] International Mobil Subscriber Identity

grâce au logiciel *GM search dark* conçu par la société Aleph Network. Ce programme permet de retrouver les traces numériques d'activités illégales commise via le réseau darkweb et aussi, le cas échéant, d'identifier les auteurs. Enfin *Icaccop. C'*est un logiciel de veille utilisé par les enquêteurs en cyber-pédopornographie afin de cibler les internautes qui mettent en lignes ou consultent habituellement les publications mise en ligne sur les sites de pédopornographie. L'utilisation de ce logiciel est soumise à une habilitation. A ce titre, à la police judiciaire de limoges seule une personne a cette habilitation.

Enfin, la loi permet également aux enquêteurs, sous le contrôle d'une autorité judiciaire, d'implanter des malwares dans le système des suspects pour infiltrer et faciliter la recherche de la preuve. Cela peut être possible notamment grâce aux fichiers cyborg.

## Chapitre 2 : La preuve numérique : le défi de sa constitution en matière cybercriminelle

L'investigation numérique est une opération très importante dans une procédure pénale portant sur des faits de qualifiés de cybercriminalité. A l'instar des autres domaines du droit pénal (meurtre, viol, empoisonnement, abus de biens sociaux, banqueroute, ...), les experts en cybercriminalité sont également investis à faire preuve de vigilance et de maitrise dans le domaine cybernétique sinon, la moindre anomalie peut entrainer l'annulation de toute la procédure, ce qui peut coûter des frais à l'Etat. Les services d'enquêtes ont développé une culture méthodologique classique afin de traiter les éléments de preuve numérique dont l'appréciation est laissée au libre arbitre du juge **(section 1)**. Pour autant, malgré l'observance rigoureuse de cette culture de méthodologie, il existe parfois plusieurs obstacles à la constitution de la preuve dans ce domaine, sans oublier le constat que certaines pratiques d'enquêtes peuvent aussi se révéler attentatoires à la privée des personnes suspectés **(section 2**).

### Section 1 : La constitution de la preuve numérique

Deux étapes sont généralement observées dans le cadre de l'établissement de la preuve numérique par les enquêteurs. La première est relative au procédé de collecte des informations (**paragraphe 1**) et la deuxième met en exergue le rôle d'appréciation du juge **(paragraphe 2**)

#### § 1 : Le procédé de la recherche des informations

Le procédé de la recherche ou de collecte consiste d'abord à collecter les informations numériques (**A**) et, ensuite, à procéder à leur stockage et préservation (**B**).

##### *A. La collecte et l'analyse des éléments destinés à constituer une preuve numérique*

Collecter les informations numériques dans le cadre d'une investigation numérique pénale suppose qu'on se trouve dans un contexte de flagrance, d'enquête préliminaire ou qu'on exécute une commission rogatoire technique. Dans l'un ou l'autre des cas, les enquêteurs sont amenés à réaliser sous la responsabilité de leur autorité judiciaire hiérarchique divers actes, allant de la perquisition informatique, l'implantation de virus informatique, l'apposition d'un mouchard, la mise en œuvre d'une injonction de communication à l'infiltration. Cela suppose également que ces intervenants aient une connaissance certaine de la forme de cybercriminalité sur laquelle ils doivent travailler.

Dans le cadre d'une perquisition informatique, conformément à l'article 56 du CPP, la collecte de données peut avoir lieu chez le propriétaire des lieux en présence de celui, ou dans les locaux de la Police. Au niveau international, la Convention de Budapest ajoute que la

collecte peut se faire en temps réel[145]. Il peut arriver des situations où les enquêteurs n'ont pas le code d'accès à un appareil ou que la personne refuse de le communiquer. Le fait de refuser de communiquer ce code est une infraction prévue par le CP. Cependant, les enquêteurs sont amenés à faire le maximum, autant que le mandat de perquisition leur permet, pour avoir accès au code et l'appareil perquisitionné. Dans le cas où ce code a été trouvé en l'absence du mis en cause sur les lieux de perquisition et que ce code a permis d'accéder à des données conservées en territoire étranger, la question s'était posée de savoir si la possession de ce code sans une autorisation particulière du juge des libertés et de la détention ne viciait pas la procédure[146]. En l'espèce, les enquêteurs de la police ont, dans le cadre d'une enquête préliminaire, effectué une perquisition informatique telle que prévue à l'article 57-1 du CPP. Une telle perquisition a été faite en l'absence du propriétaire du domicile et a permis de découvrir un code qui a servis d'accès à un serveur étranger (USA), lequel contenait des données utiles à l'enquête. Constatant ce vice procédural, les parties de la défense ont soulevé une exception de nullité de la procédure devant la Cour d'Appel, laquelle a rejeté la demande sur le fondement de l'article 32 de la convention de Budapest qui autorise les enquêteurs à accéder aux serveurs étrangers dans le cadre d'une perquisition informatique.

Insatisfaite de cette décision, la défense forme un pourvoi en cassation. Dans son pourvoir, elle expose que « la pénétration et la recherche de données sur un site internet, par les enquêteurs, à l'aide d'un code d'accès internet personnel, obtenu dans le cadre d'une perquisition, équivaut, s'agissant d'accéder à un espace privé ou clos, à une perquisition soumise, en enquête préliminaire, en absence de consentement de l'intéressé, à l'autorisation préalable du juge des libertés et de la détention »[147]. C'est-à-dire que, le pourvoi fait une analogie entre un serveur internet et un domicile physique dont la perquisition doit nécessiter, en enquête préliminaire, le consentement du propriétaire ou de l'autorisation d'un juge. Ainsi, le code ayant permis l'accès à ce serveur est comme une clé d'accès à un domicile. Cela étant, l'auteur du pourvoi soulève qu'il fallait d'une autorisation du juge, distincte de celle de la perquisition domiciliaire, afin de justifier l'usage du mot de passe. Le pourvoi soulève également le fait que, pour la procédure prévue à l'article 32 de la convention, il fallait mettre en place une procédure d'entraide pénale.

De son côté, la Cour de cassation a fait une interprétation casuistique des dispositions invoquées, en jugeant qu'« *il s'agissait d'une simple investigation et non d'une perquisition distincte exigeant une décision du JLD et que la seule domiciliation du site en cause aux USA ne justifiait pas la mise en œuvre d'une procédure d'entraide pénale* ». Cette solution à soulèvent plusieurs interprétations. D'abord, selon un auteur, cette solution évite aux juges des libertés et de la détention d'être envahis par une forte demande d'autorisation d'accès à plusieurs serveurs, dans le cadre d'une seule affaire[148]. Ensuite, cette décision vient élargir la

[145] Article 20 de la convention de Budapest
[146] Cass. Crim. 6 novembre 2013, n°12-87.130
[147] Les perquisitions « informatiques » à l'épreuve du principe de souveraineté dans un contexte de mondialisation de stockage de données, étude comparée en droit français et états-unien, Alexandre Rousselet-Magri, Cairn, P.666-667, https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2017-4-page-659.htm

[148] Ibid

compétence territoriale des autorités judiciaires mais de façon surprenante, étant donné que l'accès aux données est considéré comme un simple acte d'investigation dans le prolongement de la perquisition initiale, et non dans le cadre d'une nouvelle perquisition soumise à ses propres conditions de validité[149].

Quelques jours après cette décision, dans une autre affaire, la Cour de cassation semble réapproprier la même posture position mais cette fois-ci, en restant générale. Elle a jugé qu'était ***« régulière la saisie massive de données informatiques ; dès lors, d'une part, que ces dernières sont identifiées, inventoriées, et qu'elles ne sont pas étrangères à l'infraction ayant motivée la perquisition***, et, d'autre part, que les demandeurs, qui en ont reçu copie et ont ainsi été mis en mesure d'en connaitre le contenu, n'ont formulé aucune observation au moment où les opérations ont été effectuées et n'ont évoqué aucun élément de nature à établir que certains documents, en raison de leur objet, ne pouvaient être saisis[150] ». Il s'en déduit donc que, lorsque la personne dont le domicile est perquisitionné a été averti de la mesure et n'a fait aucune objection par à la saisie d'une donnée précise, son consentement est effectif et la perquisition est régulière.

Pour ce problème, la solution proposée dans le rapport « protéger les internautes » semble plus convaincante. Au niveau de sa recommandation n°42, les auteurs proposent au législateur de prévoir explicitement que la saisie effectuée dans le cadre d'une perquisition peut porter tant sur les terminaux et supports de stockages que sur les éléments pouvant permettre l'accessibilité aux différents systèmes informatiques (identifiant, méthode de déchiffrement…) et que lesdits éléments peuvent être utilisés par l'OPJ pour avoir accès aux données informatiques à condition d'en faire mention dans la procédure.

Ensuite, une fois l'accès à ce panel de donnée réussi, les enquêteurs vont s'appliquer à leur étude. Dans le fond, la méthode d'analyse demeure classique pour toutes les formes de cybercriminalité, et les enquêteurs font preuve d'une rigueur mesurée en s'assurant que les informations recueillies respectent les conditions de validité requises. L'analyse des données numériques se déroule de la manière chronologique suivante : la séparation, la prise en compte de l'échantillon, vérification du fonctionnement, la copie, l'interprétation et la rédaction.

- ***Séparation éventuelle de l'objet placé sous scellé en échantillon***

Cette étape est très importante, en ce qu'elle permet de déconnecter le téléphone portable ou l'ordinateur de tout réseau de connexion afin de le prémunir contre toute attaque extérieure de nature à entraver le contenu de la mémoire. Dans la pratique, par exemple, la criminalistique sépare la carte à puce du téléphone. Dès fois, ce dernier est exploité en étant complètement éteint. Par exemple, dans le cadre de l'étude du disque dur d'un téléphone ou d'un ordinateur ayant servir à échanger avec une victime de crypto-escroquerie, les enquêteurs vont démonter l'appareil, identifier les différentes mémoires de stockage par leurs éléments caractéristiques et ensuite, procéder à l'échantillonnage.

[149] Les perquisitions « informatiques » à l'épreuve du principe de souveraineté dans un contexte de mondialisation de stockage de données, étude comparée en droit français et états-unien, Alexandre Rousselet-Magri, Cairn, P.666-667, https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2017-4-page-659.htm
[150] Cass. Crim. 14 nov. 2013, n°12-87.346

- ***Prise en compte de l'échantillon et de son environnement, description de l'échantillon***

Cette étape permet de porter une attention particulière sur l'échantillon et de le décrire dans un rapport.

- ***Vérification du fonctionnement***

Cette étape consiste à tester le fonctionnement de l'appareil saisi. Le technicien procède à l'allumage de l'appareil et vérifie les fonctionnalités.

- ***Copie des données dans l'échantillon***

Généralement cette copie s'effectue de deux manières différentes selon que les données ont été ou non effacées. Dans le premier cas, les techniciens utilisent la méthode dite de copie physique ou de « bit à bit » selon le langage informatique. Cette dernière est une attaque physique du composant ou une démarche descriptive qui permet, au travers de l'interface, d'accéder à toute ou une partie des données effacées. Lorsque les données ne sont pas effacées, on utilise une deuxième technique dite de la copie logique ou simple. Ces deux copies sont utilisées souvent dans le cas de copie de supporte de données, comme l'exemple d'un disque.

- ***Interprétation et rédaction***

Cela doit répondre au besoin impérieux de rendre le travail des enquêteurs et techniciens le plus intelligible possible aux différentes parties au procès ainsi qu'au juge. Ainsi, cela suppose que les enquêteurs ou les experts sont en possession des informations recueillies par leur propre investigation ou qu'elles leurs aient été communiquées par les parties au litige. Le défaut avec le système français est que les enquêteurs ou experts ne sont pas certains d'avoir l'exhaustivité des éléments, contrairement au système américain avec le « E-discovery » qui permet d'appréhender l'entièreté des informations avant le procès. Ensuite, l'interprétation suppose aussi d'exploiter les documents et de les décortiquer[151]. Pour cela, au regard de la vulnérabilité des données numériques et de la possibilité de leur modification ou altération depuis l'extérieur, il s'avère utile de créer un environnement sécurisé d'exploitation de ces éléments. Dans ce cas, l'investigation numérique fait appel à un système connu par les services judiciaires du nom de bloqueur en écriture.

Le bloqueur en écriture, selon l'institut national des normes et de la technologie, permet la lecture d'un fichier électronique sans causer son altération. Cet outil doit présenter les caractéristiques permettant une exploitation sans faille du fichier, il ne doit pas permettre d'obtenir des informations sur ou depuis un autre lecteur à la fois. Il existe deux types de bloqueur : l'un matériel et l'autre logiciel. Les bloqueurs d'écriture logiciels et matériels font le même travail. Ils empêchent la modification des écritures sur les périphériques de stockage. La principale différence entre les deux outils est que les bloqueurs d'écriture logiciels sont installés sur un poste de travail informatique judiciaire, tandis que les bloqueurs d'écriture matériels ont un logiciel de blocage d'écriture installé sur une puce de contrôleur à l'intérieur

[151] « La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique », CNEJITA, Colloque, 13 avril 2010.P.27

d'un appareil physique portable. Un outil de bloc d'écriture logicielle fonctionne en surveillant et en filtrant certaines commandes du lecteur envoyées depuis une application ou un système d'exploitation via une interface d'accès donnée. Les programmes exécutés dans l'environnement DOS peuvent, en plus de l'accès direct via le variateur de vitesse, utiliser deux autres interfaces : l'interface de service DOS ou l'interface de service BIOS. Le but principal d'un bloqueur d'écriture matériel est d'intercepter et d'empêcher ou de bloquer toute opération de commande de modification d'atteindre le périphérique de stockage. Certaines de ses fonctions incluent la surveillance et le filtrage de toute activité transmise ou reçue entre ses connexions d'interface à l'ordinateur et au périphérique de stockage.

Outre la nécessité d'observer ces étapes précédentes, il est également nécessaire pour les enquêteurs d'établir un lien direct entre les données recueillies et l'infraction réprimée. En d'autres termes, si l'article 79-1 du code pénal incrimine le fait de détenir en vue de la vente ou d'en faire usage, un dispositif conçu pour capter frauduleusement des programmes télévisés, alors que ces programmes sont ouverts à un public abonné, cette infraction n'est néanmoins pas constituée lorsque les méthodes de collecte ont abouti à justifier la détention de cet instrument mais pas son usage illicite, parce que le fait de posséder cet outil n'est pas illégal ni illégitime, et donc dans ce cas il faudra prouver que cet outil ou le programme est spécialement conçu à des fins de détournement de code d'accès aux programmes télévisés payant[152]. Dans une affaire de piratage, le travail des enquêteurs peut aboutir à coïncider les informations recueillies sur l'ordinateur du suspect avec celles issues de l'outil de la victime[153].

La difficulté que rencontre souvent les enquêteurs dans le cadre d'une collecte de données est liée au temps et au besoin financier[154]. La procédure technique de collecte est chronophage à cause notamment de l'augmentation de la capacité des mémoires de stockages, avec donc pour conséquence un nombre impressionnant d'informations à décortiquer. Dans la pratique, le délai pour exploiter le contenu d'un disque va le plus souvent au-delà du délai légal de 48 heures de garde à vue. Dans ce contexte, le risque pour les parquetiers d'être confronté à une demande de nullité de la part de la défense oblige ceux-ci, lorsque la personne gardée n'a pas fait des aveux jusqu'à la purge complète du délai de la garde à vue, à lever cette mesure. De toute façon, cela est économe en ce qu'elle leur donne largement la possibilité d'exploiter et d'extraire des instruments saisis, toutes informations utiles à l'enquête ouverte. Toutefois, il faudra par la suite s'assurer que la personne mise en liberté sera à la disposition des enquêteurs à la fin de la criminalistique numérique.

Quant au pouvoir financier, l'exploitation et la copie de certains disques sont couteuses (achat d'un disque dur de grande capacité sur frais de justice). De fait, la solution pour pallier ce problème est de procéder de manière automatique à la saisie des ordinateurs de valeurs, ce qui n'est pas apprécié pour les mis en causes[155]. Dans certains cas, les enquêteurs procèdent autant qu'ils peuvent à l'impression des données, ce qui représente un long labeur.

---

[152] La preuve numérique, un défi pour l'enquête criminelle du 21è siècle, Erick OK, Cairn, 2003, P.205-2017, https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm
[153] Ibid., P215
[154] Ibib.
[155] Ibid.

### *B. La protection de l'intégrité de l'information numérique*

Lorsque les enquêteurs ou experts ont pu accéder, collecter et exploiter dans les conditions sécurisées les différents éléments utiles à l'enquête, il est obligatoire d'assurer leur intégrité en vue de leur production devant la justice. Sinon, la moindre anomalie détectée par la défense causera le rejet de cet élément de preuve voire tous les actes subséquents.

Si pour les documents papiers, cette préservation de la preuve n'exige pas un protocole compliqué, celle des données numériques est loin de consister à fermer, par exemple, un document dans un sachet et le scellé au moyen d'une étiquette sécurité. Dans le cadre d'une investigation numérique, la préservation de l'intégrité de la preuve numérique est informatique. On utilise la technique dite de hachage. Le hachage ou le calcul d'empreinte numérique permet d'attribuer grâce à un algorithme, le MD5 par exemple, à un fichier ou un ensemble de fichiers une série de caractères unique. En conséquence, lorsque le fichier est modifié toute la chaine de lettres est aussi modifiée. En effet, l'algorithme MD5 présente une hypersensibilité à tout changement, c'est pourquoi, les techniciens le préfère à d'autres algorithme de préservation. Par exemple, en 2021 dans une affaire relative aux attentats du 11 septembre aux USA, les services de FBI ont utilisé un autre algorithme, le CRC32, pour copier et conserver l'ordinateur portable d'une personne suspectée d'avoir joué un rôle déterminant dans la réussite de ce carnage. Il s'agit en l'espèce de Zaccaria Moussaoui, un franco-marocain soupçonné d'avoir des affinités avec Al-Qaïda, une organisation terroriste du Daesh. Dans cette affaire, les enquêteurs se sont intéressés aux mails qu'échangeaient cette personne avec l'organisation depuis les ordinateurs de son école de pilotes. Toutefois, la défense soulèvera que l'algorithme CRC32 utilisé dans cette affaire ne permettait d'assurer que l'intégrité des données recueillies n'était pas contestable. Les avocats de la défense ont ainsi essayé de faire planer le doute sur l'implication de leur client dans cet attentat, en raison du le fait que cet algorithme est loin de donner des résultats incontestables. Cela a donc obligé le juge à ordonner aux services de police d'utiliser la MD5 pour vérifier si les données ont été altérées ou non et la copie du contenu avait été réussie[156].

Néanmoins, dans certains systèmes très complexes, l'application du hachage au moyen de la MD5 n'est pas aussi fiable, notamment à cause de son état dynamique qui évolue en fonction des marchés. C'est le cas des grandes plateformes de vente aux enchères. Une attaque informatique contre ces réseaux n'est pas facile à investiguer. Mais en dehors de ce contexte, l'usage de la MD5 pour la conservation des données est à ce jour la méthode la plus sûre. En 2004, il avait été révélé au monde qu'un groupe d'hackers chinois a déjoué la sécurité de cet algorithme. Cette attaque était en effet fortuite, non généralisée à l'ensemble des systèmes MD5[157]. Sinon, la sécurité de plusieurs infrastructures numériques serait éventuellement en danger et la crédibilité des preuves numériques ne vaudrait absolument rien dans un procès pénal si ce système avait été détruit.

---

[156] [156] « La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique », CNEJITA, Colloque, 13 avril 2010,
Affaire Zaccarias Moussaoui, https://www.wsws.org/francais/News/2002/janvier02/5janv02_moussaoui.shtml

[157] « La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique », CNEJITA, Colloque, 13 avril 2010, P.27-28

Par ailleurs, lorsque les enquêteurs ont pu collecter les traces numériques et que les poursuites ont été actionnées, il s'observera une pratique juridictionnelle qui consistera pour le juge d'apprécier à la lumière de la loi et de l'intime conviction les différents éléments de la procédure qui lui ont été communiquées : c'est la phase dite de l'appréciation du juge.

## § 2 : <u>De l'appréciation des éléments de preuve par le juge</u>

A la lumière des éléments qui lui ont été fournis ainsi que des débats contradictoires, le juge va se livrer à une appréciation objective (**A**) et subjective (**B**) des traces numériques.

### *A. <u>Une appréciation objective du juge</u>*

Selon David BENICHOU, juge en charge de l'instruction au tribunal de grande instance de Nanterre, les premières attentes du juge dans le cadre de la constitution d'une preuve numérique sont relativement dépendantes des missions des experts. Ce juge détaille que les missions des experts sont d'abord des missions "*pour voir*", c'est-à-dire que, le travail de l'expert doit permettre de rendre saisissable et intelligible les données numériques contenues dans une mémoire de stockage, afin de permettre au juge de comprendre la réalité de l'infraction. Par exemple, pour une intrusion frauduleuse dans un système informatique, commise au moyen d'un programme malveillant, qu'il s'agisse de Wabbit[158], du cheval de Troie[159] ou des Vers[160], l'appréciation du juge va dépendre de la possibilité que lui donnera l'expert de voir concrètement le fonctionnement de ces virus. Cette attente est autant valable lorsque les suspects ont utilisé les procédés visant à brouiller les traces de leur forfait, ou lorsqu'il y a discordance entre les dates. Le juge n'attend que le travail de l'expert puisse rendre perceptible le mode d'opération des cybers délinquants, parce que la preuve numérique par nature est *« toute information contenue dans un objet que l'homme n'est pas en mesure d'examiner avec l'usage de ses sens directs* **»,** dira BENICHOU**.**

Ensuite, sur l'ensemble de la procédure, le juge base son appréciation objective des éléments de preuve sur des critères concrets, en passant au crible de la raison les travaux des enquêteurs et des experts. Il s'agit notamment pour lui de vérifier l'intégrité et la traçabilité des éléments de preuve. En clair, le juge doit s'assurer que les procédés de collecte et de préservation des données numériques permettent de se convaincre de leur réelle origine. Il doit veiller sur le fait que l'expert n'a rien omis dans son travail et que les parties peuvent faire confiance à son travail. Pour ce faire, il dispose du pouvoir d'ordonner ou d'autoriser une contre-expertise pour s'assurer de l'absence de contradiction technique. Toutefois, la jurisprudence de la Cour de cassation tient une appréciation relative sur ce critère d'intégrité. Elle a par exemple jugé, dans un arrêt du 19 janvier 2016, que l'ajout d'intitulés sur des

[158] C'est un programme malveillant qui se duplique lui-même avec facilité et rapidité. Il ne se propage pas.
[159] C'est un programme a apparence légitime qui exécute des routines sans l'autorisation de l'auteur. Il a pour vocation de voler les données sensibles des internautes naïfs. Il est également utilisé pour introduire dans un ordinateur une porte dérobée (c'est un ouvreur d'accès frauduleux à un système), ce qui permet une attaque informatique à distance.
[160] Les vers exploitent les ressources d'un ordinateur afin d'assurer sa reproduction, sans contaminer le programme hôte.

documents informatiques aux fins de repérages et de l'étude ne pouvait constituer une atteinte à l'intégrité de la preuve numérique[161].

Enfin, le juge se nourrit également des débats contradictoires entre les différentes parties afin de se renforcer son appréciation des éléments de preuve. A ce propos**,** une convention signée en 2009 par la Cour d'appel de Paris, les barreaux des neuf tribunaux du ressort et l'Union des compagnies d'experts près la cour d'appel de Paris oblige les experts à remettre aux parties un document de synthèse afin qu'elles émettent leurs observations sur le travail de l'expert[162]**.** Le rapport ne doit cependant pas donner le sentiment que l'expertise est à charge ou à décharge. Il doit en effet être présenté avec une telle rigueur que le juge ne doit pas le (l'expert) soupçonner dans une prise de position dans l'affaire. A titre illustratif, dans un rapport sur la pédopornographie commise au moyen des TIC, l'expert doit se contenter d'extraire les images pornographiques, ne doit aucunement mentionner lesquelles des images ont un caractère pédopornographique ou non. Une telle analyse est réservée aux juges, jurées (à la cour d'assise) et aux parties lors des débats. Selon R. GARRAUD l'expert *« donne une opinion scientifiquement raisonnée sur des faits qui lui sont soumis »*[163]. Il peut faire l'usage de précaution sémantique comme par exemple : *« les fichiers pouvant représenter des mineurs »* (hors les cas où la minorité ne fait aucun doute).

Toutefois, à la lecture des travaux de certains auteurs, il est difficile de croire que le statut de neutralité qu'on prête à l'expert dans le cadre d'un procès soit dénué de pouvoir d'appréciation. A tel enseigne que GENESTEIX affirme que dans un procès, *« l''expert n'a pas seulement vu, il a jugé* »[164]**.** C'est-à-dire que devant les questions les plus techniques d'une affaire, le point de vue du juge judiciaire s'efface totalement derrière les analyses de l'expert. La Cour de cassation était même allée suggérer aux juridictions de ne pas refuser les demandes d'expertise, d'autant plus que celles-ci les aideront à forger leur motivation. L'importance d'une telle place accordée aux experts tant au niveau des enquêtes que pendant le procès est sans doute ce qui a amené Lagneau à penser que l'expertise était devenue la seule mode de preuve qui conditionne les autres[165].

En tout état de cause, à l'issu du débat, l'intime conviction du juge ou des jurés devra être le dernier recours pour apprécier les différents éléments de preuves électroniques.

---

[161] Cass. Crim., 19 jan. 2016 n° 15.81.041, Bull. n°14

[162] La preuve numérique à l'épreuve du litige, colloque CENJI, intervention de Monsieur Patrick 2010

[163] R. GARRAUD, Traité théorique et pratique d'instruction criminelle et de procédure pénale, Larose et Ténin, 1909, Tome 1, p. 592

[164] M. GENESTEIX, L'expertise criminelle en France, A. Pédone, 1900, [Droit privé : Paris], p. 13.
Voir aussi O. DEJEAN, Traité théorique et pratique des expertises en matières civiles, administratives et commerciales, manuel des experts, A. Marescq aîné, Paris, 1881, p. 2. « *Les experts commis par les tribunaux tiennent de la justice une délégation qui leur fait emprunter, sous certains rapports, le caractère du juge »*

[165] Ch. LAGNEAU, De l'expertise à base scientifique comme moyen de preuve en matière criminelle, Domat-Montchrestien, 1934, [Droit privé : Université de Paris], p. 34.

### *B. <u>Une appréciation subjective du juge</u>*

Jean Danet, professeur à l'université de Nantes, affirmait que « l'intime conviction est une norme démocratique de la preuve »[166]. Il s'agit en effet, précise le même auteur, pour le juge de passer au crible de la raison toutes les composantes du dossier, chaque élément de preuve, chaque moyen de la défense[167]. L'intime conviction est en réalité une composante de son pouvoir souverain. En conséquence, tout pourvoi qui se borne à remettre en cause cette souveraineté du juge serait probablement rejeté devant la Cour de cassation[168].

L''intime conviction du juge doit laisser transparaitre l'effet que les différents éléments présentés par les parties ont produit sur lui, sur sa conscience[169], c'est-à-dire que le juge doit dans son raisonnement laisser entrevoir l'appréhension qu'il a de l'innocence ou de la culpabilité du prévenu de par les éléments présentés par les parties. Pour reprendre exactement la formule du code de procédure pénale, l'intime conviction consiste pour le juge ou les jurés composant une Cour d'assise à *« s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense.* »[170]. Et, la Chambre criminelle de la Cour de cassation tient une attention particulière à ce que cette intime conviction soit bien détaillée : *« Toute décision doit être motivée, l'insuffisance ou la contradiction de motifs équivaut à leur absence* ».

Avant une loi du 13 janvier 2011[171], le juge français n'avait pas l'obligation de motiver sa décision ou d'expliquer lesquels des éléments de preuves l'ont convaincu de l'innocence de ou de la culpabilité d'une personne. Cette absence de motivation était mal vue tant en droit interne qu'à l'international. Dans le même temps, la Chambre criminelle écartait l'inconventionnalité de cette pratique française[172], position approuvée par le conseil constitutionnel lors d'une réponse à une question prioritaire de constitutionnalité[173]. Le rapport du comité Léger a pris appui sur une jurisprudence de la CEDH[174] et a consacré la motivation de toute décision de jugement. Ladite jurisprudence condamnait la Belgique pour non-conformité de sa législation à la convention, du fait de l'absence de l'application effective du droit à un procès équitable dans ce pays. En effet, dans le système belge, les décisions de jugement n'étaient pas motivées

---

[166] Jean Danet, "Philosophie Droit : L'intime conviction, norme démocratique de la preuve ?

[167] Ibid.

[168] La preuve pénale, Sylvie GRUNVALD, Jean D., UNJF, « *... que les moyens, qui se bornent à remettre en question l'appréciation souveraine, par les juges du fond, des faits et circonstances de la cause, ainsi que des éléments de preuve contradictoirement débattus, ne sauraient être admis* »

[169]Cornu G., « Vocabulaire juridique », 10 éd., PUF, 2014, p. 21, « La conscience est le for interne, le lieu intime de l'examen individuel des débats (...) Qui conduit à se déterminer soit même, par adhésion aux devoirs d'une morale, d'une religion ou sous l'inspiration des devoirs que chacun se fait »

[170] Article 353 du CPP

[171] loi n° 2011-939 du 10 août 2011 sur la participation des citoyens au fonctionnement de la justice pénale et le jugement des mineurs

[172] v. Cass. crim., 30 avril 1996, Bull. 181, RSC 1996, obs. M. Dintilhac et Cass. crim., 14 octobre 2009, n° 08-86480 ou encore Cass. crim., 20 janvier 2010, n° 08-88112, 08-8798

[173]Cons. Const., n° 2011-113/115 QPC

[174] CEDH, 13 janvier 2009, Taxquet contre Belgique, requête n° 926/05

car les autorités belges considéraient que la motivation d'une décision judiciaire était en totale contradiction avec le principe de l'intime conviction. Suite à cette condamnation, dans le cadre d'une loi de 2009 relative à la réforme à la cour d'assise, la Belgique a remplacé la notion de l'intime conviction par une autre formule quasi proche de celle-ci *:* « les éléments de preuve au-delà de tout doute raisonnable »[175].

En matière de preuve numérique, l'appréciation subjective du juge va être identique à celle d'une preuve classique, avec quelques particularités près. En effet, elle doit également consister pour le juge ou le jury à se laisser emporter dans son esprit par les différents éléments numériques et le poids de raisonnement des parties et aussi de celui de l'expert, afin de produire une réponse qui transparaitra le juste milieu. Cette étape, aussi importante qu'elle puisse être, apparait moins originale à nos yeux parce qu'elle ne reproduit que dans le secret du délibéré toute l'arborescence de l'appréciation objective, mettant ainsi au cœur de la conscience du juge et, éventuellement, des jurés, les analyses de la seule personne qui maitrise la technologie numérique, l'expert. Toutefois, les juges ne sont pas obligés de considérer les rapports des experts qui peuvent parfois se révéler erronée, l'intelligence humaine n'étant pas infaillible. Cela justifie d'ailleurs le fait que la constitution de la preuve numérique peut se révéler dans certains cas difficiles voire impossible.

## **Section 2 : Les limites à la constitution de la preuve numérique en cybercriminalité**

Les limitations liées à la constitution de la preuve numérique sont de plusieurs ordres. Elles tiennent à la fois à l'inaccessibilité à certains éléments de preuve pour divers motifs (**paragraphe 1)** et aussi au fait que certaines pratiques de collecte peuvent se révéler attentatoire à la vie privée des personnes (**paragraphe 2**).

### **§ 1 : Une limitation liée aux difficultés d'accessibilité à certains éléments de preuve**

La question de l'inaccessibilité est souvent posée dans la pratique. En effet, certains cybers criminels futés ont recours à des techniques de nature à rendre opaque les éléments de preuve, ce qui constitue un revers pour les enquêteurs. Aussi, la coopération nouée entre les Etats à Budapest reste-t-elle un sujet politiquement complexe à pratiquer (A). C'est pourquoi, dans certains cas, les Etats usent de méthodes parfois trop intrusives à la liberté des personnes pour intercepter des données de communications (B).

#### **A. *Une inaccessibilité tenant à l'usage de techniques d'obfuscation***

Outre les problèmes liés au volume des données qui rendent chronophage leur exploitation informatique ainsi que les problèmes financiers, les enquêteurs sont parfois confrontés à bien d'autres problèmes techniques qui constituent un obstacle à leur travail. C'est le cas de la cryptographie, la stéganographie, le darkweb, l'horodatage et le port-source.

- ***La cryptographie***

[175] Loi du 21 décembre 2009 relative à la réforme de la cour d'assises N° : 2009090000. Service public fédéral justice., http://www.ejustice.just.fgov.be/eli/loi/2009/12/21/2009090000/moniteur

La cryptographie, encore appelée le chiffrement, est une opération de transformation des données visant à les rendre inintelligibles à toute personne autre que le possesseur de la clé de chiffrement. La cryptographie est faite d'une série de lettres de toute forme qui dissimule une information précise. Cette série de lettres cryptographiques se distingue, selon la Cour d'appel de Paris, d'un code de déverrouillage qui, lui, permet uniquement d'empêcher l'accès à une source d'information mais pas à un déchiffrement[176]. En conséquence, cette juridiction soutient que le refus par une personne de fournir son code de déverrouillage ne constitue pas une infraction au sens de l'article 434-15-2 du code pénal[177]. Toutefois, la Cour de cassation est allée dans le sens inverse en approuvant ce délit dans une décision du 10 décembre 2019[178] dans le cadre d'une affaire identique où une personne refuse aux services de la PJ de communiquer son code de déverrouillage téléphonique.

Concrètement, la technique permet à l'auteur de mettre à l'abri des enquêteurs les éléments pouvant prouver, éventuellement, son implication délictuelle ou criminelle dans une affaire. En effet, afin de protéger les données les plus sensibles des sociétés bancaires (les comptes bancaires), de l'Etat (secrets de défense d'Etat), des simples particuliers (les données à caractère personnel), il était nécessaire d'autoriser la technique du chiffrement. Toutefois, dans une enquête pénale, lorsque les enquêteurs sont confrontés à des appareils cryptés par les suspects qui refusent de leur communiquer le code de décryptage, cela devient un défi pour l'enquête. C'est pourquoi le législateur, à travers l'article 230-1 du code de procédure pénale donne pouvoir aux autorités judiciaires (procureur, juge d'instruction et juridiction de jugement) de saisir toute personne qualifiée ou expert pour déchiffrer les appareils concernés. Dans certains cas, notamment lorsqu'une peine égale ou supérieure à deux ans est encourue et que l'enquête l'exige, les autorités judiciaires peuvent recourir au service secret défense de l'Etat selon les formes prescrites par la loi. Dans la pratique, le service interministériel habilité secret défense de l'Etat est saisi par les magistrats par le biais de l'OCLCTIC de la sous-direction de la lutte contre la cybercriminalité. Cette procédure rend parfois lente les procédures d'urgences. Le rapport « protéger les internautes » de 2014 propose ainsi au niveau de sa recommandation n°43 alinéas 3 de permettre aux magistrats la saisine directe du centre technique d'assistance sans devoir passer par l'intermédiaire de l'office central de la lutte contre les TIC[179]. Même à l'issu de cette procédure, l'assistance fructueuse de ce centre dans une affaire judiciaire se limite à une communication procédurale et limitée des données. Ce qui restreint incontestablement le champ de l'enquête[180].

---

[176] CA Paris, 16 Avr. 2019, n°18/09267

[177] Article 434-15-2 du CP *« Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.*

*Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende.*

[178] Crim., 10 déc., 2019 n°18-86.878

[179] « Protéger les internautes », rapport sur la cybercriminalité, groupe interministériel sur la lutte contre la cybercriminalité, février 2014, P.231

[180] Articles L2312-4 à L2312-8 du code de défense.

Par ailleurs pour pallier ce problème de cryptographie de données, il existe en France une législation qui régularise le commerce, l'exportation et l'importation de logiciel de chiffrement de donnée. Néanmoins, il n'en demeure pas moins que la criminalistique numérique doit encore plus s'adapter aujourd'hui à la cryptanalyse qui, selon un auteur, va devenir le contournement des techniques cryptographiques le domaine essentiel de la criminalistique numérique dans les années à venir[181].

- ***La stéganographie***

La technique de la stéganographie consiste à dissimuler à l'intérieur d'un message sans intérêt particulier un autre message comportant les informations recherchées par les enquêteurs. Ce procédé a la même finalité que la cryptologie à savoir, dissimuler des informations, mais le propre de cette dernière est de rendre inintelligible les données, bloquer l'accès, là où la stéganographie permet l'accès mais sous le couvert d'un message qui à première vue ne peut attirer l'attention des enquêteurs. Ce procédé est à l'image d'une histoire relatée par l'historien Hérodote dans ses travaux. En l'an 484 avant J.C, le roi des Perses, à l'époque Xerxès 1$^{er,}$ décide d'envahir Sparte. Pour ce faire, il prévoit de mettre en place une armée. Des années de préparation après, la nouvelle de l'invasion finit par tomber dans les oreilles des Spartes par le fait d'un ancien roi sparte réfugié à Perses. Pour communiquer avec les siens, celui-ci a usé d'un stratagème qui a consisté à transcrire les projets de Xerxès 1$^{er}$ sur une double tablette dont il a gratté la cire. A la fin de la transcription, il recouvrit cette tablette de la cire ; ainsi le porteur d'une tablette vierge ne risquait pas d'ennui[182].

Selon la doctrine, il existe deux types de stéganographie : une linguistique et l'autre technique[183]. La première consiste à modifier les propriétés linguistiques d'un texte pour y cacher des informations de valeur. Cette forme est rarement pratiquée. La deuxième renvoie concrètement à la dissimulation des données dans plusieurs médias (audio, image, vidéo).

Par ailleurs, le repérage d'une information dissimulée au moyen de la stéganographie impose l'usage de la stéganalyse comme c'est le cas de la cryptanalyse pour le chiffrement. La stéganalyse permet de détecter si un medium[184] donné cache un message secret, et si possible, de récupérer ce message caché[185]. C'est une tâche extrêmement difficile qui requiert une expertise qualifiée et un pouvoir d'argent conséquent parce que, ce procédé fait appel à des outils sophistiqués de la technologie. Cette technique est encore plus délicate lorsque que l'expert se retrouve à analyser une variété de mediums, de données ou d'algorithmes d'insertion ayant créé une forte distorsion dans le contenu du message dissimulé.

---

[181] La preuve numérique, un défi pour l'enquête criminelle du 21è siècle, Erick OK , Cairn, 2003, P.205-2017, https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

[182] https://fr.wikipedia.org/wiki/St%C3%A9ganographie

[183] Sécurité de l'information par stéganographie basée sur les séquences chaotiques, Dalia Battikh, HAL Id: tel-01275346, P. 7, https://tel.archives-ouvertes.fr/tel-01275346

[184] Partie moyenne, se situant entre le grave et l'aigu, du registre des sons d'un instrument ou de l'étendue d'une voix

[185] Ibid. p.18

- ***Le darkweb et les autres logiciels d'anonymisation***

A l'occasion de mes stages à la police judiciaire, j'ai eu la chance d'échanger avec un enquêteur de la police aux frontières (PAF), spécialisé dans le Darkweb. Celui-ci m'a enseigné le fonctionnement du site et les problèmes qu'il pose aux enquêteurs.

En effet, Internet présente une architecture à trois compartiments : le *Clearweb*, le *Deep* web et le *darknet ou Web profond*. Le Clearweb ou Internet ouvert est la partie du Net qu'on peut accéder sans se confronter à un système de sécurité particulier (exemple : faire des recherches sur Google). Le Deep web quant à lui reste la partie sécurisée de l'Internet où se loge par exemple les banques, les sociétés privées, la sécurité des infrastructures fondamentales de l'Etat, etc. Le niveau de sécurité de cette partie est lié notamment à la protection des données de valeur. Ces derniers mois, on constate que cet environnement est de plus en proie à des menaces de détournement de système de sécurité (exemple de l'attaque informatique de la plateforme de cryptomonnaie *Gatehub* en 2019, de l'oléoduc Pipeline aux USA récemment, etc.).

Enfin le darknet ou internet obscur, ce site auquel on ne peut accéder que par le navigateur Tor a été conçu par l'armée américaine pour faire dominer l'idéologie de la démocratie dans le monde. Ce site a été largement exploités dans les conflits internes. C'est le cas du printemps arabe où il a permis aux journalistes alors persécutés sous les régimes dictatoriaux de pouvoir dénoncer les barbaries sans se faire repérer. De la chute en Tunisie du président Zine El-Abidine Ben Ali et d'Hosni Moubarak en Egypte à la révolution libyenne ayant conduit à l'assassinat du guide libyen Mohamed Kadhafi, le réseau Tor a été beaucoup exploité et a servi à diffuser des images de la persécution de civils, d'enrôlement d'enfant etc., ce qui a provoqué une vague de réactions protestataires déployée partout dans le monde, suivie de la mise en place d'une série d'alliances animée par une même idéologie politique.

Cependant, depuis plusieurs années, ce réseau a été détourné de la main de ses concepteurs pour devenir une niche à promouvoir la criminalité organisée dans toutes ses acceptions : trafic de drogue, pédopornographie, vente d'armes, commerce illicite d'animaux sauvages, proxénétisme, traitre d'êtres humains, vente de logiciels malveillants, bref tout le panel des infractions sévèrement punies se développe à travers ce réseau. La difficulté que rencontre les enquêteurs sur ce réseau est liée au fait qu'il permet aux criminels d'opérer sous anonymat total. Manifestement, Tor fait transiter le trafic par plusieurs couches positionnées à travers les quatre points du globe, de façon à ce que personne ne puisse déterminer l'origine et identifier les délinquants derrières ce trafic. Ce réseau fonctionne comme le logiciel VPN[186] ou un serveur Proxy[187]. Selon les services de renseignement et d'analyse de la stratégie criminelle de la police judiciaire, le réseau Tor est aussi utilisé en matière de *rançongiciel* pour masquer l'hébergement des serveurs supportant des programmes et charges virales et pour permettre la mise en relation victime-rançonneur aux fins de règlement de la rançon en cryptomonnaie. A travers ce réseau, on peut également commanditer un meurtre en demandant à un individu de poser une bombe dans un espace ouvert au public. Les utilisateurs de ce réseau communiquent

[186] *Virtual Private Network* : c'est un réseau privé virtuel qui rend l'internaute non identifiable
[187] Un serveur proxy est une machine qui sert d'intermédiaire entre les machines d'un réseau et un autre réseau

à travers des clés, lesquelles contiennent des instructions précises. Pour accéder à une clé et lire son contenu, il est nécessaire d'être en possession du code, et seul l'expéditeur peut fournir la convention secrète du décodage à son destinataire. Parfois, ce processus passe par un *escrow*[188]et très souvent, le destinataire n'accède au contenu d'un message qu'après avoir entré trois conventions secrètes. Cette précaution permet en effet aux protagonistes d'être sûrs que leur message parvient à la bonne personne.

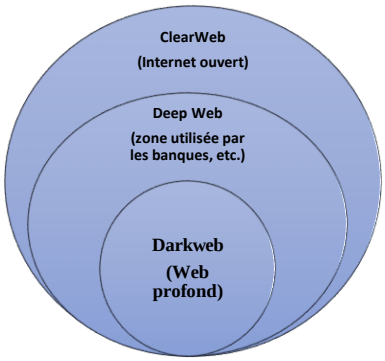
Au regard donc de cette complexe architecture du réseau, il est difficile pour les enquêteurs de collecter les preuves numériques et d'identifier les auteurs. La seule solution qui s'observe dans la pratique est soit l'infiltration ou la commission d'une erreur humaine par les criminels. Parfois la police se sert des sources[189]. Dans une affaire audiencée devant le tribunal correctionnel de Limoges le 22 avril 2021[190] et actuellement en cours devant la Cour d'appel de Limoges, affaire dans laquelle était en cause un petit réseau de trafiquant de stupéfiants, les constations policières ont révélé que le principal accusé achetait les produits sur *darknet* et les faisait livrer à l'adresse d'un autre membre de l'organisation. Il animait son trafic sous un faux pseudonyme sur Snapchat et utilisait aussi les systèmes bancaires virtuels pour convertir le produit du trafic en monnaie virtuelle, afin de brouiller leur traçabilité. Cette opération serait impossible à mettre à nu si les services de la douane n'avaient pas repéré un colis, lequel contenait une marchandise de drogue. Cela a amené les enquêteurs à perquisitionner les domiciles des suspects. A l'audience devant le tribunal, le principal accusé a préféré exercer son droit au silence, une défense qui a été maintenue devant la Cour d'Appel de Limoges. Ce qui n'a pas permis aux magistrats de céans, qui n'avaient pas une connaissance technique du fonctionnement de ce réseau (déplore d'ailleurs l'avocat général lors de sa réquisition), d'avoir plus d'information pour étudier sa cause. Ce frein à la procédure ne permettait pas au siège de comprendre l'affaire et de motiver sa décision en prenant en compte tous les aspects de la procédure. De son côté, l'avocat demande aux enquêteurs « de travailler au-delà du droit au silence ». Mais se taire, en l'espèce, ne va pas pouvoir l'aider dans un procès où l'ensemble des témoignages des autres Co-prévenus est unanime sur le rôle principal joué par son client dans l'organisation, le nombre très curieux de carte SIM retrouvé à son domicile, l'installation de logiciels VPN sur son ordinateur (même si, sur ce point, le suspect soutenait à l'audience qu'avoir un VPN sur ordinateur était légal), les nombreuses recherches effectuées en vue de comprendre le fonctionnement de la conversion de l'argent en Bitcoin, etc. Dans ces genres de procédure, à défaut d'avoir les traces numériques pour constituer la preuve, les juges se contentent de tirer des conclusions de l'erreur humaine et s base largement sur les témoignages.

Aujourd'hui, toutes les activités criminelles qui se pratiquent sur le web obscur (darknet) font partie en grande majorité de la criminalité organisée ou du moins de la catégorie des infractions punies de peine criminelle ; ce qui constitue un enjeu de grande importance pour la politique criminelle étatique. Aussi, les services d'enquêtes sont-ils limités dans leur recherche parce qu'un individu soupçonné d'être auteur ou complice d'infractions graves, lorsqu'il oppose un refus à l'accès de son compte ou son ordinateur, la police technique et

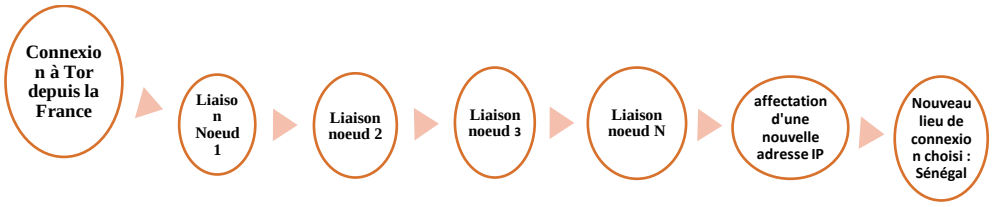
[188] C'est le nom de celui assure l'intermédiaire entre un vendeur et un acheteur sur darknet
[189] V. la partir sur les acteurs internes en charge de la preuve numérique en cybercriminalité
[190] TJ Limoges, 22 avril 2021 n°494 /2021

scientifique n'arrive pas à percer le mystère derrière ses activités sur le darknet. Enfin des comptes, celui-ci s'en sort avec une peine dont le plafond est limité en état actuel du droit à cinq ans (art. 434-15-2 du CP). Il se pourrait également, qu'il bénéficie de la grâce d'un sursis. C'est pourquoi, il serait peut-être judicieux pour le législateur d'envisager un nouvel aliéna au niveau de l'article 434-15-2 du de pénal afin de créer une nouvelle circonstance aggravante de la cyber infraction poursuivie, lorsque lors d'une enquête, les enquêteurs soupçonnent avec certitude qu'une personne arrêtée exploitent le réseau Tor à des fins criminelles, et que cette dernière oppose catégoriquement l'accès à ses activités ou à ses appareils.

*1.L'architecture de l'Internet*




*2.Un exemple du cycle d'une connexion sur le réseau Tor*




- ***La problématique liée aux dates***

Lors de la copie des données numériques par les enquêteurs, il arrive que toutes les métadonnées ne soient pas prises en compte, c'est par exemple le cas des dates. Généralement les appareils électroniques, micro-ordinateurs ou les serveurs de messagerie sont dotés d'un système qui sert à dater automatiquement les fichiers. Cependant, certains systèmes téléphoniques ne sont pas synchronisés de la même manière. Ce qui fait que dans la plupart des cas, le réglage de la date est opéré par l'utilisateur. C'est alors que les techniciens en investigation numérique constatent parfois que la date indiquée sur un fichier électronique saisi lors d'une perquisition informatique diffère de la date normale (ex : un fichier qui indique comme date le 11 mai 2040 alors que nous sommes en 2021, ou lorsqu'un fichier est daté au lundi 13 juillet 2021 alors que le 13 juillet 2021 est un mardi).

A cela s'ajoute aussi le fait que la plupart des serveurs liés à la messagerie sont externalisés. Ce qui peut avoir, parfois, un incident conséquent sur la procédure car on ne pas sur cette base tirer des conclusions évidentes sur les problématiques liées aux dates si on a la conviction que la date et l'horloge peuvent être établies par l'utilisateur du téléphone mis en cause[191]. Pour ce fait, il existe à la Police un système casuistique de reconstitution des dates. En effet, les enquêteurs prennent en compte un nombre de paramètres assez large, à savoir, identifier le contexte dans lequel un message a été envoyé et confronter ces informations avec celles issues des analyses du téléphone portable par exemple

- ***La problématique liée au « port-source »***

Selon les agents de la SDLC, cette problématique met en exergue les difficultés relatives à la non-conservation par certains opérateurs, notamment les Américains, du port-source lors d'une connexion à une adresse Internet, ce qui ne permet pas aux enquêteurs français d'identifier l'abonnement d'un smartphone lorsque celui-ci est utilisé pour se connecter au réseau comme Facebook[192]. Le problème est devenu délicat avec la démocratisation de l'Internet qui a permis de se connecter avec les réseaux mobiles. Ainsi, les opérateurs confrontés à la pénurie d'adresse IP ont dû se doter des systèmes de translation d'adresse afin de pallier la pénurie d'adresse IPv4. En conséquence, le constat était que plusieurs internautes ont accédé à Internet par la même passerelle et sous la même adresse IP. Selon la Sous-direction de la lutte contre la cybercriminalité, cette installation des logiciels de translation a le désavantage de provoquer des risques d'augmentation de la latence et de réduction de la résilience du réseau en introduisant des goulots d'étranglements ou des points de défaillances uniques, c'est-à-dire le blocage des adresses IP[193]. L'utilisation à grande échelle des logiciels de translations nuit aux enquêtes effectuées en ligne et entrave les systèmes de détections de fraude des banques. A cet amère constat s'ajoute aussi le fait que, pour obtenir d'un fournisseur d'accès à Internet des informations, les enquêteurs doivent fournir en plus de la date, l'heure, l'adresse IP de connexion et de destination, le numéro de port-source retourné par le site de destination[194], ce qui est très compliquée à avoir.

### ***B. Les difficultés liées à la collecte de données accessibles depuis un territoire étranger***

L'évolution des technologies numériques oblige à faire la distinction entre un support de stockage matériel et celui depuis lequel un ensemble de données peut être accessible. Il est en effet courant que les entreprises conservent leurs données dans des serveurs, pour la majorité, situés à l'étranger. Alors que, l'accès au support dématérialisé de stockage dans le cadre d'une procédure de cybercriminalité est chose incontournable. C'est à juste titre que l'article 57-1 du code de procédure pénale permet aux enquêteurs d'accéder aux données stockées sur support informatique physique ou dans les serveurs internes et externes à partir d'un système initial. Si

[191] La preuve numérique, un défi pour l'enquête criminelle du 21è siècle, Erick Fresney, Cairn, 2003, P.216
[192] Initiation au fonctionnement de l'Internet et aux enjeux de la gouvernance internet, SDCL, DACG, juin 2021
[193] Ibid.
[194] Ibid.

cet article a été édicté pour être mis en œuvre uniquement dans le cadre d'une enquête de flagrance, il est également possible qu'il soit mobilisé pour les autres types d'enquête, notamment l'enquête préliminaire (par renvoie de l'article 76-3)[195] et dans le cadre d'une commission rogatoire (par renvoie de l'article 97-1 du CPP[196]).

Cependant, dans le cadre d'une enquête ce n'est pas l'accès à une salle qui loge des serveurs qui sera d'une importance capitale, tout ce qui intéresse l'enquêteur, c'est en réalité l'accès aux données à travers un écran relié simplement à la salle des serveurs. En claire, l'enquêteur en matière de l'investigation numérique ne va pas prioritairement chercher à lire les courriers électroniques dans la salle des serveurs, alors que le contenu informatif de ces courriers peut être délivré à quiconque se trouve sur le lieu de situation de l'écran relié à ladite salle.

Comme il a été précédemment vu à travers une jurisprudence du 6 novembre 2013, lorsque l'accès au serveur étranger est fait par le biais d'un système initial situé sur le territoire national, cela n'impose pas d'actionner une procédure d'entraide internationale, c'est-à-dire que, la compétence territoriale des autorités policières s'étend de manière virtuelle à des serveurs localisés en territoire étranger, à la seule condition que leur accès soit possible à partir, par exemple, de l'ordinateur d'un suspect dont le domicile a été perquisitionné en France. En revanche, pour accéder aux données depuis un territoire étranger, l'officier devra se conformer aux réserves émises par le législateur au niveau du troisième alinéa de l'article 57-1 du code de procédure pénale, c'est-à-dire l'entraide pénale internationale.

Premièrement, cet article pose quelques difficultés d'interprétation. En effet, l'alinéa 3 de l'article 57-1 du CPP dispose que « s'il est préalablement avéré que ces données, accessibles à partir d'un système initial ou disponible pour le système initial, sont stockés dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur ». De cet article, la doctrine relève deux conditions à respecter par l'officier pour l'accès aux données depuis un système informatique situé en dehors du territoire national. Il s'agit de l'information préalable de l'extranéité des données de l'officier par la personne mise en cause et le respect des engagements internationaux[197].

Sur l'information préalable de l'extraterritorialité des données, la doctrine considère que cela constitue une condition optimale en vue de la prise en compte de la souveraineté du pays étranger[198]. Toutefois, elle n'a pu s'empêcher de critiquer cette condition au regard d'une certaine « hypocrisie » qu'elle incarne. En effet, suivant la lettre de cette disposition, il suffit qu'une personne mise en cause précise à l'officier que certaines données recherchées sont

[195] L'article 76-3 du CPP issu de la loi n° 2003-239 du 18 mars 2003 dispose « l'officier de police peut, pour les nécessités de l'enquête, procéder aux opérations prévues à l'article 57-1. »
[196] Article 97-1 du CPP « l'officier de police peut, pour les nécessités de l'exécution de la commission rogatoire, dans les conditions prévues à l'article 76, recourir aux opérations prévues à l'article 57-1. »
[197] Sur l'usage de cette expression par le législateur au niveau de l'al. 3 de l'article 57-1 du CPP, voir les analyses critiques d'Alexandre Rousselet-Magri, https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2017-4-page-659.htm
[198]« les perquisitions informatiques à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données, étude comparé en droit français et états- uniens », Alexandre Rousselet-Magri, Cairn, 2017, P.663, https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2017-4-page-659.htm

localisées dans des serveurs dont l'accès n'est possible qu'en dehors du territoire pour que, mécaniquement, cet officier soit obligé de respecter les engagements internationaux[199]. Ce qui est très étrange parce, ce même article, sur le fondement de ses alinéas 1 et 2, semble autoriser l'officier à ignorer la souveraineté de l'Etat étranger lorsque l'accès est possible depuis un système initial situé sur le sol français.

Mais de toute façon, la perquisition à distance telle que prévue par les dispositions de l'article 57-1, transgresse le champ légal de compétence de l'officier de police judiciaire imposé à l'article 18 du code de procédure pénale. Cette disposition limite la compétence maximale de la Police uniquement au territoire national. Il prévoie néanmoins que, sur l'accord explicite d'un Etat tiers, les autorités françaises peuvent, dans le cadre d'une commission rogatoire, mener des actes d'enquêtes sur le territoire de ce dernier et ce, uniquement pour les actes d'audition et non pour les actes de perquisition ni de saisies. C'est une telle solution qu'avait retenue par la doctrine bien avant la jurisprudence du 6 novembre 2013[200].

En outre, il est nécessaire que la demande d'une perquisition en territoire étranger, sauf les cas d'autorisation automatique issue d'un accord préalablement établi entre la France et cet Etat tiers, soit validée par l'Etat étranger. Une telle exigence de l'article 57-1 du CPP est interprété par la doctrine comme une conformité à la Convention de Budapest, notamment au niveau de son article 32. Ce qui est étonnant parce que, les articles 14 et 19 de cette même convention mettent à la charge des Etats de définir leur propre stratégie quant à l'accès ou la collecte des données transfrontières. L'article 19 pose quant à lui le régime d'extension de la perquisition, là où l'article 32 de la convention vient assujetti la mise en œuvre d'une demande de perquisition adressée à la publicité des données ou, dans le cas contraire, au consentement légal et volontaire de la personne habilitée à divulguer les informations depuis le système étranger sollicité. Cette personne peut être une autorité judiciaire ou une autorité des services de renseignement etc. Dans ce contexte, il peut exister un risque de blocage politique ou institutionnel d'une enquête pénale en cas de défaut de consentement de ladite personne.

Par ailleurs, même si les conditions posées au niveau de l'article 32 ont pu être observées, il se trouve parfois que le système de certains Etats ne soient pas aussi efficace pour rendre fructueuses les demandes d'entraide pénales. C'est le cas par exemple d'une demande d'entraine émise par la France à la Côte d'Ivoire en vue de permettre aux autorités françaises d'accéder aux serveurs situés sur le territoire ivoirien. Dans cet ordre, bien que l'Etat requis ait pu exprimer sa volonté de collaborer avec la France, il est probable que le système de connexion au réseau Internet en code d'Ivoire n'aide pas à l'enquête.

Au sein de l'Europe, la reconnaissance mutuelle des actes d'enquêtes et de jugements permet de simplifier l'échange d'information entre les Etats, par exemple en supprimant le respect de la condition de la double incrimination telle que prévue par la Convention internationale sur l'extradition. Selon ce principe, la poursuite et le jugement du délinquant ne sont possibles que si l'infraction visée existe à la fois dans l'État requis et dans l'État requérant. De plus, de nombreux textes et projets européens ne cessent d'être créés et viennent alléger la

[199] Ibid.

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

procédure d'accessibilité aux données à caractère transfrontière entre Etats membres de l'Union. Toutefois, tant dans la théorie que dans la pratique, les choses ne sont pas aussi simples, parce que même au sein de l'Union européenne, l'exécution d'un mandat d'européen d'obtention des éléments de preuve n'est pas automatique. Elle est soumise à des conditions qui parfois constituent un obstacle significatif à l'enquête. Sans être exhaustif, citons les dispositions posées au niveau des articles 694-31 et suivants du CPP, qui précisent notamment qu'une décision d'enquête européenne peut être refusée par un magistrat si un privilège ou une immunité fait obstacle à son exécution, si la demande est contraire aux dispositions relatives à l'établissement de la responsabilité pénale en matière de délits de presse, etc.[201]. De plus, le

[201] Article 694-31 « *Le magistrat saisi refuse de reconnaître ou d'exécuter une décision d'enquête européenne dans l'un des cas suivants :*

*1° Si un privilège ou une immunité fait obstacle à son exécution ; lorsque ce privilège ou cette immunité est susceptible d'être levé par une autorité française, la reconnaissance et l'exécution de la décision ne sont refusées qu'après que le magistrat saisi a adressé sans délai à l'autorité compétente une demande de levée de ce privilège ou de cette immunité et que celui-ci n'a pas été levé ; si les autorités françaises ne sont pas compétentes, la demande de levée est laissée au soin de l'Etat d'émission ;*

*2° Si la demande d'enquête est contraire aux dispositions relatives à l'établissement de la responsabilité pénale en matière d'infraction de presse de la loi du 29 juillet 1881 sur la liberté de la presse et de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle ;*

*3° Si la décision porte sur la transmission d'informations ayant fait l'objet d'une classification en application des dispositions de l'article 413-9 du code pénal ; en ce cas, la reconnaissance et l'exécution de la décision ne sont refusées qu'après que le magistrat saisi a adressé sans délai à l'autorité administrative compétente une demande tendant à la déclassification et à la communication des informations en application de l'article L. 2312-4 du code de la défense et que cette demande n'a pas été acceptée ; si la demande de déclassification est partiellement acceptée, la reconnaissance et l'exécution de la décision d'enquête européenne ne peuvent porter que sur les informations déclassifiées ;*

*4° Si la demande concerne une procédure mentionnée à l'article 694-29 du présent code et qui n'est pas relative à une infraction pénale, lorsque la mesure demandée ne serait pas autorisée par la loi française dans le cadre d'une procédure nationale similaire ;*

*5° Si l'exécution de la décision d'enquête ou les éléments de preuve susceptibles d'être transférés à la suite de son exécution pourraient conduire à poursuivre ou punir à nouveau une personne qui a déjà été jugée définitivement, pour les faits faisant l'objet de la décision, par les autorités judiciaires françaises ou celles d'un autre Etat membre de l'Union européenne lorsque, en cas de condamnation, la peine a été exécutée, est en cours d'exécution ou ne peut plus être ramenée à exécution selon les lois de l'Etat de condamnation ;*

*6° Si les faits motivant la décision d'enquête européenne ne constituent pas une infraction pénale selon la loi française alors qu'ils ont été commis en tout ou en partie sur le territoire national et qu'il existe des raisons sérieuses de penser qu'ils n'ont pas été commis sur le territoire de l'Etat d'émission ;*

*7° S'il existe des raisons sérieuses de croire que l'exécution de la mesure d'enquête serait incompatible avec le respect par la France des droits et libertés garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et la charte des droits fondamentaux de l'Union européenne ;*

*8° Si les faits motivant la décision d'enquête ne constituent pas une infraction pénale selon la loi française, sauf s'ils concernent une catégorie d'infractions mentionnée à l'article 694-32 et sanctionnée dans l'Etat d'émission d'une peine ou une mesure de sûreté privative de liberté d'une durée d'au moins trois ans, ou sauf si la mesure demandée est l'une de celles mentionnées par l'article 694-33 ;*

principe de la reconnaissance mutuelle ne se substitue pas à la forme classique d'entraide pénale internationale de la convention de 1959[202], conservant ainsi la possibilité d'échanger les informations par voie diplomatique entre les Etats. Il s'infère donc que la confiance mutuelle entre les Etats de l'UE peut être compressée ou même écartée[203]. Cet état de chose, en matière de lutte contre la cybercriminalité, a atteint un stade inquiétant dans la mesure où la décision-cadre relative au mandat européen d'obtention des preuves[204] donne la faculté aux Etats membres de préférer l'exécution du mandat par voie diplomatique plutôt que par voie directe, c'est-à-dire entre autorités judiciaires. Ainsi comme le souligne le professeur Brigitte Péreira, cette situation rend la procédure parfois chronophage et le risque de déperdition des éléments de preuve n'est pas à négliger[205]. Ce constat justifie peut-être l'idée selon laquelle nombre d'Etats européens sont réticents à mobiliser la décision-cadre sur le mandat d'obtention des preuves. Cela a été souligné en effet en mars 2015 par le secrétaire du Comité de la Convention sur la cybercriminalité en ces termes « *le processus de demande d'entraide judiciaire est jugé inefficient, et en particulier pour ce qui concerne l'obtention des preuves électroniques ; les Parties semblent ne pas mettre pleinement à profit les opportunités offertes par la Convention de Budapest sur la cybercriminalité et par d'autres accords afin de parvenir à une entraide efficace…* »[206].

Par ailleurs, en marge de l'Union européenne, certains Etats ont la réputation d'être moins coopératifs dans le domaine cybernétique, alors que la grande majorité des cyberattaques tirent leur source depuis ces pays. Il s'agit des pays comme la Russie, la Chine, l'Indonésie et la Chine. Selon Troels Oerting, à l'époque Chef du EC3, en 2014, 85% des affaires judiciaires européennes concernent des organisations criminelles russophones.

En somme, la réussite d'une entraide internationale reste suspendue à l'existence préalable d'accord entre les Etats. En matière de cybercriminalité organisée, cette entraide internationale est incontestablement l'apanage pour réaliser une meilleure enquête voire pour contrecarrer l'expansion d'un phénomène aussi complexe que la cybercriminalité. Toutefois, même s'il existe en France et au sein de l'UE, des efforts pour faire face au défi que constitue cette

---

*9° Si la mesure demandée n'est pas autorisée par le présent code pour l'infraction motivant la décision d'enquête, sauf s'il s'agit d'une des mesures mentionnées à l'article 694-33.*

*Dans les cas mentionnés aux 1°, 2°, 5°, 6° et 7° ci-dessus, avant de décider de ne pas reconnaître ou exécuter, en tout ou partie, une décision d'enquête européenne, le magistrat saisi consulte l'autorité d'émission par tout moyen approprié et, le cas échéant, demande à cette autorité de lui fournir sans tarder toute information nécessaire.*

*Le magistrat saisi informe l'autorité d'émission, sans délai et par tout moyen permettant de laisser une trace écrite, de toute décision prise en application du présent article.*

[202] Convention européenne d'entraide judiciaire en matière pénale, Strasbourg, 20 avril 1959, STCE n° 030.
[203] La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité, Brigitte Pereira, revue internationale de droit économique, cairn, 2016, https://www.cairn.info/revue-internationale-de-droit-economique-2016-3-page-387.htm#re84no84
[204] Conseil UE, décision-cadre n° 2008/978/JAI du 18 décembre 2008, *JOUE*, L 350, 30 décembre 2008, p. 72
[205] Ibid.
[206] A. Seger, « La coopération internationale contre la cybercriminalité : stratégie et défis », *Conseil de l'Europe*, 9-10 mars 2015, p. 12.

criminalité, ceux-ci n'auront réelle concrétisation que si leur mise en œuvre dans le cadre d'une coopération sereine rende la plus flexible possible l'accessibilité aux données externalisées.

Mais, les problèmes d'inaccessibilité ne sont pas les seuls enjeux que posent le défi de la constitution de la preuve numérique. En effet, la collète de la preuve dans un environnement aussi illimité que le cyberespace amène aussi peut se révéler parfois attentatoire à la liberté privée, ce qui amène à s'interroger sur l'épineuse question liée à la délimitation de la sphère privée des personnes mises en causes au moment de la recherche des traces numériques.

## § 2 : Des difficultés de conciliation de la collecte des données avec le respect effectif de certains droits fondamentaux constitutionnellement garantis

Le respect des droits de l'homme pose un véritable enjeu en matière d'investigation numérique. Cela tient notamment au caractère dématérialisé du cyberespace, ce qui soulève les difficultés quant à la délimitation de la sphère privée (**A**) et aussi du fait qu'entre plusieurs atteintes, les moyens dont disposent l'Etat oblige les enquêteurs à effectuer un tri, ce qui discrimine les victimes (**B**).

### *A. Une investigation numérique jugée parfois attentatoire au droit à la vie privée : le cas spécifique des interceptions de masse et de la durée de conservation des données personnelles*

Premièrement, avec la loi « renseignement » votée par le Parlement le 23 juin 2015, il est en effet désormais possible de considérer comme étant légal les missions de renseignement des services secrets d'Etat. Mais les lignes de cette loi qui ont provoqué la colère de certains politiques et associations, ayant conduit à la saisine du Conseil constitutionnel, sont celles qui augmentent considérablement le pouvoir de ces services de renseignement, avec pour conséquence de constituer une atteinte injustifiée à la vie privée des suspects. En en réalité, cette loi, à sa sortie de la fabrique parlementaire, étendait, sous la surveillance de la Commission nationale de contrôle des techniques de renseignement (CNCTR), la compétence des services de renseignement au-delà du champ du terrorisme, prenant ainsi en compte la surveillance électronique des communications de masse à l'échelle internationale, lorsqu'il s'agit, notamment, d'assurer la défense des intérêts majeurs de la politique étrangère, c'est-à-dire des intérêts économiques, scientifiques, et industriel. Concrètement, les services de renseignement auront la possibilité de recourir à des missions comme l'interception de communications, la sonorisation de véhicules ou de domiciles, la pose de balise de géolocalisation, la sollicitation en temps réel du réseau auprès des fournisseurs d'accès à Internet afin d'obtenir des données ou encore l'utilisation de IMSI Catcher, des dispositifs portables fonctionnant comme une antenne relais et permettant ainsi d'intercepter toutes les communications mobiles à proximité. Cette loi introduit en outre de nouvelles techniques, et notamment la « boîte noire », un algorithme censé détecter sur le réseau les comportements « suspects » et ainsi repérer les apprentis terroristes avant même qu'ils ne passent à l'acte. L'ensemble de ces missions est effectué sous le contrôle du pouvoir exécutif, avec la possibilité de recourir à la juridiction administrative en cas d'abus de pouvoir. C'est-à-dire que, bien que

la liberté des personnes soit en jeu, le pouvoir de l'autorité judiciaire[207] est absent dans ce domaine. C'est en tout cas, ce qu'a approuvé le Conseil constitutionnel en jugeant que le « recueil de renseignements par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la police administrative » et non du champ judiciaire. Cette position du Conseil semble s'accorder avec la CEDH dans l'affaire Klass, dans laquelle elle avait reconnu au législateur allemand, le pouvoir discrétionnaire quant au choix des modalités de surveillance[208]. Toutefois, cette décision de la Cour a été remise en cause tant par la Cour de justice de l'Union européenne que par plusieurs rapports des instances de l'ONU, et a donné lieu à divers points de vue dans les arrêts Roman *Zakharov* c. *Russie* et *Szabó* et *Vissy* c. *Hongrie*[209].

Ensuite, le Conseil ajoute que ces mesures s'inscrivent dans la prévention des troubles graves à l'ordre public. En revanche, les informations recueillies dans le cadre de ces missions ne peuvent être utilisées pour la constitution d'une infraction en vertu du principe de la séparation du judiciaire de l'administratif. Dans l'affaire dite de Tarnac où Julien Coupat a été mis en examen pour les faits de sabotage d'un réseau de transport ferroviaire de la société SNCF, ses avocats ont dénoncé la loyauté de la procédure au motif que les informations qui constituaient le fondement des accusations portées contre lui et son groupe ont été celles confiées par les services de renseignement britannique aux autorités françaises, lesquelles portaient les charges d'une potentielle appartenance de ces personnes à la mouvance anarchiste internationale. Ce qui semblait cohérent dans la mesure où les autorités de poursuite judiciaire ne peuvent fonder leur poursuite sur des informations reçues dans le cadre de procédure extrajudiciaires. Il s'agit là sans doute d'une atteinte au droit à la vie privée des personnes suspectées et aussi au à la loyauté de la procédure.

Par ailleurs, sur l'interception internationale de masse, la position du Conseil a été des plus protectrice de la vie privée des individus. En réalité, il a constaté l'inconstitutionnalité de l'article L 854-1 de ladite loi qui autorisait l'interception internationale de masse, au motif que les dispositions de cet article souffraient d'une imprécision suffisante qui se révélait attentatoire aux libertés publiques. Dans son arrêt *Weber* et *Saravia* contre l'Etat allemand du 29 juin 2006, repris en juillet 2008 dans l'arrêt Liberty contre Royaume-Uni, la Cour européenne des droits de l'homme s'était montrée trop exigeante sur l'effectivité de l'article 8 de la convention européenne des droits de l'homme en posant quelques garanties minimales que devaient présenter les interceptions internationales de masses afin d'être érigées au titre de mesure conventionnelle. Parmi ces garanties quelques-unes présentent un véritable enjeu d'application. Il s'agit notamment de la précision de la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées, la protection de confidentialité, la prise en charge des interceptions par une autorité indépendante. Cela a fait l'objet de deux décisions récentes rendues le 25 mai 2021 par la CEDH dans les arrêts *Big Brother Watch* et *Centrum För Rättvisa*.

[207] L'autorité judiciaire est le garant de la liberté des personnes en vertu de l'article 66 de la constitution
[208] CEDH, Klass contre Allemagne
[209] La CEDH et la surveillance de masse, François DUBUISSON, 2016, P.864-865

A l'origine de la première affaire était en cause les révélations du lanceur d'alerte américain Edouard Snowden dans le cadre de la mise en œuvre des relations bilatérales entre les services de renseignement britannique et ceux des USA. Si la Cour, sur le fondement de l'article 8 de la convention européenne, ne remet pas en cause la nécessité de cet accord bilatéral basé sur un échange d'informations entre les deux puissances en vue de lutter contre les menaces d'une gravité extrême, elle constate toutefois dans le paragraphe 347 de sa décision que « l'interception en masse recèle à l'évidence un potentiel considérable d'abus susceptibles de porter atteinte au droit des individus au respect de leur vie privée ». Afin donc de garantir contre l'arbitraire qui peut résulter de la mise en œuvre de cette mesure d'interception, la Cour a jugé « *que la transmission, par un État contractant, d'informations obtenues au moyen d'une interception en masse à des États étrangers ou à des organisations internationales devrait être limitée aux éléments recueillis et conservés d'une manière conforme à la Convention, et qu'elle devrait être soumise à certaines garanties supplémentaires relatives au transfert lui-même.* ***Premièrement, les circonstances dans lesquelles pareil transfert peut avoir lieu doivent être clairement énoncées dans le droit interne***. ***Deuxièmement, l'État qui transfère les informations en question doit s'assurer que l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées. L'État destinataire doit, en particulier, garantir la conservation sécurisée des données et restreindre leur divulgation à d'autres parties.*** *Cela ne signifie pas nécessairement qu'il doive garantir une protection comparable à celle de l'État qui transfère les informations, ni qu'une assurance doive être donnée avant chaque transfert. Troisièmement,* ***des garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière*** *– par exemple, s'il s'agit de communications journalistiques confidentielles. Enfin,* ***la Cour considère que le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant*** *»*[210]. C'est-à-dire que, comme l'interprète le professeur Jean-Pierre Marguénaud, « le processus doit être encadré par des « garanties de bout en bout ». Autrement dit, au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori »*[211]. Cette position de la CEDH reprend en majeur partie le contenu de sa décision dans l'arrêt *Uzun*, rendu contre l'Allemagne en 2010 sur la surveillance secrète interne. Elle avait jugé que *« pour apprécier si les mesures (de surveillance secrète) bénéficient des garanties adéquates et suffisantes, il faut se référer à l'étendue et à la durée de ces mesures, aux conditions requises pour les ordonner, à la désignation des autorités compétentes pour les*

[210] CEDH 25 mai 2021, Big Brother Watch et autres c. Royaume-Uni, req. n[os] 58170/13, 62322/14 et 24960/15, P§362.

[211] La Cour encadre l'interception en masse des communications, J-P Marguénaud, Dalloz, 6 juillet 2021, https://www.dalloz-actualite.fr/flash/chronique-cedh-cour-encadre-l-interception-en-masse-des-communications

*permettre, les mettre à exécution, et les contrôler, et au titre de recours fourni par le droit interne ».*

Le sujet relatif à la durée de conservation des données à caractère personnel par les fournisseurs est aussi bien plus tendu plan national et régional entre les autorités politico-judiciaire. En effet, dans un rapport produit en 2019 par les agences européennes, celle-ci se plaignent de l'absence de conservation unifiée des données, de sorte que cela constitue un enjeu majeur dans les enquêtes de cyberattaques. Toutefois, la Cour de justice de l'UE reste intransigeante sur une durée de conservation moins longue des données à caractère personnel. Dans un arrêt du 8 avril 2014[212], elle a invalidé au motif qu'elle violait les droits fondamentaux, une directive des autorités irlandaises demandant aux fournisseurs nationaux de conserver pour une durée de 6 à 24 mois les données de communication téléphoniques des usagers afin que les forces de police puissent s'en servir aux fins de prévention et d'enquête sur le terrorisme et la criminalité grave. Cette décision a causé un déchainement généralisé de déresponsabilisation de la part de plusieurs autres fournisseurs qui se sont retiré d'office des obligations de conservation à longue durée à leur imposer par les autorités politiques nationales (ex : affaire Télé2sverige contre la Suède, et Tom Watson, Peter Brice et Geoffrey Lewis contre le Royaume-Uni). Cela dit, la Cour de justice européenne pratique une politique de vigilance sur le respect de ma vie privée des citoyens quitte à aller, s'il le faut, contre toute politique pénale de collecte d'information trop intrusive des libertés fondamentales.

En somme le devoir des Etats européens est de protéger leurs citoyens. Cela justifie la mise en place de mesures d'interception des communications à grande échelle, lesquelles sont, par exemple, dans le cas de la lutte contre les cyberattaques de grande ampleur, susceptibles d'éviter des atteintes graves à plusieurs valeurs. Toutefois, l'interception internationale de masse doit être entourée de garanties conventionnelles et légales permettant de protéger la vie privée des personnes suspectées. Aussi, les autorités répressives ne doivent-elles ordonner injustement une conservation trop longue des données de communications des usagers au détriment d'une politique de prévention ou d'enquête.

La recherche de cet équilibre entre intérêt général et droits fondamentaux est parsemée d'embuches auxquelles sont confrontés les enquêteurs. Cela fait que, trop souvent, l'opportunité de l'action publique joue en faveur de classement sans suite. De sorte que certaines personnes encaissent injustement les atteintes dont elles ont été victimes.

### B. ***Des conditions de poursuite de certaines E-escroquerie jugées parfois restrictives du droit à la justice pour insuffisance de preuve numérique ou de moyens***

Comme précisé dans le rapport « Protéger les internautes » plusieurs fois cité dans les présents travaux, l'escroquerie en ligne constitue la forme de cybercriminalité la plus répandue. Qu'il s'agisse de l'escroquerie à la nigériane qui exploite la crédulité des victimes (faux appel à la charité, fraude à la loterie, fausse romance) ou de la fausse vente en ligne, Internet est devenu un véritable lieu de banditisme où l'argent se gagne facilement. La difficulté majeure est que l'ensemble des plaintes des victimes n'est souvent fondé sur aucune preuve, parce que les mails sont effacés, les personnes ont agi sous un nom ou ont eu recours aux logiciels

[212] CEDH Digital Rigths Ireland et Seitlinger, 8 avril 2014

d'anonymisation sophistiqués. Ainsi, à défaut d'éléments suffisants de nature à identifier le ou les auteurs, ou de précédentes plaintes ou dénonciations au sujet d'une même modalité d'opérer, pouvant permettre de faire un rapprochement[213], il s'offre au parquet territorialement compétent la seule possibilité un lourd embarras de choix d'enclencher ou non l'action publique. Mais le constat en est qu'en raison des dotations en frais de justice souvent limités, l'ensemble des parquetiers préfère jouer à la carte de priorité. Pour cela, pour les affaires de moindre importance, la réquisition par exemple d'un fournisseur de service en Internet en vue d'obtention d'une adresse IP peut être rare. Ce qui limite le droit de la victime à la justice.

Par ailleurs, même lorsqu'un fournisseur a été saisi et que son travail a permis d'avoir une adresse IP situant le délinquant sur le territoire national, s'il en résulte que la personne suspectée ne réside pas dans le ressort de la première juridiction saisie, il va y avoir un transfert de dossier vers le parquet compétent. Dans ce cas, le risque de déperdition de temps et d'énergie n'est pas négligeable. Lorsque l'adresse IP permet d'identifier un escroc à l'étranger, le parquetier devra encore juger de l'opportunité de mettre en œuvre une demande d'entraide pénale internationale qui nécessite d'important moyens à la charge de l'Etat demandeur.

[213] Dans la pratique, une action de poursuite pour escroquerie en ligne n'est mise en œuvre qu'à la suite de milliers de plaintes pouvant permettre de faire le rapprochement vers un mode opératoire.

## Elément de conclusion

L'enjeu que pose la cybercriminalité aux Etats relativise leur autosuffisance à lutter contre cette criminalité qui se veut par nature transfrontière. En témoignent, les récentes actualités de vague d'escroqueries en ligne liées à la pandémie de Covid. Plus encore, la constitution de la preuve numérique d'une cyber infraction reste parfois un enjeu défiant le pouvoir répressif des Etats. Si dans son propre système, la France dispose d'un important arsenal tant juridique qu'opérationnel pour faire face aux implications parfois ou peut-être même trop souvent complexe de la recherche des traces numériques à la suite de la commission d'une cyber infraction, elle s'est aussi montrée ouverte à presque tous les accords de coopération signée par l'Union européenne dans ce domaine. Elle s'est engagée avec elle dans la réussite du deuxième protocole additionnel à la Convention de Budapest afin de renforcer l'entraide pénale internationale qu'incarne ce texte.

Malheureusement, il est des cas où son pouvoir se trouve limiter à plusieurs aléas, lesquels constituent dans la plupart du temps un obstacle difficile pour les enquêteurs et les autorités judiciaires. La preuve numérique dans une procédure de cybercriminalité est fondamentale, elle est devenue sa pièce maitresse en dehors des aveux, témoignages et de l'écrit-papier. Son traitement est particulier et requiert de compétences spécifiques, quotidiennement actualisées en technologie numérique. Le nombre d'enquêteurs et de magistrats référents cybers disponibles aujourd'hui en France est très limité et insuffisant. La formation des cybers référents (magistrats et enquêteurs) doit être approfondie et actualisée en raison de la mutualité de cette criminalité. Aussi, serait-il nécessaire de mobiliser plus de ressources financières pour faire face aux exigences de la collecte de la preuve numérique dans ce sens, parce que le budget alloué au ministère de la justice reste tributaire d'une politique pénale de priorité, à laquelle chaque parquet doit malheureusement révérence. Ce qui constitue en conséquence, un revers de discrimination pour les milliers de français qui se font voler sur Internet. Cet état de chose fragilise la confiance dans le numérique, limite le rôle principal de la Justice et interroge sur l'efficacité ou la qualité de la protection pénale accordée aux français dans le cyberespace.

## Bibliographie

### Principales sources législatives et conventionnelles


- Code de procédure pénale
- Code pénal
- Code des postes et des communications électroniques
- Code de la protection des données personnelles
- Convention de Budapest sur la cybercriminalité
- Premier protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de natures racistes et xénophobes commis par le biais des systèmes informatiques
- Deuxième Protocol à la convention sur la cybercriminalité, relatif à la divulgation accélérée des informations (en l'étude)
- Convention européenne d'entraide judiciaire en matière pénale
- Convention européenne de sauvegarde des droits de l'Homme
- Traité de fonctionnement de l'Union européenne
- Discision-cadre 2003/577/JAI du conseil du 22 juillet 2003relative au gel de bien et de données de preuve
- Décision-cadre 2008/978/JAI du conseil du 18 décembre 2008 relative au mandat européen d'obtention de preuve
- Directive 2013/40 du Parlement et d Conseil relative aux attaques contre les systèmes informatiques remplaçant la décision-cadre 2005/222/JAI
- Directive d'enquête européenne du 03/04/2014
- Le règlement européen pour la protection des données à caractère personnel du 27 avril 2016
- Règlement relatif à l'injonction européenne aux fins de conservation et préservation des données (à venir)
- Traite MLAT


### Ouvrages


- Le rôle du juge pénal dans la recherche de la preuve" in Mélanges en l'honneur de G. Giudicelli-Delage, Humanisme et Justice, Dalloz, 2016
- P. Bouzat, "La loyauté dans la recherche des preuves", Mélanges Hugueney, 1964
- J. Domat, "Les lois civiles dans leur ordre naturel", Paris, éd. Cavelier, t.1, 1771
- L'ICANN et les problématiques d'abus de DNS, séminaire cyber référents, Laurent Ferrali, 112 juin 2021
- La preuve numérique à l'épreuve du litige, colloque CENJI
- Manuel des experts, A. Marescq aîné, Paris, 1881
- Initiation au fonctionnement de l'Internet et aux enjeux de la gouvernance internet, SDCL, DACG, juin 2021

- Cornu G., « Vocabulaire juridique », 10 éd., PUF, 2014
- R. GARRAUD, Traité théorique et pratique d'instruction criminelle et de procédure pénale, Larose et Ténin, 1909, Tome 1

**Source doctrinale**

- La preuve numérique, entre continuité et changement de paradigme, Etienne VERGES, éd. Justice actualité n°21, juin 2019
- « Prévenir des actes de cybercriminalité dans un contexte professionnel », Martine Exposito, UNJF
- L'expertise criminelle en France, M. GENESTEIX, A. Pédone, 1900
- Philosophie Droit : L'intime conviction, norme démocratique de la preuve ?, Jean Danet,
- La preuve pénale, Sylvie GRUNVALD, Jean D., UNJF
- Sécurité de l'information par stéganographie basée sur les séquences chaotiques, Dalia Battikh, HAL
- La preuve numérique, un défi pour l'enquête criminelle du 21è siècle, Eric Fresseynet, Cairn, 2003
- Sécurité et stratégie, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », Miriam Quéméner, cairn, 2011
- La fraude informatique, Abdoulaye Salifou, 2016
- Les perquisitions informatiques à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données, étude comparé en droit français et états- uniens, Alexandre Rousselet-Magri, Cairn, 2017
- Cybercriminalité, jouer d'un nouvel espace sans frontière, D. Bénichou, AJ pénal, 2005,
- La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité, Brigitte Pereira, revue internationale de droit économique, cairn, 2016,
- La CEDH et la surveillance de masse, François DUBUISSON, 2016, P.864-865
- La Cour encadre l'interception en masse des communications, J-P Marguénaud, Dalloz, 6 juillet 2021

**Rapports** :

- Rapport « protéger les internautes », 2016
- Rapport annuel sur la cybercriminalité organisée en France, Direction générale de la PN, et de gendarmerie nationale, Sirasco, éd., 2019

**Jurisprudences principales**

- CEDH, Digital Rights Ireland Seitlinger, 8 avril 2014
- Crim., 19 mars 2014, Bull 1193, n° 12-87-416
- Cass. crim., 15 juin 1993, Bull.
- Microsoft Corp. v. United States ; april 17, 2018
- Cass. Crim. 6 novembre 2013, n°12-87.130
- Cass. Crim. 14 nov. 2013, n°12-87.346
- Cass. Crim., 19 jan. 2016 n° 15.81.041, Bull. n°14

- Cons. Const., n° 2011-113/115 QPC
- CEDH, 13 janvier 2009, Taxquet contre Belgique, requête n° 926/05
- CA Paris, 16 Avr. 2019, n°18/09267
- Crim., 10 déc., 2019 n°18-86.878
- TJ Limoges, 22 avril 2021 n°494 /2021
- *CEDH* Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021, req. n$^{os}$ 58170/13, 62322/14 et 24960/15, P§362.
- CEDH Centrum För Rättvisa c. Suède n° 35252/08 25 mai 2021

**Liens internet**

- https://www.dalloz-actualite.fr/flash/chronique-cedh-cour-encadre-l-interception-en-masse-des-communications
- https://www.cairn.info/revue-internationale-de-droit-economique-2016-3-page-387.htm#re84no84
- https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2017-4-page-659.htm
- https://tel.archives-ouvertes.fr/tel-01275346, 2016
- https://fr.wikipedia.org/wiki/St%C3%A9ganographie
- https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm
- https://www.wsws.org/francais/News/2002/janvier02/5janv02_moussaoui.shtml
- https://www.tracip.fr/nos-produits/logiciels/x-ways-forensics/
- https://www.loi1901.com/intranet/a_news/index_news.php?Id=2630
- https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/
- https://fr.wikipedia.org/wiki/Centre_europ%C3%A9en_de_lutte_contre_la_cybercriminalit%C3%A9,
- https://eurlex.europa.eu/legalcontent/FR/TXT/?uri=CELEX%3A52019XG1209%2802%29&qid=1625574487088
- https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/
- https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/pdf
- https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/,
- https://www.cnil.fr/fr/le-systeme-api-pnr-france,
- https://www.paymon.fr/2015/03/12/la-geolocalisation-nouvelle-arme-de-visa-pour-lutter-contre-la-fraude/
- Convention sur la cybercriminalité — Wikipédia (wikipedia.org)
- https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/8eme-Conference-INTERPOL-Europol-sur-la-cybercriminalite-Plus-de-la-moitie-de-l-humanite-court-un-risque
- http://resources.mcafee.com/content/NAUnsecuredEconomiesReportwww.lemonde.fr/web/depeches/0,14-0,39-38313716@7-37,0.html

- https://www.cairn.info/revue-securite-et-strategie-2011-1-page-56.htm
- https://www.leparisien.fr/high-tech/cybersecurite-enquete-sur-le-rancongiciel-egregor-cauchemar-absolu-des-entreprises-02-12-2020-8411844.php
- https://www.cyberveille-sante.gouv.fr/cyberveille/1166-le-ransomware-lockergoga-identifie-lors-dune-attaque-contre-altran-2019-02-01
- https://fr.wikipedia.org/wiki/Petya
- D'où vient la cybercriminalité ? : Origines et évolution. | Le VPN (le-vpn.com)
- http://www.senat.fr/rap/r19-613/r19-6134.html
- https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/
- https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Histoire-de-la-police-judiciaire
- https://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=uriserv%3AOJ.C_.2014.175.01.0006.01.FRA