PANTHÉON-ASSAS
UNIVERSITÉ
PARIS

BANQUE DES MEMOIRES

Master de Droit du numérique
Dirigé par M. le professeur Jérôme Passa
2024

L'encadrement de la violence numérique et du risque cyber par les autorités

Elie Blanchard

Sous la direction de Me. Marc-Antoine Ledieu

Remerciements

Il m'était impossible de ne pas adresser ma reconnaissance à toutes les personnes qui m'ont aidé à rédiger ce mémoire.

Je tiens tout d'abord à remercier mon directeur de mémoire, Me. Marc-Antoine LEDIEU, pour avoir contribué à me donner goût à la cybersécurité, dans le cadre d'un enseignement concret, compréhensible et ludique, alliant rigueur juridique et de nombreuses références à la pop-culture qui ont rendu la matière moins abrupte qu'elle ne l'est au premier abord.

Je tiens également à exprimer ma gratitude envers le corps enseignant du Master 2 Droit du numérique de l'Université Paris-Panthéon-Assas, notamment à Me. François COUPEZ et Me. Ilène CHOUKRI, dont les enseignements m'ont grandement aidé à réaliser ce travail.

Merci à mes parents et à mes amis, qui ont pris le temps de (beaucoup) m'écouter parler de ce mémoire et qui m'ont soutenu, conseillé et encouragé.

Enfin, je remercie grandement toutes les personnes, connues et anonymes, ayant répondu et diffusé le questionnaire que j'ai élaboré, contribuant à enrichir la documentation de ce travail.

Liste des abréviations

ABE : Autorité bancaire européenne

AMRAE : Association pour le management des risques et des assurances de l'entreprise

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

Arcom : Autorité de régulation de la communication audiovisuelle et numérique

BCE : Banque centrale européenne

C3N : Centre de lutte contre les criminalités numériques

CECA : Comité européenne du charbon et de l'acier

CEPD : Comité européen de la protection des données

CNIL : Commission nationale de l'informatique et des libertés

CNPEN : Comité national pilote pour l'éthique du numérique

CP : Code pénal

CPI : Code de la propriété intellectuelle

CPP : Code de procédure pénale

CRA : *Cyber Resilience Act*

CRiP : Club des responsables d'infrastructure de technologies et de production IT

CyCLONe : *Cyber Crisis Liaison Organisation Network*

DDoS : *Distributed Denial of Service (attack)*

DMA : *Digital Markets Act*

DORA : *Digital Operational Resilience Act*

DSA : *Digital Services Act*

ENISA : *European Union Agency for Cybersecurity*

IA : Intelligence artificielle

ISO : *International Organization for Standardization*

IT : *Information Technology*

LLM : *Large Language Model*

LPM : Loi de programmation militaire

MFA : Authentification multifactorielle

MPA : Menace persistante avancée

NIS : *Network and Information Security*

NTIC : Nouvelles technologies de l'information et de la communication

OFAC : Office anti-cybercriminalité

OSINT : *Open Source Intelligence*

P2P : *Peer-to-peer*

PCA : Plan de continuité d'activité

PGP : *Pretty Good Privacy*

PMIA : Programme mondial pour l'intelligence artificielle

PRA : Plan de reprise d'activité

PSP : Prestataire de services de paiement

RGPD : Règlement général sur la protection des données

SaaS : *Software as a Service*

SCADA : *Supervisory Control And Data Acquisition*

SI : Système d'information

SIA : Système d'intelligence artificielle

STAD : Système de traitement automatisé de données

TFUE : Traité sur le fonctionnement de l'Union européenne

TUE : Traité sur l'Union européenne

VPN : *Virtual Private Network*

UE : Union européenne

URL : *Uniform Resource Locator*

Sommaire

Remerciements **2**

Liste des abréviations **3**

Sommaire **5**

Avant-propos **6**

Introduction générale **7**

I] L'appréhension de la violence numérique par le droit : les lacunes d'une approche générale et traditionnelle **13**

A) La violence numérique : une mutation cyber de la criminalité 13
1- La transformation et l'amplification des délits originels par le numérique 13
2- Les nouveaux actes illicites créés par le numérique 16

B) La frénésie législative européenne : une élévation des standards de sécurité difficilement applicable 20
1- La création d'un bloc législatif numérique européen 20
2- La décorrélation entre les exigences théoriques et la réalité technique 23

C) Les contraintes inhérentes au droit : une entrave dans la lutte contre la cybercriminalité 26
1- Les difficultés d'appréhension de la cybercriminalité 26
2- Les difficultés de répression de la cybercriminalité 29

II] L'appréhension de la violence numérique par la cybersécurité : le besoin d'une approche pragmatique et opérationnelle **33**

A) La spécialisation des autorités en matière cyber : l'objectif d'un encadrement plus efficient 33
1- La création de nouvelles autorités et la spécialisation des existantes 33
2- La coopération internationale : une meilleure coordination dans la prise en main du phénomène cyber 37

B) L'ambivalence des nouvelles technologies : outils de lutte et supports d'illicéité 40
1- Des outils au service des individus et des autorités 40
2- Des outils comme support d'illicéité et d'accroissement du risque cyber 43

C) La nécessaire coopération entre autorités publiques et acteurs privés : des intérêts et bénéfices partagés 46
1- La sécurité des systèmes d'information : pour une meilleure protection des droits fondamentaux 46
2- L'imprégnation du secteur privé dans les autorités publiques : la spécialisation pour un meilleur encadrement 50

Conclusion **53**

Annexe **54**

Bibliographie **66**

Avant-propos

Aborder, dans un mémoire de recherche, la violence numérique et le risque cyber n'est pas chose aisée : le sujet est vaste, à l'instar de la documentation existante. Cela requiert à la fois des connaissances juridiques et techniques, dans une interdépendance constante de ces deux notions. Il semblait donc impossible de traiter séparément l'un et l'autre. Cependant, pour simplifier, la violence numérique sera souvent employée ici pour qualifier de manière générique le risque cyber et vice versa, excepté lorsque leurs spécificités nécessiteront une approche propre ; auquel cas, ils seront clairement distingués.

La plus grande difficulté de ce sujet a été de le borner, tant il y a à dire et tant il restera à dire après la dernière ligne de ce mémoire. Il est bien évident que certaines problématiques ayant des enjeux en termes de cybersécurité et de réglementation (telles que la *blockchain*, les cryptomonnaies, les *smart contracts*, l'*OSINT* ou le *cloud*) ne seront pas abordées ici, ou seulement de manière subsidiaire, faute de pages à disposition.

En outre, pour enrichir et rendre plus concret ce travail de recherche, j'ai pris l'initiative de réaliser un questionnaire général à visée statistique, composé de neuf questions et dont les réponses sont anonymes. L'objectif était alors d'obtenir un aperçu général de la vision des individus y répondant, profanes et spécialistes, sur certaines problématiques, techniques, juridiques et cyber. Les résultats de ce questionnaire sont présentés en annexe, assortis d'une brève description et interprétation des chiffres donnés.

Enfin, la cybersécurité, en tant que discipline s'appuyant sur l'informatique, elle induit de nombreux aspects transnationaux, et les anglicismes seront nombreux dans ce mémoire. Ainsi, les termes techniques seront souvent mentionnés une première fois en anglais, avec leur traduction dans les notes de bas de page. Pour ce qui est des œuvres, travaux et autres documents mentionnés, lorsque leur version originale n'est pas en français, ils seront mentionnés dans leur titre original.

Ces précisions étant faites, il est désormais possible de rentrer dans le cœur du sujet.

Introduction générale

Quel est le point commun entre les films *I, Robot*[1], *Her*[2], *Mission Impossible*[3], *Terminator*[4] et, *Silk Road*[5], *The Fifth Estate*[6] ou encore *Snowden*[7] ?

Ils traitent tous de cybersécurité ou de nouvelles technologies. Mais, tandis que les premiers en abordent les contours dans un cadre fictif, si ce n'est dystopique, les trois derniers sont des films biographiques, qui nous rappellent que les problématiques liées à la cybercriminalité ou aux nouvelles technologies ne sont plus aussi futuristes que telles qu'on les imaginait à l'époque du premier *Terminator*. En sorte, les usurpations d'identités numériques, les piratages, les escroqueries en ligne, les marchés noirs en ligne, la surveillance de masse en temps réel, etc. constituent toutes sortes de dévoiements résultant de l'essor des nouvelles technologies l'information et de la communication (NTIC). Pour lutter contre ces phénomènes, il est avant tout nécessaire d'en comprendre le fonctionnement et les enjeux. La violence numérique et le risque cyber sont deux notions distinctes, pourtant complémentaires, dont l'interaction et les contingences doivent être comprises, sans qu'elles ne soient confondues.

Tout d'abord, la violence numérique, ou cyberviolence, est avant tout un acte de violence, c'est-à-dire un acte qui « se manifeste, se produit ou produit ses effets avec une force intense, brutale et souvent destructrice »[8]. Elle est également définie comme « l'abus de la force physique »[9]. Selon cette définition et par syllogisme, la violence numérique serait alors l'abus de la force, non pas physique, mais digitale. Dès lors, considérant la force comme « la capacité à imposer sa volonté »[10], la violence numérique rassemblerait tous les moyens de contrainte exercés par l'intermédiaire d'un outil digital ; plus concrètement, tous les actes de violence

[1] A. PROYAS, *I, Robot*, Davis Entertainment; Laurence Mark Productions; Overbrook Entertainment; Canlaws Productions; Mediastream IV, 2004
[2] S. JONZE, *Her*, Annapurna Pictures, 2014
[3] B. DE PALMA, *Mission impossible*, Paramount Pictures, Cruise/Wagner Productions, 1996
[4] J. CAMERON, *Terminator*, Gale Anne Hurd, 1985
[5] T. RUSSELL, *Silk Road*, Perfect Season Productions, High Frequency Entertainment, Mutressa Movies, Piccadilly Pictures, 2021
[6] B. CONDON, *The Fifth Estate*, DreamWorks SKG Participant Media, 2013
[7] O. STONE, *Snowden*, Endgame Entertainment; KrautPack Entertainment; Wild Bunch; Onda Entertainment; Vendian Entertainment, 2016
[8] Définition issue du Dictionnaire Larousse : https://www.larousse.fr/dictionnaires/francais/violence/82071#:~:text=1.,La%20violence%20d'un%20choc.
[9] Idem
[10] Définition issue du Centre National de Ressources Textuelles et Lexicales : https://www.cnrtl.fr/definition/force

pouvant être commis par l'intermédiaire du *Web*, ou d'autres outils de communication électroniques.

Le risque cyber doit, quant à lui, peut être défini par ses deux composants : le risque, c'est-à-dire le danger ou inconvénient plus ou moins probable auquel on est exposé[11] et la notion de cyber, qui renvoie à l'environnement digital. Le risque cyber est donc au secteur numérique ce que les risques économique, social et environnemental sont au développement durable ; c'est-à-dire une somme de potentialités négatives qui ont trait à un domaine, pouvant porter atteinte à son essor. Au risque cyber, répond la notion de cybersécurité, qui rassemble toutes les actions nécessaires pour protéger les réseaux et les systèmes d'information[12], les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces.[13] La cybersécurité ne saurait être dissociée de la cyberrésilience, qui renvoie peu ou prou à la même réalité mais, là où la cybersécurité englobe plutôt les aspects de protection et de prévention, la cyberrésilience est pensée pour intervenir après que le risque se soit concrétisé. Il s'agit alors de mettre en place les mesures techniques et organisationnelles qui permettront de se relever d'un incident de sécurité[14]. Ces mesures se manifesteront souvent dans le cadre de plans de continuité et de reprise d'activité (PCA et PRA). Les PCA et PRA constituent des plans d'actions ou des ensembles de mesures, souvent mis en place par les entreprises, visant à matérialiser de manière concrète la stratégie adoptée pour assurer la sécurité des systèmes d'information. En somme, la cybersécurité et la cyberrésilience visent toutes deux à lutter contre les cyberattaques[15] et les cybermenaces de manière plus générales. Il est également utile de noter que le terme de cybersécurité est souvent employé de manière générique, regroupant les volets de protection et de remise en état, pour qualifier globalement la sécurité des systèmes d'information. Cette réalité de la cybersécurité s'appuie sur quatre piliers, théorisés bien après les premières manifestations

[11] Définition issue du Dictionnaire Larousse : https://www.larousse.fr/dictionnaires/francais/risque/69557#:~:text=se%20dit%20de%20quelqu'un,Grossesse%20%C3%A0%20risque.

[12] Article 6.1 DIRECTIVE (UE) 2022/2555 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

[13] Article 2.1 du REGLEMENT (UE) 2019/881 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité)

[14] Evènement indésirable ou inattendu présentant une forte probabilité de compromettre ou menacer la SSI

[15] Acte illicite réalisé par un pirate informatique visant à compromettre un SI ou s'attaquer aux données de la victime

de son existence et de sa nécessité : la disponibilité, l'intégrité, la confidentialité et la traçabilité des données.

Si violence numérique et risque cyber sont deux notions distinctes, elles sont cependant appelées à interagir. Pourtant, elles n'ont pas exactement le même champ : tandis que la violence numérique réunit tous les actes pouvant intenter à l'intégrité physique ou morale des individus (moins physique que morale lorsque la violence est numérique), le risque cyber menace, quant à lui, l'intégrité des systèmes d'information. Mais, les deux intégrités menacées par la violence numérique et le risque cyber ne sont pas pleinement compartimentées. Par exemple, l'installation d'un *ransomware*[16] dans le système d'information (SI) d'un hôpital peut, *in fine*, aboutir à une atteinte à l'intégrité d'un individu ; de même que la diffusion d'images à caractère privé sans consentement de la victime peut résulter de la récupération de ses mots de passe, c'est-à-dire de la concrétisation d'un risque.

Par principe, il n'existe que deux exceptions à l'interdiction de l'usage de la violence[17] : la légitime défense, dont les modalités sont détaillées à l'article 122-7 du Code pénal (CP), et la violence pour motif de recherche et de sécurité informatique, mentionnée à l'article 323-3-1 CP, c'est-à-dire l'usage de la violence numérique pour des raisons de cybersécurité. Encore une fois, cybersécurité et violence numérique tendent à interagir. Le vocabulaire marin étant quelquefois utilisé en matière de cybersécurité[18], il sera nécessaire de différencier, parmi les personnes usant de la force cyber le pirate (*hacker*), l'amateur et le corsaire. Le dernier se distingue des deux premiers en ce que son usage de la force cyber est contractuellement ou légalement légitimé par l'État, qui, faut-il le rappeler, est supposé disposer du monopole de la violence légitime[19]. On citera, comme dévoiement du monopole étatique de la violence légitime, les *hackers* légitimant leurs infractions pour des raisons « morales ». Au vu de la multiplication des délinquants prétendant agir pour le bien, une chose doit être clarifiée : ces *hackers*, quel que soit leur mobile, n'agissent pas dans la légalité. Le droit pénal est d'ailleurs, par principe, indifférent aux mobiles[20].

---

[16] En français, « rançongiciel ». Désigne, selon la CNIL dans sa plaquette de cybersécurité, un programme malveillant qui vise à empêcher, par le chiffrement, l'accès de la victime à ses données.

[17] M-A. LEDIEU, Enseignement méthodologique de sécurité des systèmes d'information, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

[18] Par exemple, le Projet Aronnax, inspiré de œuvre *20 000 lieues sous les mers*, J. VERNES, 1870

[19] M. WEBER, *Wissenschaft als Beruf* & *Politik als Beruf*, discours prononcés à l'université de Munich en 1917 et 1919

[20] X. PIN, *Droit pénal général*, édition 2024, Lefebvre Dalloz, septembre 2023

En quelques dizaines d'années seulement, le développement des nouvelles technologies s'est caractérisé par des capacités de stockage bien plus conséquentes et une vitesse de calcul démultipliée, grâce à l'avènement de processeurs toujours plus petits et puissants, d'un espace de stockage dématérialisé (*cloud*) toujours plus important – dû à la floraison de *datacenters*[21] partout sur le globe –, ou d'intelligences artificielles (IA) capables de battre le champion du monde du jeu de *Go*[22]. Dans ce contexte, comment les enjeux du développement des NTIC intègrent-ils le développement de la violence numérique et du risque cyber ?

On ne compte aujourd'hui plus le nombre de cyberattaques qui se produisent quotidiennement, allant de la simple intrusion dans un système d'information jusqu'au blocage complet d'une chaine d'approvisionnement. Les motifs de ces attaques sont, eux aussi, très nombreux : crapuleux, politiques, personnels, attaques par goût de l'amusement ou du défi, etc. Il existe principalement deux catégories d'attaques. Ces attaques peuvent être directes ou indirectes et ces deux catégories se déclinent en une multiplicité de formes. Une attaque directe consiste en la tentative de la part d'un individu malveillant de s'emparer du mot de passe ou de s'attaquer au système d'authentification de sa victime. Une attaque indirecte correspond à l'utilisation d'un procédé d'ingénierie sociale pour amener la victime à communiquer des informations personnelles[23]. La communication de ses identifiants par la victime pourra parfois être réalisée avec le consentement de cette dernière, se rapprochant alors du procédé de l'escroquerie[24].

Enfin, concernant les auteurs, il peut s'agir de groupes d'individus, agissant en bande organisée[25], ou d'États (et plus souvent des cellules secrètes aux services de ces derniers). Les cybercriminels sont en effet très rarement des individus isolés agissant par leurs propres moyens : c'est une image que les spécialistes s'évertuent aujourd'hui à démentir[26]. En guise de panel non exhaustif des cyberattaques, on peut par exemple recenser l'attaque par déni de service distribuée (*distributed denial-of-service attack / DDoS*) qui a visé plusieurs ministères en mars 2024, le vol de données de près de trente-trois millions d'individus sur les plateformes de Viamedis et d'Almerys en janvier 2024, le vol de code source et de documents sensibles chez

[21] En français, « centre de données ». Correspond au lieu où sont situés les serveurs et, à fortiori, où sont stockées les données
[22] Le Monde, « L'intelligence artificielle AlphaGo bat une nouvelle fois le champion du monde de go », 25 mai 2017
[23] Définition issue du MOOC SecNumacadémie de l'ANSSI, 18 mai 2017
[24] Article 313-1 du code pénal
[25] Article 132-71 du code pénal
[26] B. BADAUD, « Le darknet et le droit », La Semaine juridique. Édition générale, 25 avril 2018

Microsoft en mars 2024 ou encore plus récemment, le piratage de l'entreprise de machines à laver CSC ServiceWorks en mai 2024[27].

Tandis que la révolution numérique bat son plein[28], de la maitrise des nouvelles technologies découle une somme d'enjeux qui mériteraient chacun un développement spécifique. Il est tout d'abord question de la souveraineté numérique et juridique de l'Union européenne, qui s'évertue à légiférer en la matière[29], parallèlement à la résurgence de l'IA au centre du débat démocratique[30], notamment avec l'apparition de Chat GPT en novembre 2022. Le but est de tenter de donner tort à ceux qui penseraient – à raison pour l'instant – que le droit est à la remorque de la technologie[31] et faire en sorte que ces technologies soient utilisées à bon escient. Il est ensuite question des droits fondamentaux des individus, et des préoccupations que ces derniers peuvent avoir pour ce sujet, qui ne sont pas des moindres (**Voir Annexe : graphe questions 2 et 3**). D'autres branches du droit sont également influencées par le développement de ces technologies. Ce sont ces enjeux – et bien d'autres encore – dont les autorités, c'est-à-dire les États, doivent s'emparer pour garder la main sur l'évolution de ce phénomène. Mais, ne seront abordées ici les nouvelles technologies qu'en tant qu'elles sont liées au risque cyber et à la violence numérique, et pour définir comment elles ont été, sont et doivent ou ne doivent pas être encadrées.

Alors qu'en France des lois aujourd'hui assez anciennes comme la loi Godfrain[32] (récemment complétée par la loi du 21 mai 2024[33]) ou la loi Informatiques et Libertés[34] ont posé relativement tôt le socle de l'encadrement du secteur digital, l'Union européenne se construit aujourd'hui dans une logique de « frénésie législative »[35], qui témoigne de sa volonté de garder le contrôle. Le vieux continent s'oppose en cela aux États-Unis, forts d'une approche plus libérale, accordant sans doute moins d'importance aux droits et libertés individuels qu'à la

[27] A. GAYTE, "Ils hackent des machines à laver et arrivent à lancer des lessives gratuitement", Numerama, 21 mai 2024
[28] R. RIEFFEL, *Révolution numérique, révolution culturelle ?*, Gallimard, Folio Actuel, 2014
[29] Sur la base des articles 16 et 114 du Traité sur le fonctionnement de l'Union européenne
[30] En ce qui concerne la postérité des débats autour de l'ordinateur et de l'IA, voir : R. LAWLOR, avocat au barreau de Californie, "What Computers Can Do : Analysis and Prediction of Judicial Decisions", 1963
[31] Me. O. ORTEGA et Me. B. LOUIS, avocats associés au sein de LexCity, Le Point, 10 juin 2022
[32] Loi n°88-19 du 5 janvier 1988
[33] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique
[34] Loi n°78-17 du 6 janvier 1978
[35] S. PORTELLI, Conférence : « La place du juge pénal face à la frénésie législative », 2017

prééminence du marché, en témoignent ses nombreux investissements dans les nouvelles technologies.[36]

Dans ce cadre, il convient de se demander en quoi l'encadrement de la violence numérique et du risque cyber par les autorités doit obligatoirement allier une approche juridique à une approche applicative de cybersécurité pour être efficient.

Si la technologie n'est pas mauvaise en elle-même, elle doit cependant être régie par un certain nombre de règles pour que ses usages soient contrôlés. Tandis que le droit appréhende les domaines qu'il tend à régir de manière hétéronome, force est de constater que cette approche a des défauts face à la mutation de la violence et à l'accroissement du risque cyber (**I)**. En découle la nécessité d'appréhender violence numérique et risque cyber par une approche plus pragmatique et opérationnelle (**II**).

[36] Selon le rapport de la Commission « Notre Ambition pour la France », les investissements américains sont environ vingt fois plus élevés que les investissements français

I| L'appréhension de la violence numérique par le droit : les lacunes d'une approche générale et traditionnelle

L'histoire des vols, des extorsions, des escroqueries, des abus de faiblesse, du harcèlement et de la violence de manière générale, ne débute pas avec le numérique. L'être humain, fort de l'intelligence développée qui le différencie de la grande majorité des êtres vivants, s'est notamment illustré pour porter atteinte à son prochain. Ce phénomène n'a pas disparu avec le numérique, il a simplement suivi le cours de l'évolution (**A**). Conscient de l'ampleur du sujet, le législateur tente aujourd'hui d'endiguer ces phénomènes de violence numérique et de diminuer le risque cyber par l'élaboration d'un grand nombre de réglementations (**B**). Mais, pour lutter contre la cybercriminalité, le droit montre rapidement ses lacunes (**C**).

A) La violence numérique : une mutation cyber de la criminalité

Les infractions visant à arnaquer les victimes, souvent pour leur soutirer, avec ou sans leur consentement, une somme d'argent, ont connu une recrudescence, ainsi qu'une exacerbation de leurs conséquences avec le développement du numérique (**1**). En parallèle, d'autres d'actes illicites ont vu le jour (**2**).

1- La transformation et l'amplification des délits originels par le numérique

Les fraudes et arnaques en tous genres prospèrent depuis l'existence des sociétés humaines[37]. Il serait faux de croire que les premières formes de *phishing*[38] remontent à la création du courrier électronique, de même que, selon le colonel Jérôme Barlatier, il n'existe pas une délinquance propre au domaine cyber[39]. Pour cause, Internet est apparu comme un vecteur propice aux arnaques, par le relatif anonymat qu'il peut conférer et l'accroissement de la facilité pour atteindre les victimes potentielles. En vérité, les arnaques de la prisonnière espagnole ou de

[37] J. RIVIERE & D. LUCAS, « Criminalité et Internet, une arnaque à bon marché », Sécurité globale, 2008
[38] En français, « hameçonnage ».
[39] Podcast Les Temps Electriques, avec le colonel Jérôme Barlatier, « Cyberarnaques : quand l'internaute mord à l'hameçon », 21 avril 2023

la lettre de Jérusalem[40] correspondent *de facto* aux premières formes de *phishing*. Le moyen de communication interposée n'était simplement pas les courriers électroniques mais la lettre. Néanmoins, il s'agissait déjà à l'époque de jouer sur des traits de caractère humains tels que l'appât du gain, la volonté d'aider son prochain[41], la propension à se fier aux apparences et même, dans certains cas, la soumission à l'autorité, depuis longtemps démontrée par Stanley Milgram[42].

Même si, selon un rapport de Verizon, près de 90% des attaques vont impliquer le courriel[43], terrain propice du *phishing*, cette cyber arnaque est polymorphe : elle peut être réalisée par le fait de cliquer sur un lien, d'ouvrir une pièce jointe, de convertir un fichier ZIP[44], de scanner un *QR Code*[45], etc. *Whaling*, *Spear phishing*, *Quishing*, *angler phishing* et *spoofing* sont des déclinaisons de l'infraction générale qui tirent leur nom du contexte dans lesquels elles sont réalisées et des moyens mobilisés pour les mettre en œuvre. En substance, aujourd'hui, ce délit consiste à se faire passer pour un tiers de confiance (conseiller bancaire, membre de la famille, etc.) et de tromper la victime pour la pousser à céder de manière consentie une somme d'argent ou des données, telles que ses *credentials*[46] ou un code de carte bleue. À première vue, il s'agirait d'une escroquerie au sens de l'article 313-1 CP, car sont constitués tous les éléments matériels caractérisant le délit : l'usage d'un faux nom ou d'une fausse qualité, l'abus d'une qualité vraie ou le recours à des manœuvres frauduleuses, la remise d'une chose par la victime, lui causant un préjudice.

Au-delà de cette qualification pénale applicable (parmi bien d'autres), les législateurs français et européen se sont emparés d'un des aspects de la problématique du *phishing* en matière bancaire avec la directive DPS 2[47], transposée par l'ordonnance du 9 août 2017[48]. Ces textes visaient, entre autres, à réglementer l'indemnisation des victimes de *phishing* en matière

[40] P. ROPERT, « Histoires d'arnaques : du mail du prince nigérian aux « lettres de Jérusalem », France culture, 21 juin 2018
[41] Sur ce point, voir : Podcast, la cybersécurité expliquée à ma grand-mère, « C'est le jeu ma pauv Lucette », remixé le 26 mars 2023
[42] S. MILGRAM, « *Behavorial Study of Obedience* », Université de Yale, 1961
[43] Rapport Verizon, « Data Breach Investigations », 2023
[44] Le ZIP est un format de fichier permettant l'archivage et la compression de données sans perte de qualité : https://www.futura-sciences.com/tech/definitions/informatique-zip-18098/
[45] D. LICATA CARUSO, « Arnaques au QR code : phishing, vol de données... pourquoi il va falloir s'en méfier cet été », Le Parisien, 14 juillet 2022
[46] En français, « identifiants », au sens d'identifiant de connexion
[47] Directive (UE) 2015/2366 du 15 novembre 2015
[48] Ordonnance n°2017-1252 du 9 août 2017

bancaire (donc de *spoofing*) en obligeant les prestataires de service de paiement (PSP) à mettre en place une authentification forte, ou authentification multifactorielle (MFA) pour que les individus accèdent à leurs comptes bancaires et fassent des opérations de paiement[49]. L'interprétation donnée de ces textes par la Cour de cassation est allée encore plus dans le sens des victimes avec l'arrêt du 30 août 2023[50], mais l'appréhension de ce phénomène par le juge n'en est pas pour autant efficace. Alors même que la loi Godfrain existe depuis plusieurs années et a créé les qualifications pour sanctionner les actes comme le *phishing*[51], mais aussi d'autres actes illicites, les cyberdélinquants ne sont que peu, voire pas du tout, sanctionnés[52]. Pourtant, le *phishing*, quelle que soit la forme qu'il prend, est un phénomène hautement répandu ; rares sont les personnes qui n'ont jamais reçu un mail ou un SMS contenant un lien ou une pièce jointe piégés (**Voir en annexe : graphe question 9**).

Tandis que le phishing est la continuation cyber d'un phénomène centenaire, correspondant plutôt à une technique d'arnaque, le *Darknet* (ou *Dark Web*)[53] est un lieu où de nombreux actes illicites ont pu se déporter depuis sa création. Le *Darknet* est un réseau général au protocole différent de celui du *World Wide Web*[54], présentant un ensemble de pages consultables au sein d'un réseau intégrant une caractéristique d'anonymat, notamment grâce au chiffrement des données de connexion ainsi qu'au masquage des adresses IP[55]. Le *Darknet* se différencie du *Clear Web*, qui rassemble l'ensemble des pages accessibles par des moteurs de recherche, mais n'est qu'un sous-ensemble du *Deep Web*, qui renvoie, quant à lui, à l'ensemble des pages non indexées, et donc non accessibles via des moteurs de recherche classiques. Pour accéder à ces pages, il faudra soit posséder le *Uniform Ressource Locator* (URL) exact menant à la page, soit posséder un lien qui y mène. Il est important de préciser, avant tout, que l'usage du *Darknet* n'est pas répréhensible en tant que tel. Il peut même s'accorder, dans sa logique d'anonymat, avec le paradigme de préservation de la vie privée défendue par les articles 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales

[49] Articles L133-1 à L133-45 du code monétaire et financier
[50] Cass. Com, n°22-11.707, 30 août 2023
[51] Articles 323-1 à 323-8 du code pénal
[52] E. CAPRIOLI & I. CHOUKRI, Cours magistral de sécurité des systèmes d'information, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024
[53] En français, « Internet sombre », traduit à tort par "internet clandestin" dans le Journal Officiel de la République française, 26 septembre 2017
[54] En français, « La toile mondiale »
[55] J. MARTINON, « Darknet : éclairage et démystification », « Propos introductifs sur le *Darknet* », Dalloz IP IT, 22 février 2021

(CEDH) et 9 du Code civil.[56] C'est la réalisation d'actes pénalement répréhensibles par l'intermédiaire de ce réseau qui caractérisera, par définition, l'illicéité. La mutation de la délinquance et de la criminalité causées par le numérique se manifeste dans le fait que le *Darknet*, malgré les quelques usages licites qui peuvent en être faits, est le lieu propice pour commettre des actes illicites. On peut donc y retrouver des propositions de produits et services dans les *Black Markets*[57] tels que de la drogue, des logiciels contrefaisants ou piratés, des armes, des données issues de cyberattaques (identifiants *Paypal*, numéros de cartes bleues, etc.), des services de piratage. On peut également y trouver de nombreuses images et vidéos à caractère pédopornographiques, de la diffusion et du financement d'idéologies extrémistes ou des services de trafics d'êtres humains ou d'assassinats, bien que ces deux derniers prennent une place plus importante dans l'imaginaire collectif que ce qu'ils ne représentent réellement[58]. Ainsi, l'Internet sombre constitue un lieu idéal pour les cybercriminels, tout en accueillant des actes illicites qui, pour la plupart, existaient également bien avant sa création. En effet, les marchés noirs, la pédopornographie, le trafic d'êtres humains sont des phénomènes que les autorités ont toujours – difficilement – combattu et qui n'avaient auparavant pas besoin d'Internet pour prospérer. Pour ce qui est des ventes de logiciels piratés, des services de piratage et autres infractions relatives aux numériques, elles ne sont pas dépendantes du *Darknet* en ce sens que, même si l'Internet sombre favorise leur prolifération, elles peuvent exister indépendamment de ce réseau.

2- <u>Les nouveaux actes illicites créés par le numérique</u>

Bien que le numérique ait exacerbé et transformé un certain nombre d'actes illicites qui existaient déjà bien avant la digitalisation de la société, il est quand même des actes qui ont vu le jour grâce à l'avènement de cette évolution sociétale. Dans le panorama des cybermenaces, il existe aujourd'hui un nombre considérable de cyberattaques différentes. Parmi les attaques directes, on recense notamment l'attaque par force brute, l'attaque par dictionnaire, l'attaque *Man in the middle*, l'attaque par démarrage à froid, etc. Parmi les attaques indirectes, il est possible de citer la grande catégorie des attaques d'hameçonnage, l'attaque par point d'eau, ou

[56] E. CAPRIOLI & I. CANTERO, « Quel cadre juridique pour le *Dark Web* ? », L'Usine digitale, 2017
[57] En français, « Marchés noirs (en ligne) »
[58] J-P. RENNARD, *Darknet : mythes et réalités*, Actu'Web, Ellipses, 2018

possiblement l'attaque à la *supply chain*[59]. Les nouvelles formes de risques cyber sont également les *malwares*[60]et les *backdoors*[61] qui, généralement installés après qu'une première cyberattaque ait porté ses fruits, et ce, afin de s'approprier un système d'information. Ces *malwares* peuvent être des *cryptolockers* qui, une fois inoculés dans le système d'information visé, chiffrent l'ensemble des données qui s'y trouvent, empêchant leur propriétaire légitime d'y accéder. Une rançon est alors demandée à la victime pour qu'elle récupère ses données. Ces *malwares* peuvent être couplés à des *backdoors*, qui permettent au pirate d'installer un accès secret, disponible à tout moment au système d'information de la victime. Ainsi, le couplage d'un *ransomware* et d'une *backdoor* permet au pirate, si la victime s'acquitte de la rançon, de réinstaller un autre *malware* quand il le souhaite, car il a désormais librement accès au système d'information de sa victime. Cette situation s'avère être très problématique pour les autorités françaises, en témoigne l'adoption de leur part d'attitudes très versatiles quant à l'encadrement juridique du paiement de la rançon. Il a même été question de sanctionner les payeurs. Mais aujourd'hui, la complexité de la situation et de la difficulté d'encadrer ces nouvelles formes d'infractions s'illustrent dans le fait que les victimes s'acquittant de la rançon ne seront indemnisées par leurs assurances que si elles ont porté plainte dans les 72 heures de la découverte de l'infestation. La solution n'est manifestement pas bonne : la France est aujourd'hui un des pays les plus visés par ce type de cyberattaque[62]. Pour cause, si les victimes paient la rançon, et donc démontrent aux pirates qu'elles sont solvables, cela revient indirectement à inciter les cyberattaquants à continuer dans cette voie. Ainsi, à défaut d'avoir trouvé un moyen efficace pour contrer ces cybermenaces, le législateur a fait le choix de protéger les victimes des conséquences de ces attaques. En outre, le secteur des cyberassurances, par son développement constant, a contribué à cette solvabilité des victimes en leur permettant d'être indemnisées des sinistres causés par des cyberattaques. Ce développement, illustré par l'étude de l'AMRAE[63], permet aux entreprises et aux individus de moins craindre les menaces informatiques mais ne contribue pas à diminuer la cybercriminalité.

Pour ce qui est des cybercriminels, on peut aussi les catégoriser selon leurs buts, leurs moyens et leur envergure. Par exemple, pour les *phishers*, il existe à la fois des individus mettant en place des plateformes de *Phishing-as-a-service*, qui vont permettre de créer des courriers

[59] En français, « Chaîne d'approvisionnement »
[60] En français, « Programme malveillant »
[61] En français, « Porte dérobée »
[62] Rapport Group-IB, « Digital Risk Trends 2023 », 2023
[63] Étude AMRAE, "Lumière sur la cyberassurance", LUCY, édition 2024

électroniques de *phishing* et les SCAMA, des kits de *phishing* qui peuvent se payer en cryptomonnaies pour l'équivalent de 150 euros[64]. Enfin, des cybercriminels *phishers* plus experts, organisés en groupe, et agissant pour le compte d'entités, se sont spécialisés dans la réalisation de *spear phishing*[65] contre des personnalités visées par cette entité. En outre des objectifs purement crapuleux, des organisations de *hackers* comme APT 41 ou Turla, des groupes respectivement chinois et russe, sont souvent considérées comme agissant pour le compte d'États. Les cybercriminels du genre sont des groupes étatiques mais peuvent poursuivre des objectifs à but crapuleux. L'idée est qu'ils agissent en partie au service des États dans lesquels ils sont implantés et qu'en contrepartie, ils bénéficient de l'impunité pour réaliser des missions à objectif purement crapuleux, telles que le *Crime as a service*[66].

La diversité dans les catégories d'attaques et les types de cybercriminels est une complexité supplémentaire pour la compréhension des individus et pour l'encadrement des autorités. En effet, les pirates se renouvèlent constamment et font montre de la plus grande ingéniosité pour mettre en place de nouvelles attaques, toujours plus efficaces pour tromper les victimes ou leur voler des données par la force ou la ruse. En outre, les failles de sécurité possibles sont très nombreuses. Elles peuvent par exemple provenir d'appareils non ou mal sécurisés, d'applications mal configurées, de fichiers non chiffrés, de mots de passe insuffisamment robustes ou de mauvais modes d'authentification des utilisateurs. Toutes ces failles potentielles sont autant de paramètres à maitriser pour les individus et sur lesquels les autorités doivent communiquer. Les outils numériques se sont aussi multipliés au sein des activités domestiques ou ludiques (robots aspirateurs, montres connectées, etc.), ayant pour conséquence d'augmenter la surface d'attaque offerte aux pirates[67].

Pour les individus, dans le cadre de leur vie personnelle ou professionnelle, les questions de la violence numérique et du risque cyber se révèlent être d'importants sujets de préoccupations. (**Voir en annexe : graphe questions 2 et 3**). Cette assertion a également pu être appuyée par le baromètre des risques Allianz 2023[68] qui indiquait que le sujet d'inquiétude principal des dirigeants français était la cybersécurité. Dans le même ordre d'idées, le cabinet

[64] Podcast Le monde de la cyber, avec Romain Basset, « Phishing : de quoi parle-t-on ? », 2023
[65] En français, « Pêche au harpon »
[66] Podcast, No Log, avec Véronique Loquet & Barbara Louis Sydney, « Le renseignement cyber », 2021
[67] C. COSQUER & J. LANCKRIET, « Les objets connectés et la Défense », Revue Défense Nationale, n°787, 2016
[68] Baromètre des risques Allianz 2023, 19 janvier 2023

d'étude et de recherche Asterès[69], mandaté par le Club des responsables d'infrastructure de technologies et de production IT (CRip), a établi un bilan des cyberattaques réussies en France en 2022. Dans ce bilan, était souligné le fait qu'il y avait eu, en 2022, environ 347 000 cyberattaques réussies sur les SI d'entreprises françaises, correspondant à une moyenne de 1.8 attaques par société par an. L'ampleur de ce phénomène est donc avérée, tout comme l'est la prise de conscience des individus sur le sujet. Cette prise de conscience est justifiée, car, si une entreprise subit une cyberattaque compromettant l'ensemble de son système d'information, telles que le chiffrement par un *cryptolocker* ou une attaque en déni de service distribuée, toute son activité est susceptible de s'arrêter puisque toutes les tâches à réaliser numériquement deviennent impossibles à effectuer (plus de paiement des salaires, plus de livraison, plus de communications électroniques, etc.). Pis encore, cette menace plane au-dessus de toutes les entités, publiques ou privées, quelles que soit leur taille. En décembre 2019, c'est le groupe Bouygues qui a subi un cryptolockage de son système d'information et qui n'avait donc plus d'informatique[70].

Pour faire face à ces enjeux et tenter de se prémunir au mieux contre la menace cyber – même si le risque ne disparait jamais totalement –, les entreprises doivent mettre en place des garanties de cybersécurité basées sur des mesures organisationnelles et techniques. Elles sont également astreintes à certaines obligations de cybersécurité, s'appuyant sur trois piliers : la gouvernance, la technique et le juridique[71]. La mise en œuvre de ces mesures permet de réduire le risque, qui, en cybersécurité, mais aussi dans d'autres domaines, se comprend comme étant le produit de la gravité et de la vraisemblance, souvent représenté dans des matrices à double entrée[72].

Mais, au-delà de ces mesures et obligations qui seront mises en œuvre par les entreprises, la théorie du contrat social[73] veut que cela soit l'État, donc les autorités, à qui il appartienne avant tout de prendre cette problématique à bras le corps pour protéger les individus et lutter contre la criminalité.

---

[69] Pour plus de détails, voir l'étude économique « les cyberattaques réussies en France : un coût de 2 Mds€ en 2022 », Asterès, 2023

[70] D. FILIPPONE, « Bouygues Construction paralysé par une cyberattaque majeure », Le Monde Informatique, 2020

[71] M-A. LEDIEU, Enseignement méthodologique de sécurité des systèmes d'information, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

[72] Site Cyber Cercle, « Une matrice pour anticiper et traiter les risques cyber », 11 juin 2021 : https://cybercercle.com/une-matrice-pour-anticiper-et-traiter-les-risques-cyber-une-parole-dexpert-de-gerard-peliks-charge-de-cours-cybersecurite-dans-les-ecoles-dingenieurs-et-institut/

[73] J-J ROUSSEAU, *Du contrat social*, Marc-Michel Rey, 1762

B) La frénésie législative européenne : une élévation des standards de sécurité difficilement applicable

L'encadrement du risque cyber et de la violence numérique a été grandement impulsé par l'Union européenne, qui a entendu créer un bloc législatif numérique européen (**1**). Mais alors que cet objectif est assez bien accompli, les exigences posées en matière de cybersécurité semblent être inadaptées à la réalité (**2**).

1- La création d'un bloc législatif numérique européen

Une prouesse que l'on peut à minima reconnaitre à l'Union européenne est de s'être affirmée comme étant le premier continent à légiférer de manière sérieuse et cohérente en matière de sécurité des SI. Sa dernière réussite en date est le vote, par les parlementaires de Strasbourg, du règlement sur l'intelligence artificielle en décembre 2023. Thierry Breton, commissaire européen chargé de la politique industrielle, du marché intérieur, du numérique, de la défense et de l'espace, n'a d'ailleurs pas manqué de s'en féliciter. Les obligations imposées par ce règlement viendront s'articuler – notamment – avec les obligations déjà en vigueur du Règlement général sur la protection des données[74] (RGPD), du *Digital Services Act*[75] (DSA) ou du *Digital Markets Act*[76] (DMA). Ainsi, ce bloc législatif numérique entend lier de manière cohérente l'ensemble des réglementations sur le numérique. Même si les réglementations mentionnées ici comportent certaines dispositions ayant des impacts en matière de cybersécurité, elles n'y sont pas spécifiquement dédiées. En revanche, la directive *Network and information Security* 2[77](NIS 2), qui fait également partie de ce bloc européen, vise à améliorer le niveau de cybersécurité au sein de l'Union européenne. Vue comme un séisme juridique et technique en matière de gouvernance, cette directive a déclenché une marée de réactions. Faisant suite à la directive NIS 1[78], NIS 2 poursuit l'objectif principal d'étendre drastiquement le nombre d'entités concernées par les obligations imposées en matière de sécurité des systèmes d'information, de renforcer ces dites obligations imposées aux opérateurs ainsi que d'augmenter les paliers de

[74] Règlement (UE) 2016/679 du 27 avril 2016
[75] Règlement (UE) 2022/2065 du 19 octobre 2022
[76] Règlement (UE) 2022/1925 du 15 décembre 2022
[77] Directive NIS 2 (UE) 2022/2255, 14 décembre 2022
[78] Directive (UE) 2016/1148 du 6 juillet 2016

sanction en cas de non-conformité. L'une des exigences principales de NIS 2 est la notification des incidents de sécurité aux autorités compétentes, aux destinataires des services ainsi qu'aux personnes impactées, en prescrivant toutes les mesures applicables en réponse à cet incident.

Cette directive est loin d'être le seul texte européen en matière de cybersécurité. Elle est épaulée par d'autres textes qui y sont spécialement consacrés, tels que le règlement *Digital Operational Resilience Act*[79] (DORA) qui s'applique aux établissements et prestataires bancaires, le *Cyberresilience Act* (CRA), ou encore le *Cybersecurity Act*[80] qui renforce notamment l'*European Union Agency for Cybersecurity*. (ENISA). En d'autres termes, entre les réglementations numériques qui ne sont pas spécifiquement consacrées à la cybersécurité mais ayant une influence en la matière, et les textes qui y sont spécifiquement dédiés, il est indéniable que l'Union européenne a souhaité encadrer ce sujet de manière complète et concrète.

La cohérence et la bonne articulation de l'ensemble de ce bloc numérique européen sont assurées par plusieurs facteurs. Tout d'abord, pour maximiser l'efficacité normative de ces textes, ils sont assortis d'une application extraterritoriale. Ainsi, les articles 3.2 du RGPD, 2.1 du règlement sur l'IA et 2.1 de la directive NIS 2 s'appliquent, en substance, non seulement aux entités implantées l'Union, mais également à celles qui fournissent leurs services dans l'UE. C'est le recours à la notion de « fourniture de services dans l'Union » qui définit l'extraterritorialité, signifiant que même si cette entité est implantée dans un pays tiers, mais qu'une partie de ses activités vise les citoyens ou le territoire de l'Union, elle devra se conformer aux textes susmentionnés. Cette application extraterritoriale renforce la cohérence du bloc européen car le secteur digital, – et par extension la cybersécurité – de par sa dimension transnationale, ne peut être contenu à l'échelle d'un continent. En sorte, si n'avaient été visées que les entreprises ou autres organismes implantés dans l'Union, une grande partie des acteurs n'auraient pas été concernés, ce qui aurait conduit à priver d'effet ces textes.

Autre point important, les règlements et directives définissent et traitent certaines notions de manière uniforme, pour entrainer le moins de divergences d'application possibles. En ce sens, l'articulation de l'ensemble de ces textes est renforcée par l'application de certaines dispositions, conditionnée par l'effectivité de la qualification de notions définies dans d'autres textes. Par exemple, l'annexe III du règlement sur l'intelligence artificielle classe, parmi les systèmes d'IA à

[79] Règlement (UE) 2022/2554 du 14 décembre 2022
[80] Règlement (UE) 2019/881 du 17 avril 2019

haut risque, ceux employés dans la gestion des infrastructures critiques. Il s'agit ici d'une classification se basant moins sur les effets de l'IA, que sur le contexte dans lequel elle est employée. Pour comprendre ce qu'on entend par « infrastructure critique », on peut se reporter à la directive NIS 2. Autre exemple, l'article 17.2 du règlement DORA impose aux entités financières d'enregistrer toutes les cybermenaces importantes. La définition d'une « cybermenace importante » est donnée dans l'article 3.13 du même texte, mais se base évidemment sur celle apportée par l'article 2.8 du *Cybersecurity Act*. De manière plus prospective, on peut également supposer que les prochains textes européens sur le numérique qui contiendront des dispositions sur l'IA se réfèreront sans aucun doute à la définition de l'*IA Act*. Il est cependant bon de préciser que, même si cette uniformité notionnelle est juridiquement bénéfique, elle ne va pas sans une complexité dans la lecture et la compréhension des textes.

Enfin, la bonne application de ces textes passe aussi – et surtout – par la bonne communication quant à leur application. Il revient donc aujourd'hui aux autorités européennes et nationales de jouer le rôle d'intermédiaires de sensibilisation en ce qui concerne l'explication des dispositions de ces textes aux sujets de droit. Sur les autorités nationales pèse donc la charge d'adapter les dispositions des textes européens aux spécificités nationales. Dans cette optique, l'ANSSI a été désignée comme l'autorité française chargée du contrôle de la bonne application de NIS 2 et de son adaptation au cas de la France. Ces autorités peuvent également communiquer sur l'état de l'art[81] en matière de sécurité des systèmes d'information, notion ayant une influence considérable dans le domaine. En outre de cette notion d'état de l'art, les normes ISO/IEC 27000 – relatives au management de la sécurité de l'information – sont mobilisées pour évaluer et certifier le niveau de cybersécurité d'une entité. Créées en 2005, modifiées en 2013 et en 2022, elles permettent aussi aux acteurs de s'aligner sur les attendus des règlements et directives. Ces normes concernent l'aspect pratique et constituent un ensemble de mesures techniques et organisationnelles permettant d'atteindre un objectif de sécurité des SI et d'y rester dans la durée[82].

Néanmoins, ces normes constituent simplement pour les entreprises des outils permettant de donner les indices d'une conformité. Par exemple, une entreprise certifiée ISO 27 701, norme

[81] L'état de l'art correspond à l'état des connaissances dans un domaine, servant notamment, en cybersécurité à définir un seuil d'exigences minimal au vu du degré de maitrise des technologies

[82] F. COUPEZ, Enseignement méthodologique facultatif d'introduction au fonctionnement des technologies de l'information et de la communication, Master 2 Droit du numérique, Université Paris-Panthéon-Assas – 2023-2024

concernant la protection de la vie privée, ne sera pas obligatoirement considérée par les autorités comme conforme aux dispositions du RGPD, alors même que certains critères d'obtention de cette certification se recoupent avec des dispositions du RGPD.

2- La décorrélation entre les exigences théoriques et la réalité technique

Cette décorrélation s'exprime surtout à travers trois facteurs, déjà rapidement mentionnés : le grand nombre de textes qui paraissent de manière continue, les hautes exigences en matière de cybersécurité caractérisées par une masse d'obligations et l'importance des sanctions en cas de non-conformité. Cette triple explication, impulsée par la dynamique générale de frénésie législative européenne, a eu pour effet de souffler un vent de panique dans le monde professionnel. Pour ce qui est du RGPD, paru en 2016, certaines entreprises sont, encore aujourd'hui, à la recherche de spécialistes en la matière, pour les aider à assurer la mise en conformité. Six ans déjà que ce texte est en vigueur et certaines entités sont encore très loin du but. Cet effet d'incompréhension générale est la conséquence logique du large champ d'application matériel de ce texte. Le RGPD s'applique en effet à toutes les entités publiques et privées qui réalisent des traitements de données[83]. C'est cette incompréhension qui a forcé des professionnels, parfois aucunement versés dans le domaine, (professionnels du chiffre, agences d'intérim, collectivités territoriales, etc.) à se tourner vers des spécialistes pour se mettre, dans l'urgence, en conformité. Cette précipitation ne pourra que se voir exacerbée lorsqu'entreront en vigueur la directive NIS 2, le règlement sur l'IA ou le règlement DORA. En effet, aujourd'hui le RGPD est la plus importante source d'implications en termes de conformité pour le monde professionnel et constitue déjà pour certains une difficulté majeure. Qu'en sera-t-il quand, au maximum en octobre 2024, la directive NIS 2 sera transposée en droit français ?

Dans le monde professionnel, le grand nombre de textes, parus et à paraitre, est une source de préoccupations dont l'effet est amplifié par leur caractère ésotérique. Pour tenter d'éviter le problème, certaines entités adoptent alors la stratégie du contournement, consistant à soutenir qu'elles ne sont pas concernées par ces textes. Cette stratégie n'est pas une stratégie gagnante. En effet, pour chaque grand texte, des autorités ont été ou seront nommées pour veiller au bon respect de leurs dispositions. Dans ce cadre, elles pourront réaliser des contrôles, qui leur permettront de constater que l'entité contrôlée n'est pas en conformité, voire n'a pas fait l'effort

[83] Articles 2, 4.7 et 4.8 RGPD

de se mettre en conformité. Pis encore, une entité victime d'une cyberattaque qui n'est pas en mesure de démontrer qu'elle est à l'état de l'art, pourra être sanctionnée. L'article 21 de la directive NIS 2 prévoit par exemple l'obligation de mettre en place des mesures de gestion des risques, impliquant de réaliser une analyse de risque. En l'absence d'une telle analyse, ou si aucune mesure n'a été mise en place à sa suite pour remédier aux failles constatées, l'entité pourra être sanctionnée si elle subit une attaque. En d'autres termes, elle pourra être déclarée coupable d'avoir été une victime négligente, et sanctionnée à ce titre. Premier constat face à cette affirmation : le devoir de vigilance qui s'analysait initialement comme une obligation de moyens s'appréciant de manière subjective, devra désormais plutôt être assimilé à une obligation de résultat, qui se calquera sur la capacité des entreprises à suivre l'état de l'art. Tout ceci paraît absolument déconnecté de la réalité de l'état de la sécurité des systèmes d'information. Pour réaliser le gouffre qui existe entre les attendus théoriques et la réalité professionnelle, il suffit de prendre l'exemple de l'obligation pour les établissements bancaires de mettre en place un processus d'authentification forte. Initialement, en vertu du règlement n°2018/389 du 27 novembre 2017, cette obligation pesait sur les établissements bancaires à partir du 14 septembre 2019. Mais, constatant les nombreux retards des prestataires de services de paiement, en partie dus à la crise sanitaire, l'autorité bancaire européenne (ABE) a finalement décalé cette obligation au 15 mai 2021[84].

En observant ce volumineux corps de règles qui est sur le point de s'abattre sur la société civile, mais aussi sur la sphère publique, l'avenir de l'innovation et de l'investissement dans les nouvelles technologies au sein de l'Union européenne est questionné. Pour le règlement sur l'IA en particulier, un certain nombre d'entreprises lobbyistes ont poussé, au cours des négociations, en faveur d'une réglementation plus souple, pour ne pas endiguer le développement de l'intelligence artificielle et par extension, le développement économique associé[85]. De plus, le bloc numérique européen ne va-t-il pas faire de l'ombre à d'autres préoccupations essentielles telle que l'environnement, incarné par le Green Deal ? Il est difficile, pour l'heure, de savoir quelles seront les conséquences et l'influence concrètes de ces textes sur l'importance accordée à d'autres sujets primordiaux, tandis que la résurgence de l'intelligence artificielle au centre du débat public a confirmé qu'il s'agissait d'un enjeu d'actualité.

[84] J. LASSERRE-CAPDEVILLE, « Sanction à l'absence de mise en œuvre de l'authentification forte », Le Quotidien, septembre 2023,
[85] « Joint statement: Let's give AI in Europe a fighting chance", novembre 2023

La question de la neutralité technologique du droit est aussi incontournable dans ces débats. Selon cette théorie, le droit, en tant que corps de règles tendant à régir le secteur digital, doit s'appliquer indifféremment, à toutes les technologies qui évoluent très rapidement[86]. Le respect de ce paradigme impliquerait que les règles résistent mieux à l'épreuve du temps, car formulées de manière plus générale pour mieux faire face aux évolutions technologiques. Pour autant, le droit ne peut pas non plus être totalement indépendant de la matière qu'il régit. Penser un corps de règles qui ne prenne pas en compte les spécificités de sa matière amène indubitablement à douter de son efficacité. Cette décorrélation trouve matière à s'exprimer à travers la méconnaissance de certains magistrats des spécificités de la cybersécurité et du numérique en général. Pourtant, les atteintes aux systèmes de traitement automatisé de données (STAD) sont pénalement sanctionnées dans le Code pénal et comme toutes infractions, sont constituées par la réunion de leurs éléments constitutifs. Il est possible de citer à ce titre l'arrêt de la Cour de cassation du 7 novembre 2022[87] dans lequel la question technique de savoir si le code de déverrouillage d'un téléphone constituait un processus de déchiffrement avait une incidence juridique en termes de procédure pénale. Plus concrètement, la question était de savoir si les autorités de police pouvaient forcer un individu gardé à vue à révéler son code de déverrouillage. En d'autres termes, de la compréhension technique du fonctionnement d'un code de déverrouillage et des processus de chiffrement dépendait la solution juridique d'une affaire.

En somme, le droit est forcément lié à la matière qu'il prétend régir, mais dans le domaine des nouvelles technologies, le principe de neutralité technologique et la technicité inhérente au secteur posent un certain nombre d'entraves dans la lutte contre la cybercriminalité.

[86] B. BERTRAND, « La proposition de régulation générale pour l'intelligence artificielle dans l'Union européenne : l'IA Act », Revue trimestrielle de droit européen, RTD Eur. p.473, 5 octobre 2022
[87] Cass. Ass Plén., n°21-83.146, 7 novembre 2022

C) Les contraintes inhérentes au droit : une entrave dans la lutte contre la cybercriminalité

Lutter contre la cybercriminalité, c'est lutter à la fois contre les menaces cyber et la violence numérique. Cette lutte doit se faire sur les plans technique et juridique. Mais, pour lutter, encore faut-il saisir toute la complexité du phénomène (**1**) et en tirer des règles adaptées (**2**).

1- Les difficultés d'appréhension de la cybercriminalité

Les difficultés d'appréhension de la cybercriminalité s'expriment à la fois à travers la compréhension et le renseignement sur le phénomène, mais aussi à travers la qualification juridique des actes cyber illicites ainsi que par la protection des victimes.

Pour ce qui est de la difficulté de compréhension du phénomène, elle a déjà été évoquée afin de souligner que lutter contre la cybercriminalité impliquait à la fois une bonne connaissance juridique et une bonne connaissance technique. Pour réglementer un secteur, encore faut-il bien le comprendre et être bien renseigné à son sujet. C'est là toute la complexité lorsqu'il s'agit de la délinquance cyber. En effet, si d'aucuns considèrent que la cybercriminalité est plus dangereuse pour les individus ou pour la société en général que la criminalité dite « classique » (**Voir en annexe : graphe question 9**), il est surtout plus difficile d'obtenir des statistiques fiables concernant la cybercriminalité par rapport à la criminalité dite « classique ». En ce sens, les victimes peuvent ne pas avoir connaissance d'une compromission, c'est-à-dire ne pas savoir qu'un individu malveillant a pénétré dans leur système d'information. Il existe aussi la situation où une victime ne découvre que très tardivement qu'elle a fait l'objet d'une cyberattaque, faussant ainsi le constat des conséquences de cette attaque. Enfin, les victimes peuvent avoir conscience que leur système d'information est compromis, mais ne pas le révéler – notamment pour des raisons d'images – parce qu'elles en minimisent ou maximisent la gravité. En prenant le cas des menaces persistantes avancées[88] (MPA) ou des *backdoors*, il apparait assez clair que ces phénomènes sont difficilement documentables de manière précise, puisque leur *modus operandi* est fondé sur l'ignorance de la victime. En ce sens, il est possible de rapprocher ces actes illicites

[88] Programme sophistiqué et systématique de cyberattaque qui se déploie pendant une longue période

du régime des infractions occultes et dissimulées de l'article 9-1 du Code de procédure pénale (CPP) – qui fait courir le délai de prescription de ces infractions au jour de leur découverte dans des circonstances permettant l'exercice de l'action publique. Cependant, ces poursuites seront confrontées à d'autres obstacles matériels, mentionnés ci-après (**I], C) 2-**). De la même manière, aujourd'hui, seules quelques entreprises produisent des solutions logicielles de *Software as a Service* (SaaS) pour détecter si des données d'entreprises ont été illicitement et illégitimement transmises sur le *Darknet*. On citera à ce titre la solution *Dark Web Monitoring* de la start-up française CybelAngel, qui propose à ses clients la fourniture d'un outil de scan. Sans ces solutions, souvent proposées uniquement aux entreprises privées ou aux entités publiques, il est presque impossible de savoir, pour un individu, si l'intégrité et la confidentialité de ses données sont préservées. Pourtant, au vu du nombre de cyberattaques que l'on recense régulièrement, dont certaines ont une ampleur extraordinaire, (**Voir en annexe : graphe question 8**), il est très probable qu'au moins une partie des données personnelles de tous les Français se trouvent sur l'internet sombre.

De cette difficulté d'être bien informé sur l'ampleur de la cybercriminalité, découle la complication dans le fait de protéger correctement les individus et les entreprises. Très concrètement, pour lutter contre la criminalité classique, les forces de police et de gendarmerie disposent de moyens pour prévenir ou faire cesser les infractions le plus rapidement possible : contrôle d'identité, patrouilles, enquêtes de flagrance, etc. Ces moyens sont considérablement diminués lorsqu'il s'agit de prévenir et faire cesser les actes de cyberdélinquance ou de cybercriminalité, en particulier car tous les moyens physiques de prévention et de répression n'ont, par définition, pas la possibilité d'être mis en œuvre. En outre, les cas où les victimes, ou les autorités elles-mêmes, peuvent intervenir pour faire cesser un acte illicite, ou pour se défendre, sont très restreints. En toute logique, si la loi pénale est d'interprétation stricte, la légitime défense l'est aussi. En vertu de l'article 122-7 CP, l'agent sera considéré comme non-pénalement responsable si, face à un danger actuel et imminent qui menace lui-même, autrui ou un bien, il commet un acte rendu nécessaire à la sauvegarde de la personne ou du bien, à condition qu'il n'y ait pas disproportion entre les moyens employés et la gravité de la menace. En matière de cyberdéfense, cette règle de la légitime défense est incarnée dans la norme PRIS de l'ANSSI[89], qui ne laisse globalement que la latitude de couper l'alimentation du serveur à

[89] ANSSI, Référentiel d'exigences, « Prestataires de réponse aux incidents de sécurité », 14 février 2023

l'origine de l'attaque. Mais, si les pirates utilisent des serveurs de rebond, notamment par l'usage d'un *Virtual Private Network* (VPN)[90] – ce qui est très souvent le cas –, en éteignant le serveur de rebond, on sort du cadre légal de la légitime défense cyber. Cela signifie que la cyberdéfense est astreinte au respect d'un certain nombre de contraintes légales qui ne mettent pas sur un pied d'égalité la défense de l'attaque, car si les individus ou entités subissant des attaques appliquaient la loi du Talion, l'Etat de droit en serait menacé. En effet, comme il a pu être précisé plus haut, l'Etat dispose du monopole de la violence légitime, mais cela ne signifie pas que cette violence doit se faire sans respecter certaines règles. C'est le respect de ces contraintes par les autorités, dans l'usage de la violence, qui permet de préserver l'Etat de droit et évite la bascule vers l'autoritarisme. En clair, l'appréhension, l'encadrement et la lutte contre la cybercriminalité sont soumis à des impératifs juridiques desquels les pirates ne s'embarrassent pas, mais qui rendent la défense contre eux autrement plus ardue.

En dernier lieu, le droit pénal, pour produire ses effets, implique la caractérisation de l'infraction. Cette opération nécessite la réunion d'un ou plusieurs éléments matériels, ainsi que d'un élément moral. En matière de cybercriminalité, le problème réside dans le fait qu'il est difficile d'associer les actes de délinquance cyber à une qualification pénale précise, qu'il s'agisse des formes originelles de violence exacerbées par le numérique, ou des nouvelles formes de violence créées (cf. **I] 1- et 2-**). D'une part, les formes originelles de violence pour lesquelles existent des qualifications pénales peuvent subir des mutations, du fait de leur adaptation au format numérique et ainsi, ne plus correspondre aux qualifications du Code pénal. D'autre part, les nouvelles formes de violence créées par le numérique, normalement encadrées par le chapitre du Code pénal consacré aux atteintes aux STAD, ne sont que peu sanctionnées, car les juges font une application très limitée de ces articles[91], hormis quelques affaires emblématiques telles que les affaires Bluetouff[92] ou Tati[93]. Cette entrave pose alors la question d'une éventuelle élaboration d'infractions spécifiques aux cyber actes illicites (ex. : infraction de *phishing*, infraction d'installation de *ransomware*, etc.). Néanmoins, deux obstacles apparaitraient si l'on optait pour cette solution. Premièrement, on irait à l'encontre du principe de neutralité technologique du droit et ces infractions, à peine créées, deviendraient inadaptées quelques

[90] En français, « réseau privé virtuel »
[91] J. FRANCILLON, « Infractions relevant du droit de l'information et de la communication », Revue de science criminelle et de droit pénal comparé, p. 559-578, 2013
[92] Cass. Crim., n°14-81.336, 20 mai 2015
[93] CA Paris, 12ème Chambre, 30 octobre 2002

années après leur création. Deuxièmement, créer des infractions spécifiques aux actes de cybercriminalité aurait pour conséquence d'enfermer ces actes dans des qualifications d'interprétation stricte. Le *phishing* par exemple, peut se décliner en des formes multiples. En effet, on ne saurait pas anticiper de manière certaine les formes futures que pourraient prendre ces cyber infractions. En sorte, le *phishing*, dans son acception la plus classique, pourrait correspondre à de nombreuses qualifications : usurpation d'identité, escroquerie, contrefaçon, collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite, accès frauduleux à un STAD, etc. Pour ce qui est du *Darknet*, en fonction des cas, pourraient être caractérisés le recel, la collecte illicite de données, le blanchiment, le trafic de stupéfiants, l'enregistrement d'images de violence, ou les infractions en matière de mise en péril des mineurs et de pédopornographie. Mais ce sont également des difficultés en matière de répression de la cybercriminalité que rencontre le droit.

2- Les difficultés de répression de la cybercriminalité

Les difficultés de répression de la cybercriminalité doivent s'entendre sur plusieurs plans : le problème de localisation des infractions à cause de leur transnationalité, qui entraine une complexité dans la détermination de la loi applicable, la difficulté d'identification des auteurs qui usent de procédés techniques (chiffrement, anonymisation, etc.) pour que les autorités ne remontent pas jusqu'à eux et l'inadaptation des règles existantes pour endiguer la cybercriminalité.

Tout d'abord, la complexité dans la localisation des infractions réside dans le fondement même de la transnationalité d'internet et des autres réseaux comme le *Darknet*. Alors que le droit pénal, pour déterminer la loi applicable et le tribunal compétent, exige de pouvoir localiser l'infraction dans l'espace, la cybercriminalité rend la chose compliquée. Ainsi, lorsqu'une infraction est commise par ce biais, il est très difficile de déterminer un lieu de commission de l'infraction. Cette question de la localisation des actes est d'ailleurs également un enjeu majeur dans les autres branches du droit lorsqu'apparaissent des litiges à caractère international nés sur internet[94]. Sur internet, les lieux de commission de l'infraction peuvent être le lieu où la victime a subi le préjudice ou le lieu où l'auteur se situe au moment de cette commission. Mais, si on

[94] Pour un cas d'application en droit de la propriété intellectuelle : Cass. Com., n°02-18.381, 11 janvier 2005

prend comme critère le lieu de situation de l'auteur dans le cadre de l'infraction d'accès frauduleux au sein d'un système d'information (Article CP sur les infractions aux STAD), doit-on considérer qu'il s'agit du lieu où se situent les serveurs de ce système d'information, celui où se situe physiquement l'agent ou le lieu correspondant à son empreinte de connexion – et si tel est le cas, comment faire en cas d'utilisation de VPN ? Toutes ces interrogations rendent évidemment plus ardue la répression de la cybercriminalité[95]. En ce qui concerne les solutions techniques permettant aux pirates de masquer la localisation de leurs infractions ainsi que leur propre localisation, ces VPN consistent techniquement en un échange de clés par chiffrement asymétrique entre l'ordinateur et le serveur de connexion, afin que l'adresse IP qui apparaisse publiquement soit celle du serveur VPN et non pas celle du fournisseur d'accès à Internet. En outre, l'usage des cryptomonnaies est également un outil permettant de brouiller la localisation des auteurs et des infractions. Cette utilisation n'est pas illégale en soi dans la majorité des pays, mais lorsque les cryptomonnaies sont mobilisées pour opérer des transactions illicites, leur usage le deviendra par contamination. En ce sens, payer ou recevoir en paiement une transaction en cryptomonnaie peut, dans certains cas, juridiquement s'analyser comme du blanchiment. Concrètement, le paiement en cryptomonnaie permet tout d'abord de se passer des intermédiaires bancaires et financiers, qui sont contraints de livrer aux autorités, si elles disposent d'un mandat, les relevés et coordonnés bancaires de l'auteur d'une infraction. Les établissements et prestataires bancaires ne sont donc absolument pas vus comme des intermédiaires de confiance. En outre, les protocoles de chiffrement qui existent sur certaines blockchains, empêchent l'identification des auteurs de cette transaction. Une fois les transactions réalisées, les cyberdélinquants et cybercriminels ont la possibilité de convertir les cryptomonnaies en monnaie scripturale par l'intermédiaire de comptes bancaires dans d'autres pays.

En ce qui concerne l'identification des auteurs, elle est également rendue plus complexe par l'utilisation de procédés techniques, certains propres à la cybercriminalité, d'autres non. On citera parmi eux les réseaux en nœuds ou les réseaux distribués, le chiffrement, notamment le chiffrement *Pretty Good Privacy* (PGP) ou, plus basiquement, l'utilisation de pseudonymes. En ce qui concerne le chiffrement PGP, il permet de chiffrer des données, telles que des

[95] R. STAMBOLIYSKA, *La face cachée d'internet*, Larousse, 2017

correspondances ou des fichiers[96]. Il s'agit d'un protocole de chiffrement très utilisé par les *darknautes*, mais puisque toute la cybercriminalité ne passe pas forcément par le *Darknet*, d'autres peuvent être utilisés. Le protocole PGP est une méthode de chiffrement asymétrique qui consiste en l'utilisation de clés publiques et de clés privées. Le principe est que, dans le cadre des communications, on peut soit assurer la confidentialité des échanges, l'intégrité de la communication ou l'authentification de l'interlocuteur, sans cependant, que l'on ne puisse jamais assurer les trois simultanément. Pour assurer l'intégrité des échanges et l'authentification de l'interlocuteur, on utilise une fonction de hachage[97] qui correspond à un résumé d'un message faisant 1 octet. Ce hachage est réalisé avec la clé privée de l'émetteur du message. Si une personne non visée par la communication, utilise la clé publique de l'expéditeur pour en modifier le contenu et qu'elle rechiffre le message avec sa propre clé privée (le chiffrement avec la clé privée de l'expéditeur étant impossible puisque seul ce dernier est censé la connaitre), le *hash* obtenu sera différent et le destinataire pourra savoir qu'une personne tierce est intervenue dans la transmission du message. La fonction de confidentialité du chiffrement asymétrique s'opère par le chiffrement du contenu transmis avec la clé publique du destinataire, de sorte que seul lui, avec sa clé privée, (puisque ce qu'une clé fait, seule l'autre peut le défaire[98]), puisse déchiffrer le message.

En plus des protocoles de chiffrement, les réseaux en nœud, comme *Tor Browser*, rendent l'identification de l'adresse IP des utilisateurs quasiment impossible. Les requêtes des utilisateurs qui se connectent au navigateur sont chiffrées et envoyées vers un nœud, puis successivement transmises entre plusieurs nœuds, jusqu'à un nœud de sortie qui l'envoie au serveur final. Le serveur chiffre les données, et les renvoie aussi vers le nœud à l'origine de la requête, avant que l'émetteur ne les déchiffre. Les caractéristiques de ce système, qui favorise l'anonymisation, résident dans le fait que les nœuds sont choisis aléatoirement, que les données des requêtes sont chiffrées et que chaque nœud ne possède que la référence de contexte du suivant et du précédent, rendant le travail d'identification des auteurs par les autorités malaisé.

---

[96] Site Varonis, « Chiffrement PGP » : https://www.varonis.com/fr/blog/pgp-encryption#:~:text=Le%20chiffrement%20PGP%20peut%20%C3%AAtre,personnes%20avec%20lesquelles%20vous%20communiquez.

[97] Transformation d'une suite de caractères en valeur ou en une clé de longueur fixe représentant la chaîne d'origine

[98] F. COUPEZ, Enseignement méthodologique facultatif d'introduction au fonctionnement des technologies de l'information et de la communication, Master 2 Droit du numérique, Université Paris-Panthéon-Assas – 2023-2024

Enfin, on citera les réseaux distribués qui s'apparentent à un système de *peer-to-peer* (P2P), ayant pour conséquence que les données ne sont pas stockées sur un serveur mais sur les postes individuels de chaque utilisateur selon la logique client-serveur. En conséquence, ces réseaux distribués sont indépendants des serveurs et surtout, les autorités ne disposent d'aucun support sur lequel ils peuvent perquisitionner les données.

Pour finir, la nature de la répression de la cybercriminalité est à interroger. Dans son fondement même, la répression pénale est assez peu dissuasive envers les pirates, elle l'est d'autant moins que les auteurs sont difficilement identifiables et que les juges sanctionnent peu sur le fondement des articles applicables. Augmenter les peines n'apparait donc manifestement pas utile dans ces circonstances.

En conclusion, l'encadrement de la cybercriminalité par le droit présente plusieurs lacunes. Face à une mutation constante de la violence et du risque cyber, les contraintes propres au droit créent un décalage entre l'encadrement par les autorités et la réalité. Ce n'est pas tout de légiférer avec zèle pour renforcer les exigences de cybersécurité et les garanties individuelles, encore faut-il pouvoir se défendre dans la pratique. C'est pour cette raison que, pour encadrer la violence numérique et le risque cyber, l'approche juridique, essentielle malgré tout, doit être complétée par une approche opérationnelle pragmatique.

II] L'appréhension de la violence numérique par la cybersécurité : le besoin d'une approche pragmatique et opérationnelle

Pour adopter une approche plus pragmatique et opérationnelle face à la cybercriminalité, un des points primordiaux est d'abord de mieux la comprendre pour mieux la combattre. C'est dans ce cadre que les autorités tentent de se spécialiser (**A**). De plus, les nouvelles technologies, à l'instar de l'intelligence artificielle, sont et seronté, amenées à jouer une place centrale dans le traitement de la cybercriminalité, étant à la fois utilisées par et contre les pirates (**B**). Enfin, lutter contre la violence numérique et contre le risque cyber implique une meilleure articulation entre les sphères publique et privées, qui ont toutes deux intérêts à la coopération (**C**).

A) La spécialisation des autorités en matière cyber : l'objectif d'un encadrement plus efficient

Le renforcement des autorités dans la lutte cyber s'effectue à la fois sur le plan interne, par la création de nouvelles autorités et la spécialisation des autorités existantes (**1**) ainsi que par un accent mis sur la coopération internationale pour rendre plus efficace la recherche, la poursuite et la sanction des auteurs d'infractions (**2**).

1- La création de nouvelles autorités et la spécialisation des existantes

La spécialisation des autorités, dans le domaine pointu et relativement nouveau – mais surtout encore en évolution – qu'est la cybersécurité, est une condition *sine qua non* de son encadrement. Cet encadrement, comme il l'a déjà été précisé, passe à la fois par l'information et la protection des individus, mais aussi des entités publiques et privées, et par la prévention et la répression des comportements et actes illicites. Le combat est cependant, dès le début, asymétrique. Les autorités – parce qu'elles disposent du monopole de la violence légitime – sont astreintes au respect d'un certain nombre de règles qui conditionnent leurs actions. De manière générale, il est aussi toujours plus facile de détruire que de réparer[99]. Cette asymétrie doit être compensée par une spécialisation de l'ensemble des autorités, de la bouche de la loi, jusqu'au

[99] Podcast France Inter, avec Jeanne Mayer, « Le Darknet », 19 novembre 2021

bras armé de l'Etat. En effet, la connaissance et la compréhension du phénomène doit s'étendre au législateur, aux juges, aux forces de police et aux autorités de contrôle et de sensibilisation comme la Commission nationale de l'informatique et des libertés (CNIL), l'Agence nationale de sécurité des systèmes d'information (ANSSI) ou l'Autorité supérieure de la communication audiovisuelle et du numérique (Arcom).

Ces autorités de contrôle, mais aussi dans une certaine mesure les législateurs français et européen, jouent un rôle de prévention et de sensibilisation. On citera à cet égard le rapport de la Commission de l'intelligence artificielle[100] le MOOC de l'ANSSI[101], les référentiels de la CNIL en matière de protection des données ou ses fiches explicatives sur des sujets brûlants d'actualité[102]. Ces communications, rapports, formations et référentiels sont à la fois élaborés à destination des individus dans le cadre de leur vie personnelle, mais également du monde professionnel. L'ensemble de cette documentation traite, en outre, aussi bien de cybersécurité spécifiquement, que de nouvelles technologies de manière générale. Ces initiatives sont fondamentales à plusieurs titres : elles permettent de rappeler que les autorités publiques n'ont pas qu'un rôle de sanction, mais permettent aussi la préservation et l'information sur les droits et libertés des sujets de droit ; elles permettent aussi un meilleur encadrement du risque cyber et de la violence numérique car une diffusion massive des bonnes pratiques et de l'information à destination de la société civile rend le travail de ces autorités plus aisé. De manière générale, la sensibilisation des individus, même si des progrès peuvent encore être faits, semble toucher une proportion assez importante de la société, qui est désormais plutôt informée sur le sujet (**Voir en Annexe : Graphe question 4**)

Malgré tout, ces autorités sont aussi des organismes de contrôle et de réception des plaintes, qui permettent aux individus de pouvoir exercer leurs droits de manière effective. L'Arcom, la CNIL et Pharos sont autant d'organismes permettant l'exercice des droits des individus, respectivement en matière d'audiovisuel, de protection des données, et de communication électronique. En prenant l'exemple de Pharos, peuvent être signalés, par toute personne, des contenus ou des comportements sur un site internet, un réseau social, un blog, un forum ou une messagerie, à la seule condition qu'il s'agisse d'un contenu ou d'un comportement

[100] Rapport Commission de l'intelligence, « Notre ambition pour la France », 13 mars 2024
[101] ANSSI, MOOC SecNumAcadémie, 18 mai 2017
[102] CNIL, « Délibération n° 2024-011 portant adoption d'une recommandation sur l'application du règlement général sur la protection des données au développement des systèmes d'intelligence artificielle », 18 janvier 2024

transmis par l'intermédiaire d'un canal public. Les signalements sont traités par des policiers et gendarmes affectés à la plateforme d'harmonisation et d'analyse, le service Pharos appartenant à la direction centrale de la police judiciaire. Le contenu signalé pourra faire l'objet d'une enquête diligentée par le procureur de la République ou être transmis à Interpol s'il provient de l'étranger, qui orientera alors vers les autorités judiciaires du pays concerné. Cette fonction de réception n'éclipse pas le rôle de sensibilisation de la plateforme, qu'elle met aussi en premier plan, à travers les rubriques « Conseils aux parents » ou « Conseils aux jeunes », qu'on peut retrouver sur sa page d'accueil. À côté de cela, pour ce qui est de l'autorité dédiée à la cybersécurité, celle-ci sera prochainement chargée de contrôler les entités concernées par NIS 2, alors qu'elle n'est pas une autorité juridictionnelle à proprement parler. Elle pourra notamment, en vertu de la directive, ordonner la cessation d'un comportement, garantir la conformité des mesures de l'entité à la directive, ordonner à l'entité d'informer les personnes sur des mesures préventives ou réparatrices et lui ordonner de rendre publics certains de ces manquements[103]. L'ANSSI fera également partie des organismes pouvant définir l'état de l'art sur certaines questions. Par exemple, en matière de cybersécurité, la CNIL et l'ANSSI ont eu l'occasion d'émettre des référentiels, changeant plusieurs fois d'avis, pour définir l'état de l'art sur la sécurité des mots de passe[104]. Cette détermination de l'état de l'art soulève un léger paradoxe juridique : les recommandations et autres communications de la CNIL ou de l'ANSSI n'ont, par définition, par de force contraignante, c'est-à-dire que leur respect n'est normalement pas obligatoire. Pourtant, dans nombres de délibérations, la CNIL s'est appuyée sur ses propres recommandations pour fonder une sanction ou en justifier le montant[105]. Il serait presque possible de se méprendre sur la capacité théorique de la CNIL à établir des normes créatrices de droit, si le Conseil d'Etat n'avait pas eu l'occasion de rappeler qu'elle ne pouvait créer *ex nihilo* des interdictions formelles[106].

En parallèle, existent également des organismes tels que l'Office anti-cybercriminalité (OFAC) ou le Centre de lutte contre les criminalités numériques (C3N), spécialement chargés de lutter contre la cybercriminalité. L'OFAC est né de la fusion entre l'Office central de lutte contre

[103] Site de l'ANSSI, « La directive NIS 2 » : https://monespacenis2.cyber.gouv.fr/directive
[104] CNIL, « Délibération n°2022-100 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017 », 21 juillet 2022 & ANSSI, « Recommandations relatives à l'authentification multifacteur et aux mots de passe », 8 octobre 2021
[105] CNIL, Délibération SAN-2022-022 du 30 novembre 2022
[106] CE, Chambres réunies, décision n°434684, 19 juin 2020

la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et de la sous-direction de la lutte contre la cybercriminalité, actée par un décret du 23 novembre 2023[107]. Cet Office est placé sous l'autorité du ministère de l'Intérieur et des Outre-mer, et est directement rattaché au directeur général de la gendarmerie nationale. Le C3N traite quant à lui des questions de cybercriminalité et d'analyse numérique, et regroupe l'ensemble des unités du pôle judiciaire de la Gendarmerie nationale. Ces deux organismes témoignent d'une spécialisation des services de police et sont dotés d'un pouvoir d'enquête ; ils sont donc plus spécialisés dans le pan concret de la lutte contre la cybercriminalité et sont moins étroitement liés aux individus que les autorités susmentionnées, mais restent toutefois essentiels dans l'encadrement de la violence numérique et du risque cyber. En d'autres termes, tandis que la CNIL ou l'ANSSI possèdent des compétences spécifiques mais ne sont pas des autorités juridictionnelles ni ne disposent d'un pouvoir de sanction spécifique contre les cybercriminels, le C3N et l'OFAC représentent le bras armé de l'Etat dans la lutte contre la criminalité numérique. L'affaire EncroChat est un exemple marquant de succès du C3N[108]. Il s'agissait d'un réseau chiffré de communication utilisé par des malfaiteurs que la gendarmerie est parvenue à décrypter, permettant de prévenir un certain nombre d'actes de cybercriminalité ayant été fomentés par l'intermédiaire de ce réseau. Ce décryptage a aussi permis de démanteler un certain nombre d'organisations criminelles importantes[109]. Également, le 15 février 2021, les autorités belges sont parvenues à accéder au réseau Sky ECC, menant à un total de 111 mises en examen, une saisie de plus de 17 tonnes de cocaïne et une masse énorme de données collectées[110]. Néanmoins, ce succès doit être pris de manière réaliste, il s'agit d'une bonne réussite, mais le démantèlement de ce genre de réseau pose une question qui n'est pas propre à la cybercriminalité : les autorités ne sont-elles pas confrontées, face à ce genre de criminalité organisée, au problème de l'hydre, qui rend les démantèlements auxquels elles procèdent beaucoup moins efficaces ?

En somme, tous ces organismes sont complémentaires et se sont spécialisés techniquement, même s'ils manquent encore un peu de rayonnement, alors pourtant que leur connaissance par les individus est fondamentale (**Voir en annexe : graphe question 7**). En

[107] Décret n°2023-1083 du 23 novembre 2023
[108] J-P. STROOBANTS, « Criminalité organisée : le démantèlement de la messagerie EncroChat a permis d'arrêter plus de 6 500 personnes », Le Monde, 27 juin 2023
[109] Podcast Les Temps Electriques, avec le colonel, Jérome BARLATIER, « Cyberarnaques : quand l'internaute mord à l'hameçon », 21 avril 2023
[110] T. SAINTOURENS & S. PIEL, « Sky ECC, l'application prisée des trafiquants, mine d'or des enquêtes sur le crime organisé », Le Monde, 18 novembre 2022

outre, l'un des défis pour ces organismes, pour faire face à la transnationalité inhérente à la cybercriminalité, est d'instaurer une coopération internationale efficiente.

2- La coopération internationale : une meilleure coordination dans la prise en main du phénomène cyber

Cette coopération doit s'entendre à plusieurs égards. Il s'agit à la fois d'une coopération internationale entre les autorités de plusieurs Etats mettant en œuvre des initiatives conjointes pour lutter contre la cybercriminalité et de la création d'autorités supranationales, particulièrement à l'échelle de l'Union européenne, qui permettent une meilleure coordination des Etats sur leurs domaines de compétences.

Concernant la coopération internationale, il s'agit avant tout de permettre un encadrement plus efficace de la violence numérique et du risque cyber par l'échange d'informations sur les auteurs, la coopération dans les recherches et la mise en commun de certains moyens. Cette coopération n'a aujourd'hui pas atteint son apogée – même si elle a eu l'occasion de démontrer son efficacité – car elle touche à la souveraineté des Etats. L'histoire de la coopération internationale se caractérise par sa progressivité. Aujourd'hui, la phrase de Robert Schuman résonne encore par sa postérité : « L'Europe ne se fera pas d'un coup, ni dans une construction d'ensemble : elle se fera par des réalisations concrètes créant d'abord une solidarité de fait »[111]. La construction européenne s'est faite sur des dizaines d'années, depuis la création de la Communauté européenne du charbon et de l'acier (CECA) jusqu'à la fondation de l'Union européenne par le traité de Maastricht[112]. Ce projet d'harmonisation économique, sociale et juridique, basé sur les deux piliers de la construction européenne que sont l'approfondissement et l'élargissement, a impliqué un abandon de souveraineté étatique sur certains sujets. Il est, pour l'heure, assez difficile d'entrevoir, de la part des Etats, un abandon total de souveraineté au profit d'une instance supranationale, alors même pourtant que l'Union européenne est le projet le plus abouti en la matière. Ainsi, la coopération en matière de cybersécurité ne fait pas exception à cette réticence à l'abandon des souverainetés. Pourtant, la coopération est une condition indispensable de l'efficacité de cette lutte. Malgré tout, quelques initiatives prometteuses ont pu

[111] Déclaration Schuman du 9 mai 1950
[112] Traité sur l'Union européenne (TUE), 7 février 1992

voir le jour, donnant l'espoir en une progression de la coopération qui permettrait de concrétiser les nombreuses initiatives législatives européennes.

Tout d'abord, le projet Aronnax donne un exemple concret de coopération interétatique en matière de lutte contre la cybercriminalité. Il s'agit d'un projet qui devrait voir le jour en 2025, dont la société Civipol a la charge du développement, visant à instaurer un service européen qui permettra de donner aux experts et enquêteurs un moyen d'accéder à des informations concernant les canaux de communication privilégiés par les criminels pour vendre et acheter des services[113]. Ce projet réunit les autorités de lutte contre la cybercriminalité de la France, la Roumanie, l'Allemagne et l'Estonie. Il servira également à fluidifier le partage des indices laissés par les pirates informatiques pour renforcer la coopération européenne dans le domaine de la cybercriminalité. Évidemment, à terme, ce plan vise à inclure le maximum d'autorités nationales en son sein pour maximiser son efficience. Néanmoins, il est utile d'ajouter que ces autorités seront astreintes au respect des contraintes réglementaires et techniques en vigueur dans la réalisation de ce projet, notamment les dispositions de la directive Police-Justice[114], ainsi que les dispositions des réglementations nationales relatives à la protection des données. En effet, un des objectifs d'Aronnax est de mettre en place une base de données d'informations utiles à disposition des autorités parties, telles que les apparitions involontaires d'adresses IP ou de portefeuille de cryptomonnaies en lien avec des infractions cyber. Encore une fois donc, la réalisation des missions de ces organismes sera conditionnée par les contraintes de l'Etat de droit, nécessaires dans le cadre d'une société démocratique, mais ne facilitant pas la lutte pratique contre la cybercriminalité.

Déjà abordé, le cas de l'affaire Sky ECC avec l'OFAC ayant agi en « *task force* » témoigne également de ces initiatives partagées. Il est cependant difficile d'imaginer, pour l'instant, une coopération réalisée avec des pays tiers à l'Union européenne. En effet, qu'il s'agisse du projet Aronnax ou de la coopération sur l'affaire Sky ECC, on comprend assez bien que l'entente européenne donne un cadre favorable à ces collaborations, cadre qui n'existe pas avec les autres continents et explique donc en partie la coopération encore très embryonnaire.

---

[113] Luca BERTUZZI, « Loi sur l'IA : la définition de l'IA et la gouvernance au cœur des débats européens », Euractiv, 8 novembre 2022

[114] DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

L'encadrement de la violence numérique peut, cependant, aussi compter sur les instances européennes créées par les différents textes pour coordonner l'action des autorités ; au premier rand desquels figure l'ENISA. Il s'agit d'une agence créée en 2004, renforcée par l'entrée en vigueur du *Cybersecurity Act*, qui contribue au développement de la cybersécurité sur le continent. Elle est notamment chargée de délivrer des certifications, de renforcer la communication entre les organes de l'Union européenne et les autorités nationales et les entreprises et de conseiller les autorités nationales. À son palmarès, figure notamment le projet *Cyber Crisis Liaison Organisation* Network (CyCLONe), réseau de coopération cyber entre les Etats membres, réunissant l'ANSSI et l'Agence de cybersécurité italienne, toutes deux à son initiative, ainsi que les autres agences européennes.

Enfin, toutes les autorités créées par l'Union européenne affiliées à des textes précis (CEPD, ENISA, prochainement CEIA…) sont sans doute les premières pierres à l'édification d'une entité plus générale disposant de plus de compétences pour assurer un niveau global de contrôle des nouvelles technologies et de la cybersécurité. Il serait en effet audacieux, mais pas totalement irréaliste, de concevoir la fusion de certaines de ces entités européennes, dont la plupart sont souvent amenées à collaborer, pour créer un organisme plus omnipotent. Ce type de réflexion irrigue la réflexion de la Commission nationale sur l'IA dans son rapport « Notre ambition pour l'IA », qui envisage au plan prospectif la création d'une Organisation mondiale de l'IA. Cette organisation réunirait les Etats, des entreprises et des individus issus de la société civile et pourrait émettre un certain nombre de normes techniques contraignantes concernant l'IA.

En somme, la spécialisation des autorités doit s'entendre pour la cybersécurité, mais également en matière de nouvelles technologies de manière générale. Elle comprend à la fois un renforcement des compétences techniques des organismes, une prise en compte poussée de l'avis d'experts dans l'élaboration des réglementations et le jugement des affaires ainsi qu'une coopération internationale grandissante permettant un partage des compétences et des informations pour un meilleur encadrement. L'usage des nouvelles technologies, au service de la lutte contre la cybercriminalité doit aussi être envisagé, tant les possibilités offertes par ces nouveaux moyens techniques sont vastes. Mais, bien sûr, les NTIC ne sont pas réservées aux autorités, aux entreprises et aux individus dans le cadre de leur vie personnelle ; elles peuvent

également servir aux pirates informatiques qui ont d'ores et déjà trouvé des moyens de les utiliser pour satisfaire leurs desseins.

B) L'ambivalence des nouvelles technologies : outils de lutte et supports d'illicéité

Parce qu'elles sont nouvelles, il est difficile de prévoir tous les impacts qu'auront les NTIC sur notre futur, notamment en matière de cybersécurité. Les technologies de l'information et de la communication peuvent aussi bien être mises au service de la protection des individus et être utilisées par les organismes pour renforcer la cybersécurité (**1**), qu'être un support d'illicéité (**2**).

1- Des outils au service des individus et des autorités

Les bénéfices – avérés ou potentiels – de ces outils, doivent s'entendre comme rendant le quotidien des individus plus facile, comme favorisant l'exercice de leurs droits tels que le droit à la vie privée ou la liberté d'expression, et comme pouvant contribuer au renforcement de la sécurité de leur système d'information. Pour les autorités et les organismes de lutte contre la cybercriminalité, les technologies de l'information et de la communication peuvent être également utilisées pour prévenir ou repérer des cyber infractions. Malgré ces possibles usages positifs des nouvelles technologies, force est de constater que le grand public est encore divisé sur la question. Ces avis divergents peuvent s'expliquer par plusieurs facteurs, tels que la réticence à la nouveauté, l'incompréhension du fonctionnement ou encore la peur de perte de libre-arbitre (**Voir en annexe : Graphe question 5**). La peur de ces technologies peut apparaitre justifiée. C'est pour cette raison qu'il est primordial d'en encadrer l'utilisation pour exploiter toutes les potentialités qu'elles recèlent, dans le respect des droits des individus et d'autres impératifs tels que la santé, la sécurité, etc.

L'IA incarne aujourd'hui un certain nombre de débats sur les nouvelles technologies, tels que les impacts sur la gouvernance, la démocratie, l'environnement, les questions éthiques et bien d'autres encore – presque au point de faire de l'ombre sur la question des impacts d'autres nouvelles technologies. En matière de cybersécurité, l'intelligence artificielle est perçue par

certains experts comme une source assez prometteuse[115]. Pour les autorités, l'utilisation de l'intelligence artificielle sera plutôt axée sur des systèmes d'IA (SIA) classificatrices. Ces systèmes sont à différencier des IA génératives, en tant qu'ils ne servent pas à créer des contenus, tels que du texte, des images ou des sons, mais permettent d'identifier et de traiter des contenus. L'objet de la classification dépendra alors de la manière dont ces systèmes seront programmés, mais également de l'exhaustivité de leurs bases de données et des capacités de leurs corpus. À cet effet, il est possible de programmer des systèmes d'intelligence artificielle pour repérer des fraudes ou des arnaques. L'algorithme de ces intelligences artificielles est conçu de telle sorte à ce qu'elles soient entrainées à repérer certains éléments (éléments graphiques, morceaux de codes, etc.) pour que, dès que la machine repère ces éléments, elle en classe la source. Les anti-spam des messageries électroniques sont un exemple d'intelligence artificielle classificatrice. Ces anti-spam ont été programmés pour repérer certains éléments dans les courriers électroniques reçus par le destinataire qui peuvent être le fait que l'adresse électronique est inconnue, qu'elle ressemble à une adresse officielle mais n'est pas identique, que sa composition (ordre des domaines, sous-domaines, etc.) est douteuse[116] ou que le contenu du message lui-même est litigieux. Pour ce qui est de l'usage de l'IA générative en défense, les autorités peuvent l'utiliser pour réaliser des règles de détection des menaces, pouvant elles-mêmes être intégrées dans la programmation des IA classificatrices. Les systèmes d'IA génératives peuvent aussi servir à faciliter l'utilisation de l'outil cyber en les rendant plus compréhensibles pour des personnes manquant d'expertise[117]. La condition la plus importante à remplir pour que l'usage de l'IA en défense face à la cyberdélinquance soit pertinent et efficace est de pouvoir disposer d'un nombre important de données pour l'entrainement de ces systèmes.

En parallèle, l'*Open source intelligence*[118] (OSINT), qui correspond au renseignement obtenu par des sources d'information publiques, est une méthode qui s'est répandue de manière exponentielle avec le développement d'internet. Le *Big Data*[119]est également un pilier du fonctionnement de l'OSINT, en ce qu'il permet le stockage d'une énorme de quantité de données

[115] Podcast Nolimit Sécu, avec Nicolas RUFF & Vladimir COLAS, & Gérôme BILLOIS, « Intelligence artificielle et cybersécurité », 24 septembre 2023
[116] Podcast La cybersécurité expliquée à ma grand-mère, C'est le jeu ma pauv Lucette », remixé le 26 mars 2023
[117] Podcast Nolimit Sécu, avec Nicolas RUFF & Vladimir COLAS, & Gérôme BILLOIS, « Intelligence artificielle et cybersécurité », 24 septembre 2023
[118] En français, « renseignement en source ouverte »
[119] En français, "données massives"

sur une base de données numériques[120]. Partant, l'OSINT est une méthode qui peut être utilisée par les autorités et par les individus pour faire de la veille informationnelle. C'est la stratégie adoptée par la start-up Storyzy, qui a mis en place une solution SaaS basée sur de l'intelligence artificielle, pour détecter et analyser les contenus de désinformation, d'incitation à la haine, de discrimination, etc.[121]. Il s'agit ici d'un cas de figure dans lequel le renseignement en source ouverte peut être utilisé pour lutter contre la violence numérique, par la détection et la prévention de la prolifération de certains propos interdits. Néanmoins, il est à préciser que l'OSINT, portant par définition sur ce qui est librement accessible, peut aussi servir aux pirates, qui peuvent aussi s'informer sur des entités, telles que des entreprises pour obtenir des renseignements, afin de perpétrer leurs méfaits (par exemple, des informations récupérées pour rendre les phishings ou les arnaques au Président plus crédibles)

De même, le chiffrement, déjà évoqué précédemment, est une technologie permettant de sécuriser ses communications par voie électronique, ses connexions ou d'autres informations[122]. Il permet donc de renforcer la sécurité des systèmes d'information, mais son ambivalence réside dans le fait qu'un protocole de chiffrement peut être utilisé par n'importe qui : individus à titre personnel, entreprises, autorités, pirates. Il s'agit donc d'un outil favorisant à la fois la défense des victimes potentielles de cybercriminalité mais aussi rendant plus difficile la poursuite et la recherche des cybercriminels. En effet, un rapport de l'Assemblée nationale a désigné le chiffrement comme « un outil de protection *ab initio* de la vie privée et de la confidentialité des correspondances » pour les individus[123]. L'utilisation d'un protocole de chiffrement est libre mais sa commercialisation est strictement encadrée par la loi, sous le contrôle de l'ANSSI.

En somme, les technologies de l'information et de la communication sont des outils qui possèdent, pour la plupart, de grandes potentialités de cybersécurité. Néanmoins, de la même manière qu'une pièce de monnaie possède deux faces, les mêmes outils numériques – et bien d'autres encore – peuvent servir aux pirates.

---

[120] J. ROBERT, "Machine Learning : Définition, fonctionnement, utilisations", Site DataScientest, 18 novembre 2020

[121] Site Storyzy, « Traquez la désinformation » : https://storyzy.com/?lang=fr

[122] Pour un historique du chiffrement, voir : S. SINGH, *The Code Book, The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, 1999

[123] Assemblée nationale, rapport d'information n°2623 sur "les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale", 11 octobre 200

2- Des outils comme support d'illicéité et d'accroissement du risque cyber

Les NTIC peuvent aussi être un support d'illicéité et d'accroissement du risque cyber sur la base de deux aspects principaux : les nouvelles failles de sécurité potentielles ouvertes par ces technologies ou l'usage qui est fait de ces nouvelles technologies par les pirates. Le cas du *Darknet* a déjà été évoqué et ne sera pas rementionné ici. Il est néanmoins possible de mentionner l'autre facette de l'intelligence artificielle et de l'ordinateur quantique comme outils pouvant être utilisés, actuellement ou à l'avenir, par les pirates, ou encore de se pencher sur le cas des systèmes hérités et sur certains comportements des individus comme source de failles de sécurité.

En ce qui concerne les sources de failles de sécurité, elles peuvent être causées par l'utilisation de systèmes hérités (ou systèmes en fin de vie) par les individus, tant dans une sphère personnelle que professionnelle. Il est cependant assez paradoxal d'évoquer les systèmes hérités au titre des nouvelles technologies, puisqu'ils se caractérisent justement par leur absence de nouveauté. Malgré tout, il s'agit indéniablement de technologies de l'information et de la communication. Ces systèmes sont évoqués à l'article 3.1 du règlement DORA et y sont décrits comme « un système de TIC qui a atteint la fin de son cycle de vie (fin de vie), qui ne se prête pas à des mises à jour ou des corrections, pour des raisons technologiques ou commerciales, ou qui n'est plus pris en charge par son fournisseur ou par un prestataire tiers de services TIC, mais qui est toujours utilisé […] ». La seule utilisation d'un système hérité nuit à la sécurité d'un système d'information, notamment car elle diminue la disponibilité et l'intégrité des données, mais aussi parce qu'en l'absence de mise à jour de ces systèmes hérités, les mesures de sécurité technique visant à protéger contre les accès indésirables finissent par devenir obsolètes. Ils deviennent alors une source bien plus importante de vulnérabilités[124]. Les vulnérabilités apparaîtront et se multiplieront de manière exponentielle à mesure que l'obsolescence du système augmentera. Le règlement DORA a vocation à encadrer spécifiquement l'usage et le remplacement de ces systèmes hérités dans le secteur financier. La directive NIS 2 n'en traite pas spécifiquement, mais les concernera forcément par les impératifs que ses transpositions impliqueront, notamment à l'encontre des *Supervisory Control And Data Acquisition* (SCADA).

[124] Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.

Concernant l'intelligence artificielle, c'est principalement l'IA générative qui peut représenter une source de dangers, de par l'utilisation que les pirates informatiques peuvent en faire. Les IA peuvent permettre d'augmenter l'efficacité des *phishings*, en les massifiant et en les rendant plus crédibles. En quelques sortes, en ce qui concerne les *phishing*s, on assiste à une confrontation de l'usage des IA en attaque et en défense, les IA classificatrices étant utilisées en défense pour détecter les tentatives d'hameçonnage et les IA génératives principalement en attaque pour tenter de duper plus efficacement les victimes en renforçant le procédé d'ingénierie sociale et en visant à contourner les détections de malveillances des diverses protections (antivirus, pare-feu…). C'est pour cette raison que les algorithmes de fonctionnement des logiciels de détection des menaces par hameçonnage sont rendus secrets et ne doivent être révélés sous aucun prétexte.

Malgré tout, les pirates informatiques possèdent généralement une forte capacité d'adaptation, expliquée par leur expertise et leur connaissance pointue du domaine cyber, qui leur permet de supposer les règles générales qui façonnent le développement de ces IA pour les contourner. En clair, les pirates, par la multiplication des tentatives d'arnaques, tirent des retours d'expérience et peuvent parvenir à déduire les critères de détection des algorithmes des IA en défense. En matière de *phishing*, on peut citer à titre d'exemple le fait que les arnaques au président, un cas plutôt classique de cybermenace, connaissent aujourd'hui une recrudescence par le recours des pirates à l'IA. Il s'agit du cas dans lequel le fraudeur se fait passer pour le dirigeant d'une société, et tente de faire transférer sur un compte bancaire lui appartenant une somme d'argent transférée au nom de la société. Cette arnaque est à craindre avec les possibilités offertes par les *deepfakes*. Ces montages par intelligence artificielle pourront en effet réaliser une synthèse intégrale de la voix ou du visage – voire les deux – du dirigeant de la société pour accroître la crédibilité de la fraude. Face à cela, il existe certains indices de détection d'un *deepfake* qui sont, déjà aujourd'hui, assez difficiles à repérer et dont la facilité de détection risque de diminuer au fil du développement de cette technologie[125]. En outre, les *deepfakes* pourront aussi être à la source d'actes de violence numérique plus « classiques » attentant à la dignité des personnes, consacrée par la Charte des droits fondamentaux de l'Union européenne[126], tels que le *deepfake porn*[127].

[125] Sur les critères de détection d'un *deepfake* : France Bleu, « Comment repérer les *deepfakes* ? », 19 février 2024
[126] Article 1 Charte des droits fondamentaux de l'Union européenne

ChatGPT est une IA générative qui illustre à elle seule un grand nombre des problématiques de cybersécurité (et bien d'autres) liées à l'IA. En effet, ce *Large Language model*[128] (LLM) est basé sur une analyse mathématique de la requête textuelle de l'utilisateur (*input*), pour générer un résultat (*output*) sans nécessité d'avoir la connaissance textuelle de la question. Chat GPT étant un système d'intelligence artificielle fonctionnant sur l'apprentissage et la rétroaction (*deeplearning*[129]), son efficacité augmente de manière exponentielle en fonction de la masse des données d'entrainement de son corpus et de son nombre d'utilisation. Ces modèles se traduisent par une inefficacité lors de leur lancement. Cette inefficacité a pu se traduire par la divulgation par Chat GPT à un utilisateur des clés de Windows 10[130] ou la création de *malwares* indétectables, signifiant en plus que ce système a été entrainé pour partie avec un corpus d'information composé de codes malveillant, selon la définition du *Large language Model*.

Enfin, l'ordinateur quantique est une nouvelle technologie qui, même si elle est encore loin d'avoir développé toutes ses potentialités, pourra être à même de changer une partie de la logique du chiffrement telle qu'on la connait aujourd'hui. Il s'agit d'une machine qui s'appuie sur des principes de physique quantique pour réaliser des calculs inaccessibles à des ordinateurs classiques. L'idée est que ces machines se basent sur l'approche probabiliste de la physique quantique pour arriver beaucoup plus rapidement à une solution, pour des problèmes d'une complexité similaire[131]. Ces ordinateurs, s'ils atteignent leur maturité, pourraient parvenir à casser des clés RSA[132], résoudre des problèmes combinatoires dans la finance, émettre des analyses de risques beaucoup plus fiables, etc. En d'autres termes, ils n'auraient pas qu'un impact dans la cybersécurité, mais pourraient impliquer de repenser tout le processus de chiffrement et de calcul. Pour éviter ces effets négatifs, on pourrait recourir à la cryptographie post-quantique, qui s'appuie sur des principes mathématiques pour ériger des problèmes trop complexes, même pour l'ordinateur quantique, ou sur la cryptographie quantique qui reposerait

---

[127] Interview L. LANDES-GRONOWSKI « Le *deepfake porn* », France 24, 23 mars 2024

[128] En français, « grand modèle de langage ». Correspond à un modèle de fondation entrainé sur un corpus de texte

[129] En français, "apprentissage profond"

[130] Site Futura, « ChatGPT peut générer des clés de licence pour Windows 10 et 11 ! » : https://www.futura-sciences.com/tech/actualites/intelligence-artificielle-chatgpt-peut-generer-cles-licence-windows-10-11-105932/

[131] Podcast La cybersécurité expliquée à ma grand-mère, avec Olivier EZRATTY, « L'ordinateur quantique et la cybersécurité », 4 mars 2024

[132] Clé de chiffrement basée sur le fait qu'il est facile de multiplier deux grands nombres premiers mais difficile d'en factoriser le produit

sur des principes de physique quantique pour pouvoir aboutir à une génération simultanée et aléatoire de clés de chiffrement qui rendrait impossible le fait de pouvoir les deviner.

En somme, les technologies de l'information et de la communication se caractérisent par leurs usages ambivalents, tant en défense qu'en attaque. Qu'il s'agisse des systèmes hérités, de l'ordinateur quantique, de l'intelligence artificielle, ou de toute autre technologie pouvant être utilisée pour renforcer ou affaiblir la sécurité des systèmes d'information, ces outils doivent être encadrés juridiquement. Mais, si l'approche juridique ne suffit pas à elle seule, laisser complètement libre cours aux nouvelles technologies n'est pas non plus une solution viable. En plus de cela, il est nécessaire qu'une collaboration étroite soit établie entre la sphère privée et la sphère publique, pour donner un terreau fertile à cet encadrement.

C) La nécessaire coopération entre autorités publiques et acteurs privés : des intérêts et bénéfices partagés

La coopération entre la sphère privée et la sphère publique est à la fois bénéfique pour les entreprises, les individus et les autorités. L'ensemble des normes de droit dur et de droit souple doivent être prises en considération dans la pratique, notamment pour protéger les droits et libertés des individus (**1**). Cette interdépendance peut également être une opportunité pour rendre plus efficiente la spécialisation des autorités dans le domaine de la cybersécurité qui pourront alors mieux encadrer la violence numérique et la cybercriminalité (**2**)

1- La sécurité des systèmes d'information : pour une meilleure protection des droits fondamentaux

Assurer la sécurité des systèmes d'information ne revient pas seulement à limiter le risque cyber et prévenir la prolifération de la violence numérique. Ce pan, axé sur la poursuite et la répression de la cybercriminalité, doit incontestablement être doublé de la protection des victimes et de la garantie de leurs droits fondamentaux. C'est une considération que les législateurs européen et français ont bien assimilée. Appréhender la loi Godfrain avec une approche exégétique fait, en ce sens, remonter aux justifications originelles du droit pénal. Même si tous les textes liés, de près ou de loin, à la cybersécurité ne possèdent pas un aspect pénal

entendu dans le sens de la sanction des criminels et délinquants, ils partagent en revanche l'idée qu'il est nécessaire de protéger la société. En matière de numérique, les articles 16 et 114 du Traité sur le fonctionnement de l'Union européenne (TFUE) fondent l'élaboration de textes visant à la construction d'un marché unique des données au sein de l'Union européenne. La volonté de fonder un marché européen des données n'est pas basée que sur des considérations économiques, il s'agit aussi de préserver les droits numériques des ressortissants européens face aux risques que peuvent présenter les nouvelles technologies. Comment ne pas citer, alors, la série d'amendements pris en mai 2023 par les députés européens des commissions des libertés civiles et du marché intérieur, visant à ce que les règles et obligations du règlement soient plus protectrices des droits et libertés des individus, mais aussi de l'environnement ? Cette série d'amendements manifeste, s'il en est, la complexité des débats qui ont guidé l'élaboration du texte sur l'intelligence artificielle, opposant la frange des députés en faveur d'une protection sans nuances des droits des individus, aux parlementaires européens soutenant un règlement plus souple pour les entreprises – au détriment des individus – dans la droite ligne de ce vers quoi les lobbies d'entreprise voulaient tendre[133].

De manière générale, un grand nombre de textes européens régissant le secteur du numérique consacrent des garanties pour la protection des droits des personnes physiques : le DSA, le DMA, le RGPD et l'IA Act en sont autant d'exemples. À ce titre, on citera les articles 15 à 22 du RGPD, consacrés aux droits des personnes concernées[134], et l'article 32 qui concerne les mesures techniques et organisationnelles devant être prises par les responsables de traitement et sous-traitants pour assurer la sécurité des données. Sont notamment citées dans cet article l'intégrité, la confidentialité et la disponibilité des données (mais pas la traçabilité). Il est possible de déduire de la réunion de ces articles que la sécurité des systèmes d'information est liée aux droits fondamentaux des individus. Ce postulat est également présent dans le considérant 10 du règlement sur l'IA qui indique que la protection des droits des individus implique une application non discriminatoire et sécurisée du règlement aux entités qui y sont soumises. Le considérant 14 de la directive NIS 2 concerne, quant à lui, l'articulation entre les textes européens, mentionnant que l'application de cette directive ne doit pas porter atteinte au droit

[133] C. CASTETS-RENARD et B. DABAN, « Proposition de réglementation de l'IA : le Parlement européen renforce la protection des individus », Le club des juristes, 23 juin 2023

[134] Au sens de l'article 4.1 du RGPD, une personne concernée est une « personne physique identifiée ou identifiable »

applicable en matière de protection des données. Un grand nombre de ces textes européens a donc été pensé, au moins pour partie, selon le postulat que la technologie devait être encadrée pour ne pas que ses potentielles dérives soient néfastes pour les droits des personnes physiques. Cette idée ne signifie pas que la technologie est mauvaise en elle-même, mais plutôt que de son usage, peuvent naitre différents types de risques cyber pour les droits fondamentaux, risque qui doivent ainsi être contenus. D'une part, ces risques peuvent être causés par l'usage commercial de ces technologies. D'autre part, le risque peut provenir de l'utilisation même de ces appareils par les individus.

L'enjeu de préservation des droits des individus, qui pourraient se voir menacés par l'usage que les entreprises font des nouvelles technologies, est plutôt une question de droit de la concurrence. Il n'est pas strictement nécessaire de l'aborder dans ce cadre. En revanche, pour ce qui est des risques intrinsèques à l'usage des nouvelles technologies, la pertinence de la problématique s'impose d'elle-même. Il s'agit bien ici de traiter spécifiquement de l'influence des nouvelles technologies sur les droits fondamentaux, spécifiquement par rapport à l'influence des NTIC en attaque et en défense (cf. **II], B) 1-** & **2-**).

La technologie, à travers les usages qui en sont faits, a des impacts sur les droits des individus. Il convient donc d'encadrer cet usage. Malgré tout, un paradoxe apparait assez rapidement lorsqu'on s'attache à encadrer l'utilisation des outils numériques. En effet, il est nécessaire que la manière de se servir de ces outils ne nuise pas, directement ou indirectement, aux droits des individus. Pour éviter cela, il faut réglementer les nouvelles technologies dans leur ensemble, depuis leur création jusqu'à leur diffusion. Pourtant, un encadrement trop strict du rapport entre les NTIC et les individus peut conduire à des ingérences dans l'utilisation qu'ils en font et donc, nuire à leurs droits et libertés. Il convient alors de trouver le bon équilibre entre la protection de chaque sujet de droit contre les risques intrinsèques au secteur digital et la liberté, au sens du droit objectif, qui doit leur être laissée. Cet équilibre à trouver entre liberté et droit individuel existe de manière générale et n'est pas propre au numérique[135]. Une fois encore, l'intelligence artificielle apparait comme la caisse de résonnance de cette affirmation. De fait, les nombreux biais pouvant naitre de l'utilisation faite de l'IA illustrent très bien les impacts que peuvent avoir les nouvelles technologies sur le comportement et par extension, les droits des

[135] F. CHALTIEL, « L'équilibre entre sécurité et liberté devant le juge constitutionnel », Revue de droit constitutionnel, Actu-Juridique, Lextenso, 11 juillet 2019

individus. L'IA et tout ce qui l'entoure (algorithmes, logiciels…) sont à la fois des réceptacles, des amplificateurs et des créateurs de biais influençant le comportement humain. Il est principalement possible de constater deux catégories de phénomènes menant à des biais. Premièrement, le fonctionnement de l'intelligence artificielle peut créer ou exacerber certains biais de pensée chez les utilisateurs, lorsque ces derniers sont le public cible de l'utilisation du SIA. Ce principe même de renforcement des biais de pensée existe avec d'autres outils numériques, depuis plusieurs années, tels que les réseaux sociaux. Deuxièmement, les individus à l'origine du SIA (producteurs, développeurs, testeurs, etc.) peuvent être eux-mêmes soumis à certains biais de pensée qui ont alors une influence notable sur la manière dont l'intelligence artificielle fonctionnera. Dans le premier cas, la confiance excessive accordée par les individus en l'IA les pousse vers un biais d'automatisation, dérivé du biais d'autorité, qui se manifeste dans l'idée chez certains utilisateurs que l'intelligence artificielle a toujours raison. Pour ne pas céder à ce biais, il faut avoir conscience qu'il y a toujours un risque de conclusions erronées (faux positifs et faux négatifs) dans ces systèmes, justifiant la nécessité de contrôle humain, elle-même consacrée par l'article 14 du règlement sur l'IA. Dans le second cas, ce sont les propres biais des développeurs d'IA qui se matérialisent dans le SIA ; ce système les amplifie alors et les transmet au public visé à travers son utilisation.

De manière plus générale, la sécurité des systèmes d'information est liée à la protection des droits et libertés puisqu'attenter au bien-être numérique des individus les prive d'un certain nombre de droits. Par exemple, s'infiltrer dans l'ordinateur personnel d'une personne physique, copier ses données personnelles et les diffuser sans son consentement attente au droit à la vie privée de ce dernier. Bien évidemment, il existe une infinité d'autres cas de figure illustrant l'intrication des droits fondamentaux dans la sécurité des systèmes d'information et l'interdépendance entre ces deux notions.

En somme, la bonne compréhension par les autorités de la manière dont la sécurité des systèmes d'information garantit l'effectivité des droits des individus est cruciale. Cette compréhension passe par une forte compétence sur le sujet et sur la réalité pratique que vivent ces personnes, dans le cadre personnel et dans le cadre professionnel. En outre, l'encadrement de la violence numérique et du risque cyber ne pourra se faire de manière optimale que si les bons usages préconisés par les autorités sont respectés par l'ensemble des sujets de droit.

2- L'imprégnation du secteur privé dans les autorités publiques : la spécialisation pour un meilleur encadrement

La spécialisation des autorités s'entend en partie par des liens plus solides avec la sphère privée, notamment professionnelle. En effet, viser un encadrement optimal de la violence numérique et du risque cyber ne peut s'entendre que par une bonne connaissance de la réalité pratique. C'est ainsi que, d'une part, les agences comme l'ANSSI seront à même de recruter leurs membres directement parmi les experts du domaine (ingénieurs, informaticiens, juristes…) et que, d'autre part, elles laisseront une plus grande latitude aux acteurs professionnels pour assurer la sécurité de leurs systèmes d'information.

Pour illustrer le fait que les autorités décident de s'appuyer sur le secteur privé pour recruter leurs membres, on citera le cas de l'OFAC qui s'est appuyé sur des ingénieurs contractuels, ne venant pas de la police, pour augmenter son expertise dans la cybersécurité[136]. Mais, cette initiative, pour une autorité de police comme l'OFAC, pose un problème majeur rapidement identifiable. Si ces ingénieurs et autres experts apportent des connaissances et des méthodes pratiques indéniables, ceux-ci n'ont pas les bases de l'investigation, des poursuites judiciaires, de la répression pénale, etc. Ils doivent donc être formés aux activités de l'OFAC pour agir conformément à la réglementation.

En parallèle, les autorités, permettent et encouragent le développement d'initiatives permettant au monde professionnel de mieux se protéger contre les cybermenaces, au premier rang desquels, les *Hackers* éthiques. Les *Hackers* éthiques sont des personnes physiques salariées d'une entreprise ou employées par un organisme public, chargées de déceler et corriger les failles existant dans un système d'information[137]. Cette dénomination, bien qu'assez équivoque, ne doit pas porter à confusion : un *hacker* éthique ne doit pas être confondu avec une personne amatrice qui porte atteinte à des STAD pour des raisons dites « éthiques ». En effet, les *hackers* éthiques sont des experts dans la cybersécurité, contractuellement chargés de tester la sécurité des systèmes d'information d'une entreprise. Ce sont les contrats passés avec les entreprises ou avec l'Etat qui légalisent leurs actions. De manière générale, cette profession s'est développée et démultipliée à mesure que les entreprises et l'Etat réalisaient la nécessité d'assurer

[136] B. SIMON, « Pirates, Darkweb et cryptomonnaie : la police lance son superservice anti-cybercriminalité », Le Point, 19 janvier 2024

[137] Site Rendre notre monde + sûr, « Des *hackers* éthiques au service de la cybersécurité des entreprises » : https://rendre-notre-monde-plus-sur.goron.fr/des-hackers-ethiques-au-service-de-la-cybersecurite-des-entreprises/

leur cybersécurité. Très concrètement, un *hacker* éthique doit penser comme un cyberattaquant pour identifier les failles de sécurité d'un système d'information et déjouer le piratage avant qu'il ne survienne. Cette immixtion dans l'esprit d'un cyberattaquant implique que la personne chargée de tester la cybersécurité d'une entité trouve un moyen d'accéder dans un système d'information ou d'y porter atteinte d'une quelconque manière[138]. En clair, un *pentester*[139] fait partie de la catégorie des *hackers* éthiques, bien que ces derniers regroupent une réalité beaucoup plus large, puisque cela comprend, selon Haris Pylarinos, PDG de *Hack The Box*, « toutes les personnes utilisant des outils et techniques utilisés pour mettre en place des attaques et tester les faiblesses d'un environnement informatique ». Cependant, en prenant le cas du *pentest*, qui donne lieu au plus de contrats de prestations, il est absolument indispensable de bien définir le champ d'application du contrat, pour déterminer de manière exhaustive les missions du *pentester*. Dans le cas contraire, si un prestataire réalise une intrusion dans un système hors du champ du contrat, ce dernier pourrait voir sa responsabilité contractuelle, mais aussi pénale engagée. Néanmoins, la responsabilité pénale ne pourra être engagée que par la réunion de l'élément matériel (une intrusion) et de l'élément intentionnel qui nécessité de démontrer l'intention frauduleuse du prestataire. L'intention pourra être présumée par l'absence patente d'autorisation du maitre du système[140] et la connaissance de cause du *pentester*. Enfin, concernant le développement de la profession des *hackers* éthiques et la meilleure prise en compte de cette réalité par les autorités, il est possible de mentionner la plateforme *YesWeHack*[141], notamment utilisée par le ministère de la Défense français fonctionnant sur le principe du *bug bounty*. Également, BreizhCTF[142] est une compétition créée en 2015, mise en place pour faire valoir les talents parmi les *hackers éthiques.* Cette compétition illustre bien le développement de l'intérêt pour cet aspect de la cybersécurité.

À côté des prestataires d'*hacking*, professionnels contractuellement chargés de tester le niveau de sécurité du système d'information d'une entité, la *Threat Intelligence*[143] constitue également une procédure mise en place pour être plus préparé aux cybermenaces. Il s'agit, ici aussi, d'une méthode mise en place pour comprendre comment fonctionne les attaquants et ainsi

[138] Site ZDNET, « Qu'est-ce qu'un *hacker* éthique ? » : https://www.zdnet.fr/actualites/cyberattaque-4000237415q.htm/page/68
[139] En français : « testeur d'intrusion »
[140] Cour d'appel de Toulouse, 21 janvier 1999
[141] Site, YesWeHack : https://www.yeswehack.com/fr
[142] Site BreizhCTF : https://www.breizhctf.com/
[143] En français, « renseignement sur les menaces »

mieux s'en protéger. Cette activité existe depuis une vingtaine d'années et s'est considérablement développée en parallèle des menaces persistantes avancées et de l'essor de l'OSINT[144]. De manière générale, la *Threat Intelligence* consiste moins à se questionner sur les auteurs que sur les mobiles, la méthode employée et les conséquences potentielles de la menace. En guise d'exemple, pour traquer le groupe de *hackers* APT 41, la *Threat Intelligence* avait permis de retrouver des traces de noms de domaine, de logiciels malveillants fréquemment utilisés, afin d'analyser les cas de figure dans lesquels ces noms de domaine et ces logiciels malveillants réapparaissent, plutôt que de se concentrer uniquement sur les personnes à l'origine de ces cyberattaques. Pour rendre plus efficace cette méthode, il est aussi possible de se servir de bases de données spécialisées permettant de scanner internet tels que Shodan, ou VirusTotal, afin de maximiser l'efficacité d'une collecte en ligne en rapport avec tout ce qui concerne les menaces. Enfin, la *Threat Intelligence* peut être renforcée par des activités de *purple team*, qui constituent le versant plus opérationnel du renseignement cyber[145]. Cette activité consiste à faire collaborer les *blue* et les *red teams* pour renforcer la compréhension des cybercriminels.

En somme, au-delà de permettre une meilleure protection des droits fondamentaux, la coopération entre les sphères privée et publique permet une spécialisation des autorités et des entreprises par la mise en commun de moyens et de connaissances pour renforcer la protection contre les cybermenaces. Ces initiatives de renforcement doivent cependant être strictement encadrées sur le plan juridique pour rester légales, tandis qu'aujourd'hui, les réflexes cyber sont loin d'être complétement assimilés par les individus (**Voir en annexe : graphe question 8**)

[144] Podcast No Log, avec Barbara LOUIS SIDNEY, « Le renseignement cyber », 11 janvier 2021
[145] Idem.

Conclusion

En conclusion, il n'est pas exagéré de dire que la violence numérique et le risque cyber n'ont jamais été aussi prégnants dans notre société. Avec le développement des nouvelles technologies, les pirates informatiques et délinquants en tous genres ne cessent de se renouveler pour attraper le maximum de cyber victimes dans leurs filets. Face à cela, la frénésie législative européenne et, de manière plus générale, le droit, ne peuvent endiguer ce phénomène avec une approche qui ne soit que juridique. En effet, la nouveauté, la complexité et le développement continu du numérique amènent à penser que le droit, à la remorque de la technologie ne pourra suffire à lui seul (**Voir en annexe : graphe question 6**). L'ensemble des autorités, c'est-à-dire le législateur, les juges, les autorités de police et les organismes de contrôle et de prévention, doivent – et ont entrepris de – se spécialiser en la matière pour combattre à armes égales les délinquants. L'enjeu de l'appropriation des nouvelles technologies comme l'IA entre aussi en ligne de compte, entrainant une sorte de course à l'armement entre ces autorités et les cyberdélinquants qui visent à orienter la direction que prendront les nouvelles technologies dans leur sens. Enfin, il est impératif que les autorités et le secteur privé soient en étroite collaboration, afin que la lutte contre les cybercriminels soit plus efficace et adaptée à la réalité de ce que sont aujourd'hui les pirates informatiques.

Si le problème de l'encadrement de la cybercriminalité est celui du retard, aussi bien technologique que juridique à cause des contraintes légales à respecter par les autorités, doit-on considérer que ce retard est propre à la cybercriminalité, ou est-il plus généralement inhérent à la lutte contre la délinquance ? Autre question : tandis que les SIA de police prédictive ont été interdits par l'IA Act, nous éloignant ainsi d'une société semblable à celle que l'on connait dans *Minority Report*,[146] prévoir un système de détection anticipée des cyber infractions, ou un système de justice prédictive[147], pour rattraper ce retard patent, pourrait-il être envisageable, tant sur le plan juridique que technique ?

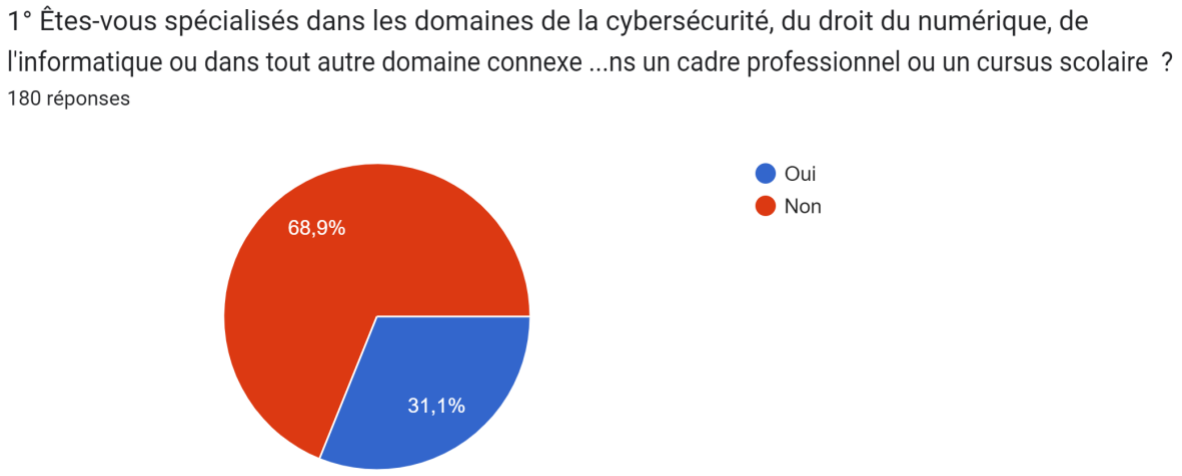
[146] S. SPIELBERG, *Minority Report*, Amblin Entertainment, 20th Century Studios, DreamWorks SKG, Cruise / Wagner Productions, 2002

[147] A. COLETTA, « La prédiction judiciaire par les algorithmes, thèse délivrée par l'Université de Nîmes », Hal open science, 27 janvier 2022

Annexe

Cette annexe est composée d'un questionnaire de neuf questions ayant obtenu 180 réponses. Parmi les 180 personnes ayant répondu au questionnaire, 56 (environ 30%) ont des connaissances en matière de cybersécurité ou dans une filière connexe (**Graphique question 1)**. Cette proportion a une influence sur les réponses obtenues. À chaque question posée est associée un graphique permettant de rendre compte des proportions des réponses obtenues. Les pourcentages obtenus ont été arrondis, expliquant que les pourcentages totaux des graphiques ne soient pas parfaitement équivalents à 100%. Tous les graphiques présentés seront ici expliqués et commentés.

Questionnaire :

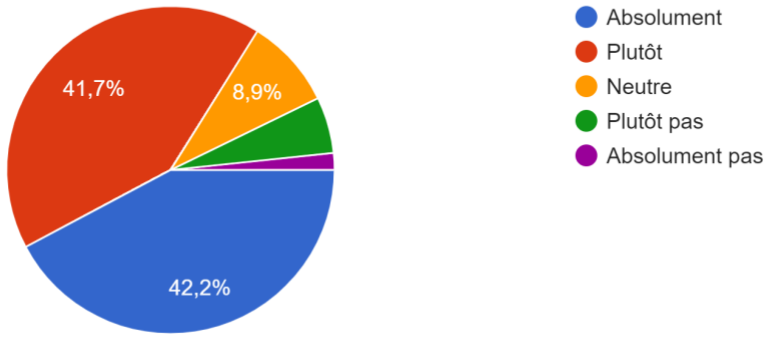


• Oui : 56 personnes (31.1%)

• Non : 124 personnes (68.9%)

2° La violence numérique (diffusion non consentie d'images à caractère privée, pédopornographie, cyberharcèlement…) est une source de préoccupation pour vous :

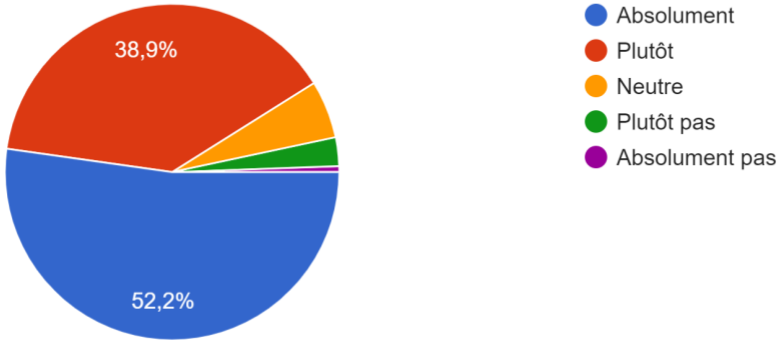
180 réponses



- Absolument : 76 personnes (42.2%)
- Plutôt : 75 personnes (41.7%)
- Neutre : 16 personnes (8.9%)
- Plutôt pas : 10 personnes (5.6%)
- Absolument pas : 3 personnes (1.7%)

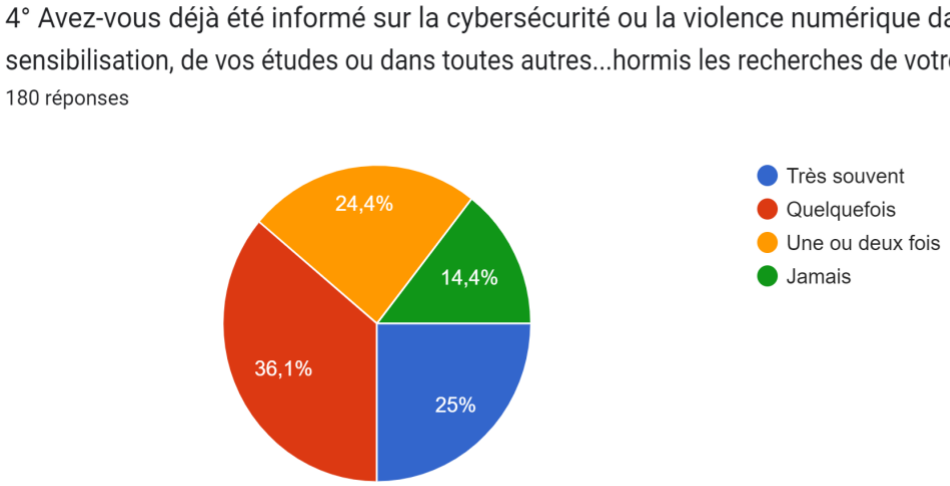
3° Le risque cyber (protection de vos données personnelles, cyberattaques, usurpation d'identité numérique…) est une source de préoccupation pour vous :

180 réponses



• Absolument : 94 personnes (52.2%)
• Plutôt : 70 personnes (38.9%)
• Neutre : 10 personnes (5.6%)
• Plutôt pas : 5 personnes (2.8%)
• Absolument pas : 1 personne (0.6%)

À la lecture de ces graphiques traités ensemble, on constate que la violence numérique et le risque cyber sont des préoccupations assez, voire très importantes, pour les individus (83% des répondants sont préoccupés par la violence numérique et 90% par le risque cyber), qu'ils aient des connaissances approfondies en cybersécurité, ou non. Il est possible de constater un intérêt plus net pour le risque cyber, mais, malgré tout, l'enjeu représenté par la violence numérique et le risque cyber semblent tous deux largement assimilés par les individus.



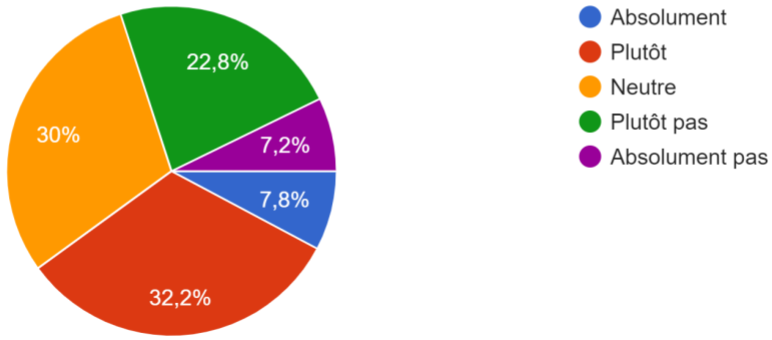
Question : « Avez-vous déjà été informé sur la cybersécurité ou la violence numérique dans le cadre d'une sensibilisation, de vos études ou dans toutes autres circonstances (hormis les recherches de votre propre initiative) ? »

• Très souvent : 45 personnes (25%)
• Quelquefois : 65 personnes (36.1%)
• Une ou deux fois : 44 personnes (24.4%)
• Jamais : 26 personnes (14.4%)

Ici, il à noter que 154 personnes (85.6% de la population interrogée) ont été informées ou sensibilisées au moins une fois à la cybersécurité. Cela constitue un nombre satisfaisant paraissant être en adéquation avec la proportion de personnes qui se sentent concernées par le risque cyber. Évidemment, on ne peut qu'encourager le fait que le pourcentage de personnes n'ayant été que peu ou pas informées diminue pour augmenter la part d'individus renseignés sur le sujet. En prenant en compte le fait que les technologies évoluent rapidement et avec elles, les cybermenaces, il est important que des opérations de sensibilisation soient régulièrement effectuées dans des cadres professionnels, scolaires, etc. Cette information doit être faite pour toutes les tranches d'âge – car le risque cyber concerne l'ensemble de la population – détaillant à la fois les enjeux du risque cyber et les mesures à prendre pour se protéger au mieux.

5° Vous voyez les nouvelles technologies telles que l'intelligence artificielle (IA), la chaîne de blocs (blockchain) ou les cryptomonnaies d'un bon œil :

180 réponses

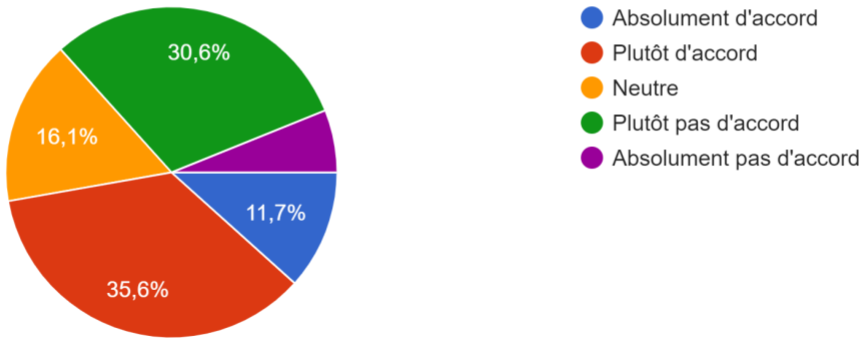


• Absolument : 14 personnes (7.8%)
• Plutôt : 58 personnes (32.2%)
• Neutre : 54 personnes (30%)
• Plutôt pas : 41 personnes (22.8%)
• Absolument pas : 13 personnes (7.2%)

Pour cette question, deux déductions principales sont à tirer. Premièrement, les parts des personnes qui voient d'un mauvais œil et d'un bon œil les nouvelles technologies sont assez similaires. En effet, 72 des personnes interrogées (40%) voient les nouvelles technologies comme une bonne chose contre 54 (30%) qui les voient comme une mauvaise chose. Deuxièmement, outre ce clivage, la part des personnes se disant « neutres » n'est pas négligeable. Ce deuxième constat a son importance et témoigne bien du fait qu'il est difficile de se prononcer de manière définitivement positive ou négative sur les technologies de l'information et de la communication. Cette réticence à prendre partie peut notamment être expliquée par un manque de connaissance, réel ou supposé, menant à un sentiment d'illégitimité sue le sujet.

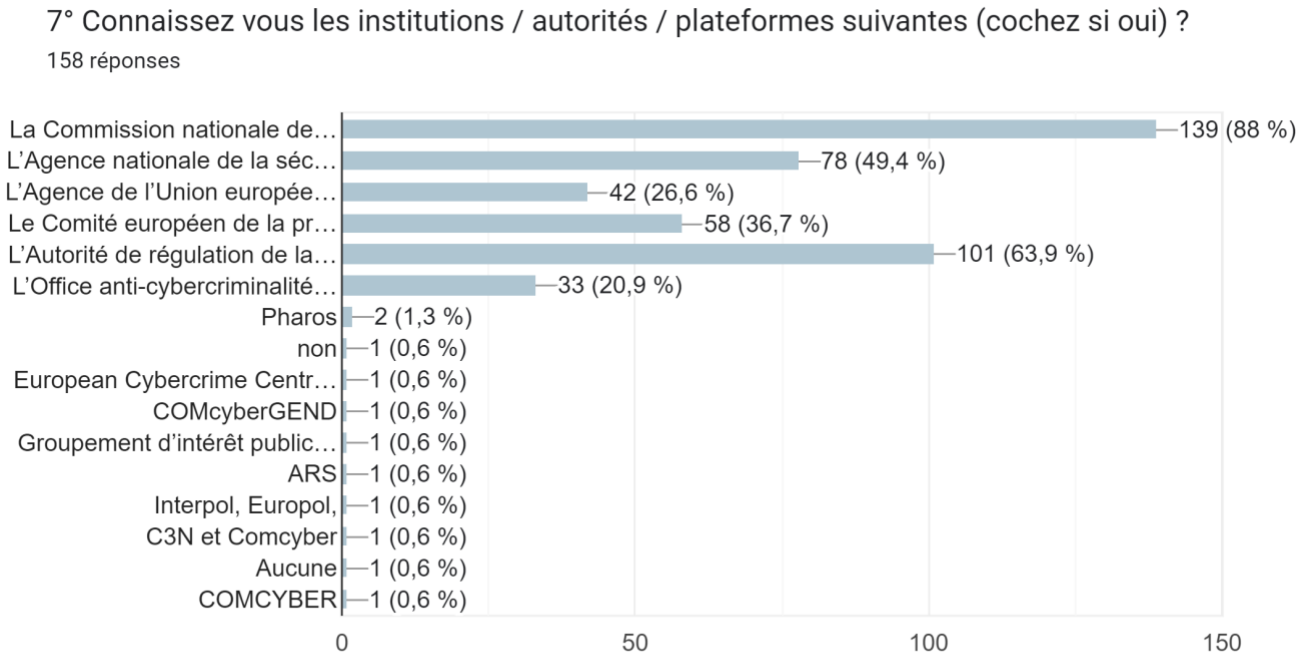
6° Le droit est impuissant pour encadrer le secteur numérique (réseaux sociaux, cybercriminalité, usage des nouvelles technologies…) :

180 réponses



• Absolument d'accord : 21 personnes (11.7%)
• Plutôt d'accord : 64 personnes (35.6%)
• Neutre : 29 personnes (16.1%)
• Plutôt pas d'accord : 55 personnes (30.6%)
• Absolument pas d'accord : 11 personnes (6.1%)

Ce diagramme circulaire indique que la part des personnes interrogées considérant que le droit est absolument ou plutôt impuissant pour encadrer le secteur numérique est légèrement supérieure à celle des personnes considérant qu'il ne l'est pas. (85 contre 66 personnes). Malgré tout, l'écart n'est pas considérable et doit être relativisé par le fait que le numérique, par son caractère nouveau et la puissance de certaines entreprises associées à ce secteur, peut être vu, de l'extérieur, comme un domaine incontrôlable. En outre, pour cette question non plus, la part de sondés se disant « neutres », même si elle est moins importante que pour la question précédente, n'est pas négligeable. Cela témoigne encore une fois de la complexité de cette question ou d'une relative méconnaissance de certaines personnes qui justifierait qu'elles ne prennent pas parti.

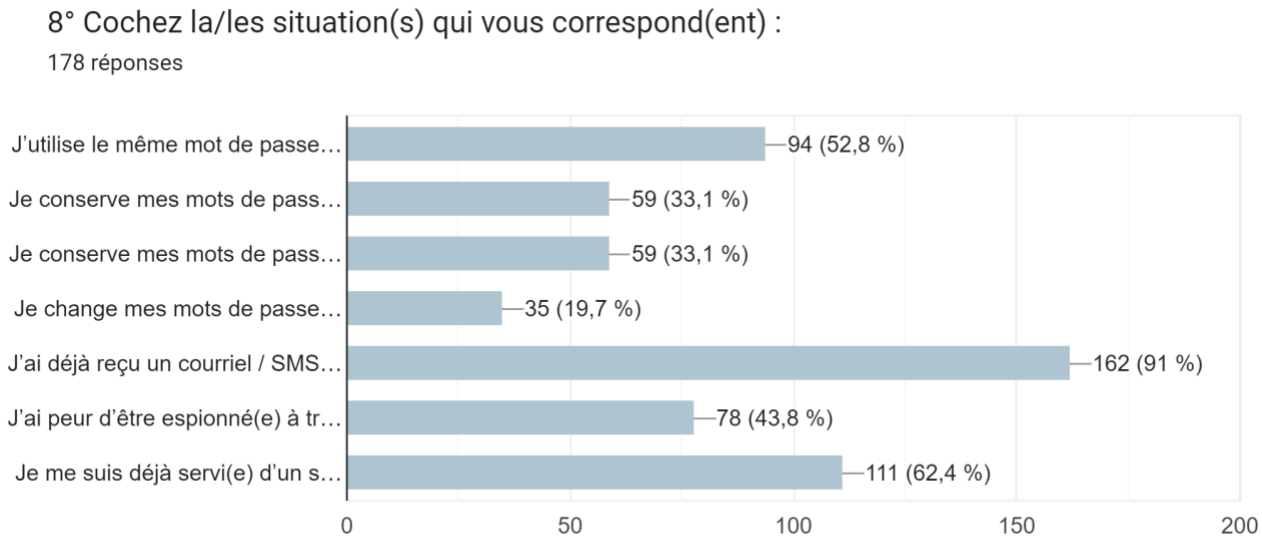


NB : Les noms des organismes (de haut en bas) sont : la CNIL, l'ANSSI, l'ENISA, le CEPD, l'Arcom, et l'OFAC. Les réponses libres (à partir de Pharos jusqu'à COMCYBER) apportées par les personnes interrogées, bien qu'intéressantes, ne seront pas mentionnées ici car elles ne sont pas assez nombreuses pour former des statistiques fiables. En outre, ces réponses ont pu être apportées par des personnes expertes en cybersécurité ; cette incertitude étant admise, il n'est pas possible de tirer un intérêt de ces réponses.

Les résultats de ce graphique en barres doivent être pris avec plus de précautions que les précédents. D'une part, seules 158 personnes ont inscrit au moins une réponse. Les pourcentages obtenus sont basés sur le total des personnes ayant inscrit au moins une réponse et non sur le total des personnes interrogées. D'autre part, le fait que sur l'ensemble des 180 personnes interrogées, 56 ont des connaissances en matière d'informatique, de cybersécurité ou de tout autre domaine connexe doit être pris en compte. En outre, étant donné que le nombre des personnes ayant répondu à cette question n'est pas égal au nombre de personnes interrogées, il

est possible de se demander quelle est la part de personnes ayant des connaissances en cybersécurité dans les personnes ayant répondu.

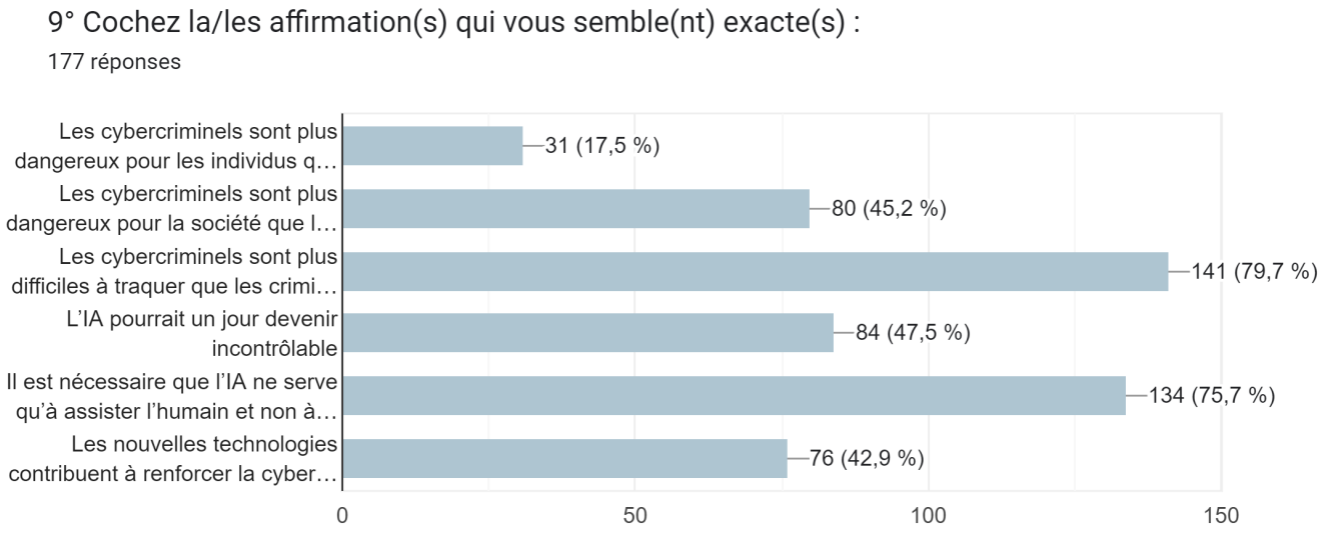
Malgré tout, il est possible de noter que la CNIL bénéficie de la renommée la plus notable (88% des répondants), suivie par l'Arcom (63.9% des répondants). Plus d'un répondant sur deux ne connait pas l'ANSSI (49.4%). Les organismes européens, au vu de ce graphique, souffrent clairement d'un manque de renommée (36.7% pour le CEPD et 26.6% pour l'ENISA). Enfin, l'OFAC est connue par moins d'une personne sur quatre (20.9%). Le manque de renommée de l'OFAC est moins problématique que celui de l'ANSSI étant donné que l'agence nationale de la sécurité des systèmes d'information est beaucoup plus en lien avec les individus, chargée de réaliser des communications, des recommandations, etc. En clair, de sa renommée, dépend une partie de son efficacité dans la réalisation de ses missions. Cette renommée inférieure à la CNIL et à l'Arcom peut s'expliquer par une création postérieure. En effet, la CNIL est apparue avec la LIL en 1978, l'Arcom sous sa forme originelle du CSA en 1989, tandis que l'ANSSI a vu le jour en 2009 seulement. En outre, l'Arcom et la CNIL sont des institutions plus médiatisées qui sont très certainement plus en contact des profanes, tandis que la connaissance de l'ANSSI semble conditionnée par une appétence minimale à la cybersécurité. Pourtant, la sécurité des systèmes d'information doit être prise au sérieux au même titre que la protection des données, au vu de son importance actuelle. Le degré de connaissance de l'ANSSI souffre donc de la complexité inhérente et de l'expertise nécessaire à la cybersécurité.



NB : les situations proposées sont (de haut en bas) :

- *J'utilise le même mot de passe pour accéder à plusieurs sites / comptes / applications différents*
- *Je conserve mes mots de passe dans un coffre-fort électronique sécurisé*
- *Je conserve mes mots de passe sur les notes de mon téléphone / en photo / sur une clé USB / sur un papier*
- *Je change mes mots de passe au moins une fois par an*
- *J'ai déjà reçu un courriel / SMS douteux me demandant de cliquer sur un lien ou d'ouvrir une pièce jointe pour bénéficier d'une offre ou régler une somme*
- *J'ai peur d'être espionné(e) à travers mon utilisation des outils numériques (sites consultés, conservation par les caméras d'ordinateurs ou de téléphone, géolocalisation en temps réel)*
- *Je me suis déjà servi(e) d'un système d'intelligence artificielle générative (ChatGPT, Midjourney, Dall-E…)*

Plusieurs phénomènes doivent être relevés dans le cas présent. Premièrement, le *phishing* est un phénomène de très grande ampleur, étant donné que neuf répondants sur dix ont déjà fait l'objet d'au moins une tentative d'hameçonnage. Deuxièmement, les pratiques des personnes interrogées concernant les mots de passe sont améliorables : plus d'une personne sur deux utilise le même mot de passe pour plusieurs authentifications différentes, augmentant le risque d'attaque par *crendential stuffing*, seul un cinquième des personnes change annuellement ses mots de passe, un tiers des individus conserve ses mots de passe dans un format non conforme aux recommandations de l'ANSSI. En outre, il est possible de remarquer que la peur d'être espionné n'est pas négligeable (43.8% des répondants). Enfin, 62.4 % des répondants se sont déjà servis d'une IA générative. En se penchant sur les statistiques concernant le phishing et les statistiques sur les mots de passe, un paradoxe apparait : les cybermenaces sont très répandues, mais les pratiques de cybersécurité restent améliorables.



NB : les affirmations proposées sont (de haut en bas) :

- *Les cybercriminels sont plus dangereux pour les individus que les criminels « classiques »*
- *Les cybercriminels sont plus dangereux pour la société que les criminels « classiques »*
- *Les cybercriminels sont plus difficiles à traquer que les criminels « classiques »*
- *L'IA pourrait un jour devenir incontrôlable*
- *Il est nécessaire que l'IA ne serve qu'à assister l'humain et non à la supplanter*
- *Les nouvelles technologies contribuent à renforcer la cybersécurité*

L'analyse de ce diagramme renseigne tout d'abord sur le fait que les répondants considèrent dans la globalité que les cybercriminels ne sont pas plus dangereux pour les individus que les criminels dits « classiques ». Il est intéressant de relever l'écart observé des réponses entre la question de la dangerosité des cybercriminels pour les individus et celle de la dangerosité pour la société. En outre, la grande majorité des sondés est consciente que les cybercriminels sont plus difficiles à traquer que les criminels dits « classiques ». Concernant l'intelligence artificielle et les nouvelles technologies, il est d'abord possible de relever que trois

quarts des sondés considèrent que l'IA doit conserver un rôle d'assistance de l'être humain (75.7%). Près d'une personne sur deux (47.5%) craint que l'IA ne devienne incontrôlable. Enfin, 76 personnes soutiennent que les nouvelles technologies contribuent à un renforcement de la cybersécurité. Ces statistiques concernant l'IA et les nouvelles technologies sont encore une fois assez partagées et doivent être mises en parallèle avec la question concernant la vision que les personnes interrogées en ont (**question 5**). Pour ce qui est des cybercriminels, la conscience qu'ils sont plus difficiles à traquer par les autorités est globalement admise (à raison). En revanche, la dangerosité de ces derniers, notamment pour les individus, est probablement sous-estimée. Cependant, la manière dont les questions sur les cybercriminels sont formulées doit être prise en compte. En effet, ne pas cocher les cases affirmant que les cybercriminels sont plus dangereux que les criminels dits « classiques » ne signifie pas forcément que les personnes ne s'étant pas alignées avec cette assertion pensent que les criminels dits « classiques » sont plus dangereux. Les sondés peuvent ne pas avoir d'avis sur ces questions ou considérer que les cybercriminels sont tout aussi dangereux que les criminels dits « classiques ».

Bibliographie

Droit européen : droit primaire & dérivé

- Traité sur le fonctionnement de l'Union européenne (TFUE) n° C 326/47, 26 octobre 2012
- Traité sur l'Union européenne (TUE), n°C326/01, 7 février 1992
- Règlement sur la résilience opérationnelle numérique du secteur financier (UE) 2022/2554 du 14 décembre 2022
- Règlement sur l'intelligence artificielle (UE) 2021/0106, 21 avril 2021
- Règlement sur la gouvernance européenne des données, (UE) 2020/340, 25 novembre 2020
- Règlement relatif à l'ENISA (UE) 2019/881, 17 avril 2019
- Règlement général sur la protection des données (UE) 2016/679, 27 avril 2016
- Directive NIS 2 (UE) 2022/2255, 14 décembre 2022
- Directive NIS 1 (UE) 2016/1148, 6 juillet 2016
- Directive Police-Justice (UE) 2016/680 du 27 avril 2016
- Directive DSP 2 (UE) 2015/2366 du 15 novembre 2015

Droit français : lois, ordonnances, décrets & codes

- Loi n°2024-449, 21 mai 2024
- Loi de programmation militaire n°2023-703, 1er août 2023
- Loi pour une République numérique n°2016-1321, 7 octobre 2016
- Loi pour la confiance dans l'économie numérique n°2004-575, 21 juin 2004
- Loi « Godfrain » n°88-19, 5 janvier 1988
- Loi informatique et libertés n°78-17, 6 janvier 1978
- Ordonnance portant transposition de la directive 2015/2366 concernant les services de paiement dans le marché intérieur n°2017-1252, 9 août 2017
- Décret portant création de l'office anti-cybercriminalité n°2023-1083, 23 novembre 2023
- Code pénal

- Code de procédure pénale

- Code de la propriété intellectuelle

- Code civil

Décisions juridictionnelles, actes administratifs & référentiels

- Cass. Com, n°22-11.707, 30 août 2023

- Cass. Ass Plén, n°21-83.146, 7 novembre 2022

- Cass. Crim., n°14-81.336, 20 mai 2015

- CE, Chambres réunies, décision n°434684, 19 juin 2020

- CA Toulouse, 31ème chambre, 21 janvier 1999

- CNIL, « Délibération n° 2024-011 portant adoption d'une recommandation sur l'application du règlement général sur la protection des données au développement des systèmes d'intelligence artificielle », 18 janvier 2024

- CNIL, « Délibération n°2022-100 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017 », 21 juillet 2022

Rapports, études & référentiels

- Rapport, Sénat n°503, concernant la proposition de loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinées au grand public 16 février 2022

- Rapport, Assemblée nationale, « les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale », 11 octobre 2000

- Référentiel d'exigences, ANSSI, « Prestataires de réponse aux incidents de sécurité », 14 février 2023

- Recommandations, ANSSI, « Recommandations relatives à l'authentification multifacteur et aux mots de passe », 8 octobre 2021

  Rapport, CNIL, « Comment permettre à l'Homme de garder la main ? », 15 décembre 2017

- Avis, CNPEN, « Systèmes d'intelligence artificielle générative : enjeux d'éthique » sur les IA génératives, 30 juin 2023

- Rapport, Commission de l'intelligence artificielle, « IA : notre ambition pour la France », 13 mars 2024

- Rapport, Verizon, « Data Breach Investigations 2023 », janvier 2024

- Étude, AMRAE, « Lumière sur la cyberassurance », LUCY, 2024

- Rapport, Group-IB, 2023

Déclarations & communiqués de presse

- DigitalEurope, « *Joint statement: "Let's give AI in Europe a fighting chance"* », 23 novembre 2023

- Rapport, Banque centrale européenne (BCE), « *IT and cybersecurity: no ground for complacency* », 15 novembre 2023

Doctrine juridique

- C. AGHROUM, « La lutte contre la cybercriminalité : la France au cœur du concert européen... », Sécurité Globale, 2008

- B. BADAUD, « Le darknet et le droit », La Semaine juridique. Édition générale, 25 avril 2018

- B. BERTRAND, « La proposition de régulation générale pour l'intelligence artificielle dans l'Union européenne : l'IA Act », Chronique Droit européen du numérique, RTD Eur, 5 octobre 2022

- E. CAPRIOLI, « La proposition de règlement européen sur l'intelligence artificielle se précise », L'Usine Digitale, 6 juillet 2023

- E. CAPRIOLI, « Economie des données et intelligence artificielle : un ensemble contractuel complexe », L'Usine Digitale, 16 novembre 2022

- C. CASTETS-RENARD & B. DABAN, « Proposition de réglementation de l'IA : le Parlement européen renforce la protection des individus », Le club des juristes, 23 juin 2023

- F. CHALTIEL, « L'équilibre entre sécurité et liberté devant le juge constitutionnel », Revue de droit constitutionnel, Actu-Juridique, Lextenso, 11 juillet 2019

- C. COSQUER & J. LANCKRIET, « Les objets connectés et la Défense », Revue Défense Nationale, n°787, 2016

- J. FRANCILLON, « Infractions relevant du droit de l'information et de la communication », Revue de science criminelle et de droit pénal comparé, p. 559-578, 2013

- V. GAUTRAIS, « Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques », Le club des juristes, 23 juin 2023

- H. LAVOIX, « Revisiter l'idée de cybersécurité pour le monde digital du 21e siècle », Sécurité globale, 2019.

- R. LAWLOR, « What Computers Can Do : Analysis and Prediction of Judicial Decisions », American Bar Association Journal, 1963

- J. MARTINON, , « Darknet : éclairage et démystification », « Propos introductifs sur le Darknet », Dalloz IP IT, 22 février 2021

- T. MESZAROS & F. DESPINASSE, « L'innovation de défense pour la gestion des crises : dispositifs Red team et Blue team », Revue Défense Nationale, 2020

- X. PIN, *Droit pénal général*, édition 2024, Lefebvre Dalloz, septembre 2023

- C. PLEDEL, D. GALBOIS-LEHALLE & B. CASSAR, « L'articulation du projet de règlement sur l'intelligence artificielle avec le droit du numérique européen », IP/IT et Communication, 17 juillet 2023

- X. RAUFER, « Évolutions criminologiques », Sécurité Globale, 2022

- J. RIVIERE & D. LUCAS, « Criminalité et Internet, une arnaque à bon marché », Sécurité globale, 2008

- J. SENECHAL, « Les dynamiques actuelles de la future régulation de l'IA, aux niveaux européen et français : entre complexité et angle mort », IP/IT et Communication, 19 octobre 2023

- A. TRICAUD, « Vers une co-souveraineté nationale et européenne en matière de cybersécurité, Revue Défense Nationale 2022

Cours magistaux, enseignements méthodologiques & travaux universitaires

- E. CAPRIOLI & I. CHOUKRI, Cours magistral de sécurité des systèmes d'information, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

- E. CLAUDEL, Cours magistral de droit de la concurrence appliqué aux activités numériques, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

- A. COLETTA, « La prédiction judiciaire par les algorithmes, thèse, sous la direction de G. CERQUEIRA, Université de Nîmes, 27 janvier 2022

- F. COUPEZ, Enseignement méthodologique facultatif d'introduction au fonctionnement des technologies de l'information et de la communication, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

- M. GRIGUER & W. ADDOUN, Cours magistral de droit de la protection des données à caractère personnel, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

- J. JOMBART, « Les violences numériques en droit pénal », thèse, sous la directino de C. ROBACZEWSKI, Université de Lille, 9 décembre 2021

- M-A. LEDIEU, Enseignement méthodologique de sécurité des systèmes d'information, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

- L. MAISNIER-BOCHE & N. BOTCHORICHVILI, Enseignement méthodologie de droit de la protection des données à caractère personnel, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

- S. MILGRAM, « Behavorial Study of Obedience », Université de Yale, 1961

- V. VARET, Cours magistral de contrats électroniques, Master 2 Droit du numérique, Université Paris-Panthéon-Assas, 2023-2024

Articles de presse

- L. BERTUZZI, « Loi sur l'IA : la définition de l'IA et la gouvernance au cœur des débats européens », Euractiv, 8 novembre 2022

- D. FILIPPONE, « Bouygues Construction paralysé par une cyberattaque majeure », Le Monde Informatique, 2020

- A. GAYTE, « Ils hackent des machines à laver et arrivent à lancer des lessives gratuitement », Numerama, 21 mai 2024

- J. LASSERRE-CAPDEVILLE, « Sanction à l'absence de mise en œuvre de l'authentification forte », Le Quotidien, septembre 2023

- J. MARIN, « L'Europe envisage une réglementation à trois niveaux de l'IA générative », L'Usine Digitale, 19 octobre 2023

- Me. O. ORTEGA & Me. B. LOUIS, « Par nature, le droit est en retard sur les innovations technologiques… mais le cas n'est pas désespéré ! », Le Point, 10 juin 2022

- S. REYNOLDS, « La France et d'autres Etats signent un accord sur la sécurité de l'IA », Le Monde Informatique, 28 novembre 2023

- P. ROPERT, « Histoires d'arnaques : du mail du prince nigérian aux « lettres de Jérusalem », France culture, 21 juin 2018

- B. SIMON, « Pirates, Darkweb et cryptomonnaie : la police lance son superservice anti-cybercriminalité », Le Point, 19 janvier 2024

Monographies & œuvres philosophiques

- N. ARPAGIAN, *La cybersécurité*, Presses Universitaires de France, 2022

- J-P. RENNARD, *Darknet : mythes et réalités*, Ellipses, 2018

- R. RIEFFEL, *Révolution numérique, révolution culturelle ?*, Gallimard, 2014

- J-J ROUSSEAU, *Du contrat social*, Collection complète des œuvres, 2012

- S. SINGH, *The Code Book, The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, 1999

- R. STAMBOLIYSKA, *La face cachée d'internet*, Larousse, 2017

- M. WEBER, *Wissenschaft als Beruf* & *Politik als Beruf*, discours prononcés à l'Université de Munich, 1917 et 1919

Podcasts et interviews

- *Affaires sensibles*, avec Jeanne Mayer, France Inter, « Le Darknet », 19 novembre 2021

- *La Cybersécurité expliquée à ma grand-mère*, avec Olivier EZRATTY, « L'ordinateur quantique et la cybersécurité », 4 mars 2024

- *La Cybersécurité expliquée à ma grand-mère*, avec Nicolas RUFF, « L'IA, ChatGPT et la cybersécurité » 12 juin 2023

- *La Cybersécurité expliquée à ma grand-mère*, C'est le jeu ma pauv Lucette », remixé le 26 mars 2023

- *Le Monde de la cyber*, avec Romain Basset, , « Phishing : de quoi parle-t-on ? », 2023

- *Les Temps Electriques*, avec le colonel Jérôme Barlatier, « Cyberarnaques : quand l'internaute mord à l'hameçon », 21 avril 2023

- *Nolimit Sécu*, avec Nicolas RUFF, Vladimir COLAS, & Gérôme BILLOIS, « Intelligence artificielle et cybersécurité », 24 septembre 2023

- *No Log*, avec Barbara LOUIS SIDNEY, « Le renseignement cyber », 11 janvier 2021

- Interview L. LANDES-GRONOWSKI, « Le deepfake porn », France 24, 23 mars 2024

Sites internet

- Site de l'ANSSI : https://cyber.gouv.fr/

- Site BDM : https://www.blogdumoderateur.com/

- Site Coheris, « Qu'est-ce que le *Machine Learning* » : https://ia-data-analytics.fr/machine-learning/usages/

- Site de la Commission européenne : https://commission.europa.eu/index_fr

- Site de la Commission nationale de l'informatique et des libertés (CNIL) : https://www.cnil.fr/fr

- Site Cyber Cercle, « Une matrice pour anticiper et traiter les risques cyber » : https://cybercercle.com/une-matrice-pour-anticiper-et-traiter-les-risques-cyber-une-parole-dexpert-de-gerard-peliks-charge-de-cours-cybersecurite-dans-les-ecoles-dingenieurs-et-institut/

- Site DataScientest : https://datascientest.com/

- Site Futura : https://www.futura-sciences.com/

- Site de Pharos : https://www.internet-signalement.gouv.fr/PharosS1/

- Site Rendre notre monde + sûr : https://rendre-notre-monde-plus-sur.goron.fr/

- Site Varonis, « Chiffrement PGP » : https://www.varonis.com/fr/blog/pgp-encryption#:~:text=Le%20chiffrement%20PGP%20peut%20%C3%AAtre,personnes%20avec%20lesquelles%20vous%20communiquez.

- Site YesWeHack : https://www.yeswehack.com/fr

Œuvres cinématographiques

- J. CAMERON, *Terminator*, Gale Anne Hurd, 1985

- B. CONDON, *The Fifth Estate*, DreamWorks SKG Participant Media, 2013

- B. DE PALMA, *Mission impossible*, Paramount Pictures, Cruise/Wagner Productions, 1996

- S. JONZE, *Her*, Annapurna Pictures, 2014

- A. PROYAS, *I, Robot*, Davis Entertainment; Laurence Mark Productions; Overbrook Entertainment; Canlaws Productions; Mediastream IV, 2004

- T. RUSSELL, *Silk Road*, Perfect Season Productions, High Frequency Entertainment, Mutressa Movies, Piccadilly Pictures, 2021

- S. SPIELBERG, *Minority Report*, Amblin Entertainment, 20th Century Studios, DreamWorks SKG, Cruise / Wagner Productions, 2002

- O. STONE, *Snowden*, Endgame Entertainment; KrautPack Entertainment; Wild Bunch; Onda Entertainment; Vendian Entertainment, 2016