MARS 2021

RAPPORT

LE DROIT PÉNAL À L'ÉPREUVE DES CYBERATTAQUES

Groupe de travail présidé par Bernard Spitz,
président du pôle International et Europe du MEDEF,
ancien président de la Fédération française de l'assurance (FFA)

Rapporteur : Valérie Lafarge-Sarkozy, avocate associée, cabinet Altana

le club des juristes

COMMISSION AD HOC

LE DROIT PÉNAL À L'ÉPREUVE DES CYBERATTAQUES

RAPPORT DU CLUB DES JURISTES

Commission ad hoc
MARS 2021

4, rue de la Planche 75007 Paris
Tél. : 01 53 63 40 04
www.leclubdesjuristes.com

RETROUVEZ-NOUS SUR

PRÉFACE

À l'ombre de la crise sanitaire qui tient la planète sous son joug depuis 2020, les épisodes de cyberattaques se sont multipliés. Qu'on se garde d'y voir une simple coïncidence, la conjonction inopinée de calamités qui, au fil d'une série noire, se déchaîneraient sans rapport les uns avec les autres. Au contraire, les perturbations ou acclimatations majeures engendrées dans nos sociétés par la pandémie du Covid-19 ont été propices à la recrudescence d'infractions qui, pour être diversement ancrées dans le numérique, sont autant de symptômes des vulnérabilités contemporaines. La vulnérabilité de certaines personnes aura été le terreau psychologique d'infractions commises *via* le numérique pendant la crise sanitaire. En août 2020, le secrétaire général d'Interpol alertait sur l'augmentation des cyberattaques qui s'était produite quelques mois auparavant, des attaques *« exploitant la peur et l'incertitude causées par la situation économique et sociale instable du fait du Covid-19* ». Anxieuses face à la maladie, fragilisées par la solitude, des personnes que leur désarroi rend vulnérables – la victime d'une particulière vulnérabilité, figure récurrente du droit pénal contemporain – sont les victimes toutes désignées de ceux qui excellent à tirer profit de la crédulité d'autrui. Lors du confinement du printemps 2020, une centaine d'escroqueries répertoriées en France furent commises en ligne par des individus qui se faisaient passer pour des dirigeants d'entreprises écoulant des stocks de masques. Le numérique se contente alors de parer d'atours contemporains des agissements aussi classiques que ceux constitutifs d'escroqueries. La vulnérabilité des systèmes d'information, elle, est fille du numérique. Les confinements successifs, en favorisant le télétravail, la télémédecine, le commerce à distance, jusqu'aux actes devenus les plus banals de la vie quotidienne, tel le paiement sans contact, ont contribué à démultiplier les circonstances pouvant donner prise à la commission d'attaques informatiques. La défense, ici comme ailleurs, repose sur l'impossibilité d'accès. Las ! Mots de passe piratés, failles de vulnérabilité non corrigées, simples défaillances humaines (tel le téléchargement par inadvertance d'un cheval de Troie) ouvrent littéralement la porte des systèmes informatiques.

Et si tout cela révélait une vulnérabilité structurelle, celle de nos sociétés ? Pieds et mains liés au numérique, les sociétés contemporaines y puisent ce qui les rend aussi performantes que fragiles, dans un témoignage édifiant de l'ambivalence du numérique. De fait, la pandémie de Covid-19 n'a fait qu'exacerber des tendances existantes. Depuis longtemps déjà, les risques liés aux cyberattaques sont bien identifiés, quand ils ne sont pas déjà en train de se réaliser. La dimension immatérielle de la commission des cyberattaques n'exclut

pas, faut-il le rappeler, que celles-ci puissent causer, directement ou non, une atteinte à l'intégrité physique, voire à la vie d'une personne. En 2019, le Département de la Sécurité intérieure des États-Unis alertait sur les vulnérabilités du système de communication radio de certains défibrillateurs cardiaques : l'exploitation de ces vulnérabilités par des personnes malintentionnées pourrait leur permettre de causer la mort du patient. En Allemagne, une femme, en urgence vitale, n'a pas pu être opérée dans un hôpital parce que celui-ci était visé par un rançongiciel perturbant une trentaine de ses serveurs : la femme est morte durant son transfert dans un autre hôpital, prise en charge trop tard. À plus grande échelle, le croisement des cyberattaques et du terrorisme représente « la » menace du XXIe siècle. Dans une configuration jouant sur les deux tableaux, des actes de terrorisme « conventionnels », tels les assassinats commis au Bataclan, pourraient être épaulés par des attaques informatiques, visant par exemple les systèmes des feux de la circulation : à la clé, une désorganisation totale de la circulation entravant l'arrivée des secours et des forces de l'ordre. Un pas de plus dans la dématérialisation et, à l'image de ce que nous montre déjà la cyberguerre (on songe au piratage du programme nucléaire iranien par le virus Stuxnet, attribué à la NSA, en tout cas considéré comme la première cyberarme), le spectre de cyberattaques visant les OIV, opérateurs d'importance vitale, s'impose à l'esprit. Mais d'ores et déjà, le lien est bien établi, sur un autre plan, entre terrorisme et cyberattaques. La manne financière qui résulte de celles-ci, *via* les rançons ou la vente de données, contribue à alimenter les circuits de financement du terrorisme.

Les particuliers, mais aussi et surtout les entreprises, paient le prix fort de ces attaques. Cibles privilégiées des cyberattaques, les entreprises, quelle que soit leur taille, doivent s'y préparer et savoir comment réagir quand l'attaque survient. Une approche globale de ce phénomène a été proposée au Club des juristes par Valérie Lafarge-Sarkozy, avocat et expert du Club. Une commission a été mise en place sous la présidence de Bernard Spitz, la Commission *ad hoc Cyber Risk*, qui réunit des experts venant de domaines très différents, mais dont les centres d'intérêt convergent vers le numérique. D'emblée placée sous l'angle du risque, la réflexion collective a débouché, à l'issue d'un travail mené par une sous-commission chargée de réfléchir aux enjeux assurantiels des cyberattaques, sur un premier rapport, « Assurer le risque Cyber », publié par le Club des juristes en janvier 2018. Dans le prolongement de cette réflexion, une autre sous-commission fut dédiée au volet répressif. Elle livre, à l'issue de ses travaux, ce rapport sur « Le droit pénal à l'épreuve des cyberattaques ». Les rédactrices de ce rapport y ont apporté toute leur expérience de professionnelles qui sont au plus près des cyberattaques. Valérie Lafarge-Sarkozy et Laetitia Dage, avocates, Myriam Quéméner, avocat général près la cour d'appel de Paris et Anne Souvira, commissaire divisionnaire, chargée de mission aux questions relatives à la cybercriminalité au sein du cabinet du préfet de police de Paris, ont mis en commun leurs compétences et expériences pour élaborer ce rapport, dont l'auteur de ces lignes a eu le privilège de suivre la genèse et, aujourd'hui, le plaisir d'écrire la préface.

Dans ses deux premières parties, le rapport est articulé entre droit pénal de fond et procédure pénale. Sous l'angle du premier, le lecteur trouvera une présentation pédagogique des infractions. Le rapport, sondant les ressources des incriminations classiques – en tout cas d'application générale –, rappelle que peuvent être mobilisées des incriminations classées aussi bien dans les infractions contre les biens – le vol, l'escroquerie – que dans les infractions contre la personne, telle l'usurpation d'identité. Par ailleurs la part belle est faite, bien entendu, aux incriminations plus spécifiques que sont les atteintes aux systèmes de traitement automatisé de données (STAD), associées à certaines infractions afférentes plus particulièrement aux traitements de données à caractère personnel. S'esquisse ainsi une éventuelle inversion des perspectives, puisque l'entreprise victime d'une cyberattaque visant ses STAD pourrait bien, elle-même, être responsable d'une insuffisante protection de ceux-ci. Il faut donc discerner, dans cette évocation des infractions, un appel à la prudence, qu'expriment d'ailleurs explicitement les développements consacrés à la mise en place de règles préventives de cybergouvernance dans les entreprises. Mais quand le mal est fait, place à la réponse judiciaire. La seconde partie lui consacre des développements fort riches, à la tonalité très pratique, qui constitueront un guide bien utile aux victimes de cyberattaques. Les deux premières parties du rapport sont émaillées de divers focus et conseils, mais aussi d'interviews de spécialistes, qui donnent à l'ensemble une tournure résolument concrète et opérationnelle. Mais le rapport n'en reste pas là. Une troisième partie lui offre, en guise de conclusion, « 10 préconisations pour faire avancer la lutte contre la cybercriminalité ». On ne peut que souhaiter que ces préconisations soient entendues par les institutions diverses à l'adresse desquelles elles sont formulées. Osera-t-on en formuler une 11e, une recommandation qui n'est d'ailleurs que la traduction de ce qui court en filigrane dans l'ensemble de ce rapport, à savoir que le numérique ne fait pas oublier le bon sens élémentaire : prudence reste mère de sûreté, même dans le numérique, surtout dans le numérique.

Agathe Lepage
Professeur à l'Université Panthéon-Assas (Paris II)

TABLE DES MATIÈRES

PRÉFACE 3

INTRODUCTION 8

PREMIÈRE PARTIE

TRAITEMENT JURIDIQUE DES CYBERATTAQUES ET CONSÉQUENCES ÉCONOMIQUES ET SOCIALES 19

CHAPITRE I. :
Les infractions visant les systèmes de traitement automatisés de données (STAD) 20

SECTION I Définition des STAD et des traitements de données 20

SECTION II Le cas particulier des objets connectés 21

SECTION III Les différentes atteintes aux STAD et leur répression 22

SECTION IV Les conséquences pour les entreprises des atteintes à leurs STAD 26

IV-1. Le « vol » des données personnelles, des secrets industriels et commerciaux 26

IV-2. Les conséquences financières et d'image 27

IV-3. Le risque de sanctions en cas de défaut de sécurisation des STAD 29

SECTION V L'indispensable mise en place de règles préventives de cybergouvernance dans le cadre du dispositif de gestion globale des risques des entreprises 35

CHAPITRE II. :
Les infractions classiques dans le cyberespace 40

SECTION I Les atteintes aux biens 40

SECTION II L'usurpation d'identité portant atteinte à la réputation de l'entreprise 43

DEUXIÈME PARTIE :

CYBERATTAQUE : QUELLE RÉPONSE JUDICIAIRE ? 47

CHAPITRE I. :
Les acteurs et leur cadre institutionnel 48

SECTION I Le système français 48

I-1. La spécialisation des services d'enquête 48

I-2. La spécialisation des magistrats 54

I-3. Le rôle de l'agence nationale de la sécurité des systèmes d'information et des autorités administratives indépendantes 59

SECTION II La coopération policière et judiciaire internationale 59

II-1. Les acteurs au niveau européen et international 59

II-2. Les textes actuellement en discussion 61

II-3. Le 2e protocole de la convention de Budapest 61

CHAPITRE II :
La mise en œuvre de l'action publique et les moyens de preuve 63

SECTION I La plainte 63

I-1. Le dépôt de plainte 63

I-2. Le traitement de la plainte 66

I-3. L'enquête 66

I-4. Les suites judiciaires possibles de l'enquête 67

SECTION II La preuve et ses limites 70

II-1. Les procédures d'accès à la preuve numérique 70

II-2. La conservation des données par les opérateurs 73

II-3. Les moyens d'accès aux données chiffrées 74

TROISIÈME PARTIE

10 PRÉCONISATIONS POUR FAIRE AVANCER LA LUTTE CONTRE LA CYBERCRIMINALITÉ 76

COMPOSITION DE LA COMMISSION 84

INTRODUCTION

1. Si **le cyberespace** est porteur de croissance et d'innovation, il est aussi en proie à l'exploitation malveillante de ses failles et vulnérabilités. C'est l'ambivalence du numérique : à la fois levier économique, source de valeur et de préservation d'une activité économique, comme nous l'avons connu dernièrement avec la première crise sanitaire de mars **2020**, et source de cyberdélinquance comme l'a révélé la même crise sanitaire, avec une augmentation considérable des attaques, le travail à distance étant devenu la source de **20 %** des incidents de cybercriminalité.

En France, en **2018**, **80 %** des entreprises ont constaté un incident de cybercriminalité[1]. En **2019**, ce taux est passé à **90 %**, **43 %** étant des PME et en **2020** ce taux a été multiplié par 4, nécessitant que le président Macron présente, le **jeudi 18 février 2021**, sa stratégie de cyberdéfense visant à répondre à la croissance exponentielle des menaces et attaques.

2. Nombre de rapports internationaux mesurent les coûts directs et indirects des attaques numériques. Ainsi, en **2017**, le coût global a été de **600 milliards de dollars**. En **2018**, le coût moyen par entreprise a été de **8,6 millions d'euros**[2] pour les entreprises françaises et de **27,4 millions de dollars** en moyenne pour les entreprises américaines.

L'année **2019**, quant à elle, a confirmé la montée en puissance des attaques indirectes exploitant les relations entre partenaires. En effet, compte tenu du niveau de maturité actuel des cibles finales, les cybercriminels les contournent en attaquant un partenaire/fournisseur de services numériques, d'accès internet, de sociétés d'infogérance, etc. La portée de l'attaque en est démultipliée et dans les prévisions **à 5 ans**, **23 %**[3] du coût des attaques pourrait résulter de ces agressions ciblant les systèmes d'information des tierces parties, afin d'atteindre la cible réelle.

Quant à l'année **2020**, elle sera, sur la base du premier semestre, une année record en France, avec par exemple une augmentation de **667 %** des attaques par *phishing* enregistrées entre le 1er et le 23 mars[4]. Selon un rapport de VMware Carbon Black[5], entre février et mars 2020, les attaques de *ransomwares* ont augmenté de **148 %** dans le monde, avec une attaque toutes les 14 secondes.

3. Au niveau mondial, la cybercriminalité devrait coûter aux entreprises **6 000 milliards de dollars** par an à partir de **2021**[6].

4. Le rapport risque/coût/gain de la cybercriminalité est très favorable aux délinquants qui se procurent facilement en ligne et sur le darknet des kits aux alentours de **5 $** qui leur permettent de commettre des dénis de services, et faire usage de la technologie numérique pour industrialiser et globaliser leurs méfaits.

Les changements de méthode de travail et l'augmentation massive du télétravail leur ont donné de nouvelles et nombreuses opportunités. L'application Zoom a ainsi dû freiner au cours du dernier semestre **2020** le développement de ses fonctionnalités pour se concentrer sur celui de sa sécurité, afin de faire face à la hausse significative du nombre de ses utilisateurs quotidiens, passé de **10 millions en décembre 2019 à plus de 200 millions en mars 2020**.

FOCUS

INTERVIEW DE GUILLAUME POUPARD
Directeur général de l'ANSSI
par Brigitte Bouquot, AMRAE et Valérie Lafarge-Sarkozy, ALTANA

1/ La pandémie a renforcé les usages numériques, a-t-elle fait évoluer la menace cyber ?

L'augmentation de la menace cyber est en effet particulièrement inquiétante puisque le nombre d'attaques par rançongiciel traitées par l'ANSSI a été multiplié par 4 entre 2019 et 2020, passant de 54 à 192.
Depuis le début de l'année 2021, cette courbe n'a pas fléchi et nous apportons sans cesse une assistance à près d'une quarantaine de victimes simultanées. Des victimes d'importance en termes de sécurité nationale, économique ou sanitaire…

Certes, la situation sanitaire est un facteur de légère aggravation de la menace cyber, en ce sens qu'elle complique la vie des défenseurs, mais pas forcément celle des attaquants. Mais force est de constater que la croissance rapide de la menace cyber précède la crise sanitaire et que la tendance de fond est extrêmement négative. Quand la crise sanitaire s'arrêtera, la crise cyber perdurera. Il est indispensable de

1. Rapport du Ministère de l'Intérieur « État de la menace numérique »
2. https://www.accenture.com/fr-fr/insights/security/etude-cout-du-cybercrime
3. https://www.accenture.com/fr-fr/insights/security/etude-cout-du-cybercrime
4. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/
5. https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/
6. Rapport annuel de Cybersecurity Ventures et de Herjavec Group, 2019, https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

décorréler les deux sujets et traiter le sujet cyber qui nous préoccupera durablement.

2/ Pourriez-vous commenter les annonces du président Macron relatives à la stratégie nationale de cybersécurité ?
La stratégie annoncée par le président de la République comprend deux volets. Un volet conjoncturel lié aux cyberattaques qui ont frappé deux établissements de santé, coup sur coup, en février, et un volet économique fondé par la volonté de la France de développer considérablement l'écosystème industriel de la cybersécurité. Cela traduit à la fois une inquiétude forte pour notre société menacée par les cyberattaques, mais également la nécessité de mettre en valeur notre base industrielle, pour faire à face à l'augmentation de la menace et pour affirmer sa position d'acteur majeur de la cybersécurité sur la scène internationale. Nous avons effectivement beaucoup d'acteurs performants en France qui investissent massivement dans le cyber et qui sont capables d'apporter des solutions de confiance aux acteurs français, européens et internationaux. À l'échelle internationale, les solutions françaises sont particulièrement appréciées, car elles sont souvent gages de confiance. Cela représente de vraies opportunités économiques pour les entreprises françaises.

Ce milliard d'euros se décompose en plusieurs axes de financement majeurs : le financement de la recherche, le plan d'investissement d'avenir (PIA4) et France Relance, qui comprend une enveloppe de 136 millions d'euros pour renforcer le niveau de cybersécurité des acteurs publics de manière durable (hôpitaux, collectivités territoriales, administrations centrales).

Le Campus cyber annoncé, très symboliquement par le Président Emmanuel Macron, bénéficiera également de ce financement. Véritable ambition française portée au plus haut niveau politique, ce campus fédérera des grands groupes, des PME, des startups, des chercheurs, des administrations autour de projets de cybersécurité. C'est très hétéroclite en apparence, mais en réalité c'est une véritable équipe de France. Le lancement d'un tel Campus est une étape majeure dans notre stratégie cyber qui comprend une forte dimension européenne, avec en point d'orgue la présidence française du Conseil de l'Union européenne en début 2022.

3/ En quoi le développement d'un volet pénal spécifique peut-il conforter la politique de sécurité numérique menée par l'ANSSI ?
En notre qualité d'autorité nationale, nous coopérons au quotidien avec les services d'enquêtes et de renseignement. Nous avons développé une collaboration étroite avec les services de renseignement et avec les services d'enquête (le C3N, l'OCLCTIC, la BL2C, la DGSI) et le parquet spécialisé cyber (J3). Il y a aujourd'hui une véritable convergence de vues sur les sujets cyber au sein de l'État. L'ANSSI travaille très efficacement avec tous ces services pour partager ses connaissances et ses méthodes. À l'avenir, il serait bénéfique d'approfondir davantage le partage d'informations entre les services de renseignement et d'enquête, le partage d'informations techniques étant indispensable à la lutte contre la menace cyber.

La coopération judiciaire internationale fonctionne de mieux en mieux pour lutter contre la cybercriminalité. Récemment, nous avons ainsi eu de beaux succès avec, par exemple, le démantèlement des réseaux Emotet et Egregor.

Ces exemples font changer la peur de camp et délivrent un message positif. La coopération judiciaire internationale se développe très nettement en Europe, mais également avec nos alliés occidentaux et même au-delà. Nous avons tous intérêt à réduire le nombre de lieux où peuvent agir et se cacher les cybercriminels.

4/ Quels sont vos conseils aux dirigeants pour la sécurité numérique ?
Il faut intégrer le risque numérique dans la gestion globale des risques de chaque entreprise. Les dirigeants doivent utiliser le levier réglementaire et investir 5 à 10 % de leur budget IT dans la cybersécurité pour se doter de solutions efficientes. Notre écosystème de prestataires de confiance, dont nombre détiennent un Visa de sécurité ANSSI, est capable d'accompagner et de conseiller efficacement les entreprises. Une meilleure protection de nos entreprises permettra de limiter les cas graves d'attaques, d'élever le niveau de cybersécurité et de gérer le risque résiduel de façon efficace, notamment en développant les mécanismes assurantiels. Il est essentiel que chaque entreprise utilise les leviers dont elle dispose pour se sécuriser et soit responsable en la matière pour chacun puisse continuer à tirer pleinement parti des opportunités du numérique.

■ **5.** Dans ce contexte, il est apparu nécessaire, pour une bonne compréhension de cet ouvrage et des enjeux de la cybersécurité pour les entreprises, de définir en préambule les notions de cyberespace (i), cybercriminalité(ii), cybersécurité (iii) et cyberdéfense (iv) :

(i) **Le cyberespace** est un univers de communication et de partage composé d'infrastructures, de réseaux et de systèmes d'information (SI), ainsi que de communications électroniques, qui sont interconnectés au monde entier, même spatial. Il s'agit donc d'un espace immatériel qui n'a pas de frontière, ce qui nourrit des débats autour de la coopération des États (par exemple, dans la recherche de la preuve numérique), lesquels brandissent leur souveraineté en compliquant les réponses à imaginer aux niveaux national et international, l'ANSSI veillant au respect de l'autonomie stratégique européenne de sécurité du numérique[7].

7. Cf. www.ssi.gouv.fr

(ii) **La cybercriminalité** a été définie, par le groupe de travail interministériel présidé par le procureur général Marc Robert[8], comme les faits constituant des infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication et des données qu'il recèle.

(iii) **La cybersécurité** peut, elle, se définir comme l'état recherché pour permettre à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

À cette fin, le double objectif de la cybersécurité est, d'une part, la formation et la sensibilisation de tous les acteurs (entreprises, collectivités, particuliers) aux risques cyber et aux bonnes pratiques, ainsi qu'à l'hygiène informatique à mettre en œuvre au quotidien pour réduire le coût des cyberattaques et, d'autre part, l'acquisition de solutions techniques pour protéger les données et les SI.

Pour les entreprises, la cybersécurité est une affaire de gouvernance transversale, confiée à plusieurs acteurs tels que les DSI, les RSSI, les DPO ou le COMEX, sous le contrôle des dirigeants qui doivent déterminer le risque acceptable compte tenu des enjeux pour l'entreprise et des arbitrages financiers.

Consciente de ces difficultés, l'ANSSI a créé les « Visas de sécurité », qui visent à certifier et qualifier des produits ou services de solution de sécurité dont la fiabilité est reconnue à l'issue d'une évaluation par des laboratoires agréés.

(iv) Ainsi, la cybersécurité, comme la lutte contre **la cybercriminalité**, concourt à la cyberdéfense, puisqu'elles luttent pour prévenir utilement les attaques en tentant d'identifier les auteurs et de les interpeller.

La cyberdéfense est un *« ensemble de mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels. »* Depuis la création de l'ANSSI en **2009**, la loi n° 2013-1168 du **18 décembre 2013** relative à la programmation militaire pour les années **2014 à 2019** est venue préciser le cadre juridique de notre cyberdéfense qui est organisée en 4 volets : protection, action militaire, renseignement et investigation judiciaire.

8. Rapport sur la Cybercriminalité de février 2014 en ligne
http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite_annexes.pdf

■ **6.** **Ce cadre de contexte et de définitions étant posé, il y a lieu de s'intéresser aux conditions dans lesquelles notre droit pénal s'est adapté afin de répondre aux cyberattaques protéiformes.**

En France, la cybercriminalité est appréhendée juridiquement depuis la loi relative à l'informatique, aux fichiers et aux libertés du **6 janvier 1978**, puis par la visionnaire loi Godfrain 88-19 du **5 janvier 1988** relative à la fraude informatique, qui a introduit les articles **323-1 et suivants dans le Code pénal** afin de réprimer toutes les atteintes aux systèmes de traitement automatisé de données (STAD), tels que les piratages et les entraves par déni de service distribué (DDOS), ainsi qu'aujourd'hui, les *ransomwares* chiffreurs de données.

Il faut également citer la loi pour la confiance dans l'économie numérique (LCEN) du **21 juin 2004** avec son **article 6** relatif aux fournisseurs d'accès internet, aux hébergeurs et éditeurs de contenus manifestement illicites. La LCEN a également introduit un nouvel article dans le Code pénal **(323-3-1)**, visant directement la détention et la mise à disposition d'équipements conçus pour commettre les faits d'intrusion dans un système ou d'entrave au fonctionnement de ce système.

La loi du **30 septembre 1986** dite « CANAL+ » pour la captation de programmes audiovisuels, le **Code de la propriété intellectuelle (articles L. 335-1 et suivants)**, et le Code monétaire et financier **(article L. 163-4-1 du Code monétaire et financier)** prévoient de nombreuses incriminations ; par exemple, les fraudes et la contrefaçon érigeant, pour certaines d'entre elles, le recours à un réseau de télécommunication en circonstance aggravante (articles L. 521-10, L. 615-14, L. 623-32, L. 716-9 du Code de propriété intellectuelle).

La loi Lemaire n° **2016-1321** du **7 octobre 2016** pour une République numérique a également sa dimension pénale et, dernièrement, la loi du **23 mars 2019** de programmation **2018-2022** et de réforme pour la Justice (LPJ) prévoit l'extension de recours à l'enquête sous pseudonyme et l'harmonisation des techniques spéciales d'enquête qui sont adaptées en matière de lutte contre la cybercriminalité.

Le législateur adapte donc en permanence l'arsenal pénal au regard de l'évolution constante et rapide des cybermenaces.

■ **7.** Un rapport IOCTA de **2018** d'Europol[9] décrit ainsi **sept types de cybermenaces** particulièrement prégnants dont peuvent être victimes les entreprises, auxquels il convient d'ajouter la délinquance classique :

9. (IOCTA), https://www.europol.europa.eu

(i) Les *ransomwares* (rançongiciels) qui chiffrent les données tant sur les postes de travail que sur les serveurs en réclamant un paiement, notamment en cryptomonnaie telle que les bitcoins ou Ethereums, en échange de la clé de déchiffrement censée permettre de les mettre au clair. Si on estime à **80 %** les données récupérées, elles ne sont pas toujours réutilisables, car elles sont souvent rendues dans le désordre et/ou encore chiffrées.

En **2019, 2020 et 2021**, les attaques par rançongiciels[10] ont constitué la menace informatique la plus préoccupante, elles ont ciblé des entreprises et organisations publiques, ainsi que des systèmes d'information critiques tels que ceux de la santé et ont souvent donné lieu, en plus du chiffrement, à des vols de données.

Une grande attaque restera dans les mémoires : le rançongiciel chiffreur de données autorépliquant **WannaCrypt** qui, en **juin 2017**, a infecté des milliers d'ordinateurs dans le monde (**300 000** victimes dans **150** pays) et aurait été facilité par une faille de sécurité non corrigée par les mises à jour[11] pourtant disponibles.

Plus récemment, en **mai 2019**, des hackers ont pris en otage le système informatique de la ville de Baltimore. Ils ont bloqué **10 000** ordinateurs de la ville avec un *ransomware*, ils ont exigé une rançon de **100 000 dollars (89 410 euros)** en bitcoins pour débloquer l'intégralité des fichiers concernés, ou alors une rançon moins élevée par fichier[12]. En **2020**, l'attaque par le rançongiciel Maze qui a sévi dans le monde et a frappé aussi bien Bouygues construction en France, Southwine, Pitneybowes ou Cognizant aux USA, qu'Asco en Belgique, doit être mentionnée, notamment parce qu'elle a nécessité que l'ANSSI et ses partenaires internationaux reconsidèrent les frontières jusqu'alors délimitées entre cybercriminalité et sécurité nationale[13]. À l'**automne 2020**, c'est le rançongiciel Egregor qui a sévi dans les mêmes conditions.

Les services du renseignement étranger de la Corée du Nord, de la Chine et de la Russie ont été identifiés comme des attaquants et leurs avoirs gelés par un arrêté du ministre de l'Économie, des Finances et de la Relance, du **30 juillet 2020**[14].

Dans la nuit du **15 au 18 janvier 2021**, le maire d'Angers et la communauté urbaine Angers Loire Métropole ont été victimes d'un

10. https://www.zdnet.fr/actualites/ransomware-des-operateurs-d-egregor-interpelles-en-ukraine-39917907.htm
11. https://tribune.com.pk/story/1423609/shadow-brokers-threaten-release-windows-10-hacking-tools
12. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html
13. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/ ; https://www.lefigaro.fr/secteur/high-tech/qu-est-ce-que-maze-ce-rancongiciel-qui-seme-la-terreur-dans-les-entreprises-20200206
14. JORF n° 0188 du 1er août 2020

ransomware qui a bloqué tout leur système d'information. Un mois plus tard, la situation n'était toujours pas revenue à la normale.

C'est une véritable déferlante qui, en **2020** et début **2021**, a frappé les villes françaises (La Rochelle, Aix, Marseille, Vincennes, par exemple), mais également les hôpitaux : **27** cyberattaques majeures ont ainsi visé les hôpitaux français.

(ii) **Les attaques en déni de service** ou DDoS, qui saturent de trafic un réseau ou un service en ligne, rendant celui-ci indisponible (le site tombe).

À titre d'exemple, en **juin 2019**, au cours des manifestations qui secouent alors Hong Kong, le service de messagerie cryptée Telegram a été victime d'une attaque par déni de service qui a empêché son utilisation par les manifestants pour se donner rendez-vous anonymement. Il s'est révélé que l'attaque provenait d'adresses IP localisées en Chine[15].

En **septembre** de la même année, c'est l'encyclopédie en ligne Wikipédia qui est touchée par une attaque massive en Europe, en Afrique et au Moyen-Orient, avant de s'étendre partiellement aux États-Unis et à l'Asie. Cette attaque a altéré le bon fonctionnement du service pendant au moins **neuf heures**[16].

En **octobre 2020**, c'est Google qui a été visée par la plus importante attaque DDoS, jamais enregistrée, de 2,54 Tb/s.

(iii) Les attaques par ***cryptojacking*** permettent l'utilisation clandestine d'un ordinateur préalablement infecté par un virus, afin d'y installer un logiciel créateur (mineur) de cryptomonnaie.

Le *cryptojacking* utilise la puissance de calcul ou la bande passante d'un ordinateur ou d'un périphérique pour créer et extraire des devises à l'insu de l'utilisateur qui ne fait pas correctement les mises à jour antivirales. Les cas de *cryptojacking* sont peu signalés, car les victimes ne remarquent pas souvent l'attaque qui cause un simple ralentissement de leur machine, et sont rarement suffisamment lésées pour déposer plainte.

(iv) **La fraude au faux support informatique**, en se faisant passer par exemple pour un éditeur de logiciel pour un dépannage et une mise à jour, est la deuxième cause de perte financière aux USA (au

15. https://www.pcmag.com/news/chinese-ddos-attack-hits-telegram-during-hong-kong-protests
16. https://nakedsecurity.sophos.com/2019/09/11/wikipedia-fights-off-huge-ddos-attack/

titre d'attaques cyber), selon un rapport du FBI du **11 février 2020** qui détaille les attaques et leur coût[17].

(v) Le ***phishing*, ou hameçonnage** qui permet, notamment *via* des virus dotés de fonctionnalités de « *machine learning* », d'usurper l'identité numérique par un envoi massif de messages piégés.

Des milliers de victimes potentielles sont ainsi ciblées et renvoyées, par exemple, vers des sites corrompus pour leur dérober leur couple « identifiant/mot de passe », ou toutes les autres données personnelles aisément monnayables sur le darknet. Ces données seront ensuite utilisées pour attaquer comptes bancaires ou e-boutiques, etc.

Ainsi, aux États-Unis, en **2015**, des cybercriminels se sont servis d'informations personnelles volées à des citoyens américains pour répondre à des questions de sécurité du site web des impôts (IRS) et ainsi accéder à leur déclaration de revenus, qui comporte leurs adresses[18].

La pandémie de Covid-19 a favorisé le développement du *phishing*. Le télétravail de collaborateurs pas suffisamment méfiants et ne disposant pas des outils de sécurité appropriés étant une porte ouverte aux mails d'hameçonnage (*phishing*).

(vi) **L'espionnage économique**, menace prégnante qui vise à atteindre le patrimoine informationnel d'entreprises. Très discrètes, ces attaques informatiques peuvent n'être détectées que très tardivement, avec des conséquences parfois difficiles à évaluer en termes de pertes économiques.

Ainsi, l'équipementier aéronautique français SAFRAN a été victime d'une cyberattaque orchestrée par les services de renseignement chinois, attaque rendue publique par le ministère de la Justice américain en **octobre 2018**[19].

En **mai 2019**, Europol a annoncé le démantèlement d'un gang de cybercriminels ayant dérobé près de **90 millions d'euros** au préjudice de **41 000 victimes**[20] à l'aide du logiciel espion Goznym, qui enregistrait tout ce que sa victime tapait sur son clavier.

17. https://pdf.ic3.gov/2019_IC3Report.pdf
18. https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html
19. https://www.reuters.com/article/us-usa-china-hacking/u-s-charges-chinese-intelligence-officers-for-jet-engine-data-hack-idUSKCN1N42QG
20. https://www.lemonde.fr/pixels/article/2019/05/16/demantelement-d-un-gang-de-cybercriminels-aux-41-000-victimes_5463030_4408996.html

Cette dernière se faisait dérober ses identifiants bancaires par les pirates qui accédaient à ses comptes, viraient ces fonds vers des comptes qu'ils contrôlaient, puis blanchissaient les sommes obtenues, notamment à travers des portefeuilles en bitcoins.

Le rapport annuel **2019** de l'ANSSI révèle que les opérations d'espionnage se poursuivent avec une tendance à la hausse, la recherche d'informations stratégiques sur les politiques extérieures et de défense, ainsi que l'accès aux secrets industriels et commerciaux ou le vol de données personnelles, mais également l'influence par les *fake news* étant les principaux mobiles[21].

(vii) **Le sabotage**, qui occasionne une panne du système informatique.

L'attaque dont a été victime TV5 monde[22] est un sabotage emblématique de la facilité à commettre des faits de grande ampleur pouvant paralyser totalement l'accès à l'information.

On peut aussi citer la cyberattaque NotPetya, qui a infecté un logiciel de comptabilité utilisé par nombre d'entreprises à travers le monde. Selon ZDnet, l'entreprise française Saint-Gobain estime que la campagne de *ransomware* dont elle a été victime lui a coûté 1 % de ses revenus, soit pas moins de **220 millions d'euros**[23]. Ce sabotage a touché le cœur de fonctionnement des matériels informatiques.

(viii) Il faut aussi citer le **hacking de logiciel**, qui permet d'entrer dans le système d'information de l'entreprise sans être repéré *via* la mise à jour du logiciel qui s'est vu implémenter le *malware* dans son code source.

La cyberattaque Solarwinds, toujours active, en est une illustration majeure : il s'agit d'une des attaques les plus imposantes et sophistiquées à ce jour.

Elle a permis, *via* la mise à jour du logiciel Solarwinds utilisé comme vecteur de diffusion à des « pirates », de pénétrer dans les systèmes d'information de **18 000 000** d'organisations (grandes entreprises, infrastructures et institutions gouvernementales) critiques.

21. Rapport annuel d'activité, ANSSI, 2019, https://www.ssi.gouv.fr/uploads/2020/06/anssi-papiers_numeriques-2020.pdf
22. https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html
23. https://www.zdnet.fr/actualites/notpetya-a-coute-cher-a-saint-gobain-39855594.htm

Ce panorama de cybermenaces à la croissance exponentielle et leurs conséquences économiques et sociales commandent un traitement judiciaire efficace. D'où, notamment, l'importance pour les enquêteurs de disposer des moyens technologiques et humains nécessaires afin de leur permettre d'établir les éléments constitutifs des infractions et d'identifier les cyberdélinquants. Cela nécessite aussi une coopération internationale effective au niveau européen et au-delà. Dans ce contexte menaçant, un besoin impérieux d'intérêt général est de disposer de services réactifs et compétents, capables d'intervenir rapidement auprès des entreprises pour les conseiller au mieux, intégrer les enjeux de l'attaque, sécuriser la situation et mener à bien les enquêtes. À cet égard, l'ANSSI constitue un atout reconnu dans le monde économique, notamment par les entreprises qui ont eu recours à son intervention.

PARTIE I

TRAITEMENT JURIDIQUE DES CYBERATTAQUES ET CONSÉQUENCES ÉCONOMIQUES ET SOCIALES

Si les infractions visant les systèmes de traitement automatisé de données doivent bien sûr être envisagées en premier lieu (Chapitre I), il convient, par ailleurs, de souligner que des infractions plus classiques sont également commises dans le cyberespace (Chapitre II).

CHAPITRE I

LES INFRACTIONS VISANT LES SYSTÈMES DE TRAITEMENT AUTOMATISÉS DE DONNÉES (STAD)

Seront évoqués dans ce chapitre la définition des STAD et du traitement automatisé de données (I), le cas particulier des objets connectés (II), les atteintes aux STAD, leur répression (III) et leurs conséquences pour les entreprises (IV) à qui il est conseillé de définir des règles de cybergouvernance (V).

SECTION I
DÉFINITION DES STAD ET DES TRAITEMENTS DE DONNÉES

■ **8.** Un STAD est un ensemble composé d'unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, devant être protégé par des dispositifs de sécurité.

■ **9.** Ces traitements automatisés de données correspondent à différents procédés de collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement, de données personnelles ou non.

Ces systèmes et données sont protégés par la loi n° 88-19 du 5 janvier 1988 dite loi Godfrain et également, lorsqu'il s'agit de données personnelles, par la loi Informatique et Libertés, ainsi que par le RGPD qui définit les notions de données personnelles, de traitement, de fichier et de responsable de traitement[24].

Concrètement, pour une entreprise, il s'agit de son patrimoine informationnel, de son savoir-faire et des données concernant son personnel, ses clients, ses prospects, ses fournisseurs.

24. RGPD/UE 679/2016

Ces données de l'entreprise constituent un bien à protéger, car ce sont elles qui sont convoitées par les cyberdélinquants.

■ **10.** Presque tout, des appareils électroménagers aux véhicules, en passant par les jouets pour les enfants, est en passe d'être paré de la connectivité réseau et communication.

La particularité de la qualification de STAD, c'est qu'elle est amenée à se développer en permanence puisque les dispositifs qui assurent, en exécution d'un programme, un traitement automatisé de données se multiplient et envahissent le quotidien de l'entreprise, notamment par le biais des objets connectés.

SECTION II
LE CAS PARTICULIER DES OBJETS CONNECTÉS

■ **11.** L'objet connecté peut être défini comme *« un objet physique dans lequel sont intégrés des moyens techniques lui permettant de collecter, stocker, traiter et émettre des données grâce à des technologies sans fil*[25] *»*.

Ces objets intelligents, capables de collecter, d'analyser et de transmettre des informations liées à leur environnement, se sont déployés au sein de l'entreprise par le prisme, notamment, de la domotique et de la téléphonie mobile.

Ainsi, peuvent être qualifiés de STAD, dès lors qu'ils stockent et traitent des données numériques, aussi bien les caméras de vidéosurveillance que les photocopieurs, scanneurs, imprimantes, ou encore le réseau de téléphonie interne.

L'expansion de ces objets connectés multiplie la surface d'exposition des entreprises aux attaques et a donc conduit à une augmentation massive du cybercrime organisé ou « indépendant ».

■ **12.** Ces objets peuvent être classés en trois catégories par nature :

- les objets capteurs-actionneurs qui communiquent des données sur un réseau ;
- les objets capteurs-actionneurs, stockeurs, émetteurs qui communiquent un nombre de données importantes à des logiciels ;
- les objets capteurs-actionneurs, émetteurs, stockeurs qui dialoguent entre eux par des passerelles-relais reliées à plusieurs réseaux.

25. Bernheim-Desvaux S., L'objet connecté sous l'angle du droit des contrats et de la consommation, Contrats, conc., consomm. 2017, étude n° 1)

Aussi, les enjeux de sécurisation des objets connectés libres ou sous licence qui communiquent *via* le wifi, la 5G ou le RFID sont-ils différents et dépendants de l'interconnexion communicante.

■ **13.** Ces objets sont exposés non seulement aux risques généraux du numérique, comme l'accès physique à l'objet et à son port USB, qui permet de le modifier ou d'accéder à sa mémoire. Ils sont également exposés aux risques particuliers du fait de leur nature d'objets connectés à un réseau avec lequel ils communiquent.

L'objet connecté peut donc être attaqué en raison de sa finalité, en raison de l'intérêt de l'information qu'il reçoit ou donne, ainsi que pour l'utilité de sa prise de contrôle.

■ **14.** Les objets connectés sont ainsi particulièrement vulnérables et doivent nécessiter une attention particulière souvent négligée au sein des entreprises.

C'est ce que démontre, notamment, le moteur de recherche intitulé « Shodan », créé par John Matherly, qui répertorie les appareils et les périphériques vulnérables connectés à internet : webcams, installations de traitement de l'eau, alarmes, éoliennes, lecteurs de plaques d'immatriculation, téléviseurs intelligents, installations industrielles sensibles telles que des centrales électriques, raffineries, ou encore des réacteurs…[26]

■ **15.** Les cybercriminels ont ainsi une infinité de possibilités d'infecter les systèmes *via* les objets connectés, comme l'a démontré l'attaque menée contre DYN Managed DNS, aux États-Unis, en **octobre 2016**, au moyen notamment du code source mis à disposition en ligne, ce qui a permis d'infecter **100 000** objets connectés[27]. Ou encore, en **2016**, celle de MIRAI menée à partir de la constitution d'un *botnet* de caméras publiques dont le contrôle avait été pris à distance[28].

SECTION III
LES DIFFÉRENTES ATTEINTES AUX STAD ET LEUR RÉPRESSION

■ **16.** Les atteintes aux STAD d'une entreprise peuvent être multiples, il peut notamment s'agir :

- ▸ d'un sabotage des réseaux et infrastructures par altération, modification, introduction, suppression, extraction de données, entrave, transmission de données indue ;
- ▸ d'un accès à un système d'information pour le dépôt d'un virus et autre logiciel :
  - un virus CryptoLocker qui va chiffrer les données, voire les serveurs, afin de rançonner l'entreprise mal sécurisée ;
  - un logiciel d'espionnage ;
- ▸ d'entraver l'accès aux systèmes de messagerie, de téléphonie, de serveur de partage de données, par spamming ou exploitation d'une vulnérabilité pour déposer un virus chiffreur ;
- ▸ d'intervenir dans les communications entre une ou plusieurs machines pour intercepter des données, des correspondances, ou encore d'envoyer des données en usurpant l'identité du titulaire de la machine.

■ **17.** **Les infractions d'atteintes aux STAD sont prévues aux articles 323-1 et suivants du Code pénal qui répriment :**

- ▸ le fait d'accéder ou de se maintenir frauduleusement dans un STAD ;
- ▸ le fait d'entraver ou de fausser le fonctionnement d'un STAD ;
- ▸ le fait d'introduire frauduleusement des données dans un STAD ;
- ▸ le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée, conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions.

26. https://money.cnn.com/2013/04/08/technology/security/shodan/index.html
27. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
28. https://www.zdnet.com/article/mirai-ddos-botnet-powers-up-infects-sierra-wireless-gateways/

Infraction visée	Peine encourue	Texte d'incrimination
Accès ou maintien frauduleux dans tout ou partie d'un STAD	Deux ans d'emprisonnement et 60 000 € d'amende. Lorsqu'il en est résulté soit la **suppression ou la modification de données contenues** dans un STAD, soit une **altération du fonctionnement** du STAD en question, la peine est portée à **trois ans d'emprisonnement et 100 000 € d'amende, cinq ans et 150 000 € d'amende** sur un STAD à caractère personnel mis en œuvre par l'État et, si en bande organisée, **10 ans et 300 000 € d'amende**.	Article 323-1 du Code pénal
Entraver ou fausser le fonctionnement d'un STAD	Cinq ans d'emprisonnement et 150 000 € d'amende. Lorsque cette infraction a été commise sur un **STAD à caractère personnel mis en œuvre par l'État**, la peine est portée à sept ans d'emprisonnement et 300 000 € d'amende et, si en bande organisée, **10 ans et 300 000 € d'amende**	Article 323-2 du Code pénal

Infraction visée	Peine encourue	Texte d'incrimination
Introduire frauduleusement des données dans un STAD	Cinq ans d'emprisonnement et 150 000 € d'amende Lorsque cette infraction a été commise sur un **STAD à caractère personnel mis en œuvre par l'État**, la peine est portée à sept ans d'emprisonnement et **300 000 € d'amende** et, si en bande organisée, **10 ans et 300 000 € d'amende**.	Article 323-3 du Code pénal
Extraire, détenir, détériorer, reproduire, transmettre, supprimer ou modifier frauduleusement les données que contient un STAD	Cinq ans d'emprisonnement et 150 000 € d'amende. Lorsque cette infraction a été commise sur un **STAD à caractère personnel mis en œuvre par l'État**, la peine est portée à sept ans d'emprisonnement et **300 000 € d'amende** et, si en bande organisée, **10 ans et 300 000 € d'amende**.	Article 323-3 du Code pénal

■ **18.** Ces atteintes aux biens nécessitent la volonté libre et consciente de commettre les faits dont la tentative est punissable (C. pén., art. 323-7), **la personne morale qui aurait bénéficié de la fraude pouvant être déclarée responsable**.

En pratique, l'identification des auteurs de ces infractions s'avère complexe en raison de la dimension internationale de la cybercriminalité et des difficultés inhérentes à l'obtention de la preuve à l'aide de traces et d'indices numériques la plupart du temps situés à l'étranger.

SECTION IV
LES CONSÉQUENCES POUR LES ENTREPRISES DES ATTEINTES À LEURS STAD

Les atteintes aux STAD ont principalement, outre la destruction malveillante, pour objectif l'appropriation frauduleuse de biens immatériels (données personnelles, secrets industriels et commerciaux…) et ont des conséquences financières et d'image majeures pour les entreprises, lesquelles peuvent même faire l'objet de sanctions.

IV-1.
LE « VOL » DES DONNÉES PERSONNELLES, DES SECRETS INDUSTRIELS ET COMMERCIAUX

■ **19.** L'appropriation de ses données est le risque majeur pour une entreprise lors d'une atteinte à son STAD puisqu'elle peut se faire dérober aussi bien ses secrets industriels et commerciaux que les données personnelles de ses clients ou de ses salariés.

L'article 323-3 du Code pénal a été complété en ce sens en **2014**, afin de permettre la répression de la copie des données personnelles lorsqu'elles n'ont pas été supprimées, puisque le fait *« d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données (…) »* contenues dans un STAD est puni de **5 ans** d'emprisonnement et **150 000 €** d'amende.

En **2011**, le PlayStation Network, le service de jeux multijoueur, d'achats de jeux en ligne et de diffusion de contenus en live de la marque japonaise Sony s'est ainsi fait dérober les données personnelles de **77** millions d'utilisateurs, ainsi que les coordonnées bancaires de quelques dizaines de milliers de joueurs[29].

En **2013**, *Vodafone GmbH*, deuxième opérateur mobile allemand, s'est fait pirater les coordonnées personnelles de près de deux millions d'abonnés[30].

En **2014**, l'attaque informatique du site internet d'Orange a également permis de dérober les données personnelles de plusieurs centaines de milliers de comptes clients[31].

En **novembre 2014**, la filiale *Sony Pictures Entertainme*nt a été attaquée par un malware dont l'ampleur des répercussions a conduit au départ du dirigeant de l'entreprise.

29. https://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html
30. https://www.bbc.co.uk/news/technology-24063621
31. https://www.theregister.com/2014/05/08/orange_france_hacked_13_million_seeing_red/

Les hackers (les *Guardians of Peace*) avaient dérobé **100** téraoctets de données comprenant de nombreuses informations confidentielles. Avaient été volés, par exemple, le scénario du James Bond en préparation, les données personnelles de **47 000** employés (noms, adresses, e-mails, numéros de Sécurité sociale, salaires…), ainsi que différents échanges de mails.

En raison du contenu de certains de ses mails (notamment jugé insultant envers le président de l'époque, Barack Obama), la directrice de Sony Pictures Entertainment, Amy Pascal, a quitté ses fonctions et Sony a versé l'équivalent de **8** millions de dollars de dédommagement à ses salariés et ex-salariés à la suite d'une cyberattaque ayant occasionné la divulgation de leurs coordonnées personnelles[32].

Entre **mars et juillet 2019**, la banque américaine Capital One a été victime du vol de données personnelles de **106** millions de clients. Il s'agit de l'un des plus importants piratages informatiques affectant une grande banque américaine, Capital One étant le cinquième émetteur de cartes de crédit bancaires aux États-Unis[33].

IV-2.
LES CONSÉQUENCES FINANCIÈRES ET D'IMAGE

■ **20.** Une entrave aux systèmes de messagerie, de téléphonie, de serveur de partage de données, par spamming ou exploitation d'une vulnérabilité, impacte directement l'activité de l'entreprise qui peut se trouver ralentie, totalement arrêtée ou se poursuivre en mode dégradé.

Dès **2011**, l'attaque subie par la société EDF, dite par « déni de service distribué », dans le cadre d'une offensive d'envergure menée par l'organisation « Anonymous », et apparaissant sous l'intitulé « opération *Greenrights* », a ainsi eu pour conséquence de mettre hors service les sites internet d'EDF à trois reprises, entre **avril et juin**[34].

L'attaque, en **novembre 2016**, visant des services gouvernementaux allemands, qui a touché le réseau téléphonique *Deutsche Telekom* a, quant à elle, entraîné des difficultés à se connecter au réseau pour près de **900 000** personnes[35].

32. https://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed
33. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
34. https://www.lefigaro.fr/flash-actu/2014/11/07/97001-20141107FILWWW00322-juge-pour-avoir-bloque-le-site-d-edf.php
35. https://www.bbc.com/news/technology-38130352

21. La conséquence de cette interruption/ralentissement de l'activité est notamment financière.

Ainsi, selon un rapport établi par IBM, le coût moyen mondial d'une attaque informatique pour une entreprise était estimé à **3,62** millions de dollars en **2017**, **3,86** millions de dollars en **2018** et **3,92** millions en **2019**. Le rapport note, par ailleurs, que le coût pour les entreprises d'une violation de leurs données a augmenté de **12 % sur les cinq dernières années**[36].

Ces chiffres tiennent compte non seulement des coûts liés aux éventuels dommages infligés aux appareils et systèmes touchés par l'attaque, mais également de tous les coûts indirects tels que l'impact sur l'image de l'entreprise, la perte de chiffre d'affaires, ainsi que les frais des éventuelles procédures judiciaires, qu'il s'agisse du montant des dommages et intérêts alloués aux victimes, des amendes, ou des honoraires des conseils. Saint-Gobain a ainsi évalué à **220 M €** le coût de l'attaque subie en **2020**[37]. Le coût de l'attaque *via* un rançongiciel, subie en juin **2019** par le groupe français Eurofins, spécialisé en bio-analyse, a été estimé à **62 M €**[38].

Une cyberattaque peut également induire une perte de confiance des partenaires, actionnaires et clients de l'entreprise, en renvoyant une image de fragilité ou un manque de fiabilité.

La société de traitement de paiements américaine *Heartland Payment Services* en a livré un exemple concret lorsqu'à la suite d'une fuite de données en **2009**, elle a vu sa relation avec l'un de ses principaux clients, Visa, être remise en cause[39].

En **mars 2017**, l'agence américaine d'analyse de crédit Equifax a, à son tour, été victime d'une attaque d'envergure ayant permis aux pirates informatiques de soustraire les données personnelles de plus de **145,5 millions de clients**. L'entreprise, qui a reconnu ne pas avoir agi en conséquence après avoir pourtant décelé une faille, n'a révélé l'attaque à ses clients qu'en **juillet 2017**. En **septembre** de la même année, l'action Equifax avait alors perdu **28 %** de sa valeur à Wall Street[40].

22. Cette atteinte à l'image et à la réputation peut également avoir un impact non négligeable sur les salariés de l'entreprise et la capacité de celle-ci à attirer des talents.

36. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years#assets_all
37. https://www.zdnet.fr/actualites/notpetya-a-coute-cher-a-saint-gobain-39855594.htm
38. https://www.silicon.fr/ransomware-75-millions-e-perdus-pour-eurofins-scientific-335439.html
39. https://www.bankinfosecurity.com/heartland-breach-inside-look-at-plaintiffs-case-a-1844
40. https://www.capital.fr/entreprises-marches/le-pdg-dequifax-demissionne-apres-le-piratage-informatique-1246206

Elle n'est pas non plus exempte de risque de sanction, tant administrative que judiciaire, pour l'entreprise victime de l'attaque dans le cas d'usurpation et/ou divulgation de données personnelles de clients, de fournisseurs ou de salariés.

IV-3. LE RISQUE DE SANCTIONS EN CAS DE DÉFAUT DE SÉCURISATION DES STAD

23. Depuis le **25 mai 2018**, le règlement européen sur la protection des données (RGPD) a introduit de nouvelles règles d'utilisation et de diffusion des données personnelles concernant l'ensemble des personnes physiques et morales ayant vocation à détenir et traiter des données à caractère personnel.

L'article **32** du RGPD et l'article **4 alinéa 6** de la loi informatique et libertés modifiée par la loi d'adaptation au RGPD du **20 juin 2018**, puis par l'ordonnance n° 2018-1125 du 12 décembre 2018, précisent que le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

24. L'imprudence et la négligence des entreprises lors du traitement de données sensibles sont donc désormais directement et lourdement sanctionnées par le RGPD, et ne pas prendre les mesures nécessaires afin de protéger les données personnelles constitue une faute pouvant entraîner la responsabilité de l'entreprise victime d'un incident cyber et de son dirigeant.

Deux sortes de sanctions, administratives et pénales, de natures différentes – donc cumulables – sont prévues si les entreprises violent les dispositions du RGPD et celle de la loi Informatique et Libertés codifiée dans le Code pénal.

(i) Les sanctions administratives

Les violations des dispositions concernant la sécurité des données peuvent être sanctionnées par une amende administrative d'un maximum de **10** millions d'euros ou de **2 %** du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

C'est, dans ce contexte, que les sociétés Dailymotion et Uber ont été sanctionnées par la CNIL, **en juillet et décembre 2018**, pour manquement à la sécurité des données de leurs clients, à des amendes respectives de **50 000 €**[41] et de **400 000 €**[42].

41. https://www.lemonde.fr/pixels/article/2018/08/02/la-cnil-sanctionne-dailymotion-pour-un-piratage-de-comptes-d-utilisateurs-en-2016_5338652_4408996.html
42. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037830841/ ; https://www.lesechos.fr/industrie-services/tourisme-transport/piratage-de-donnees-uber-mis-a-lamende-en-france-par-la-cnil-240511

Étant précisé que le recours à un prestataire pour la gestion des données n'exonère pas la société de son obligation de garantir la sécurité des données traitées pour son compte. C'est ce qu'a retenu la CNIL [dont les décisions peuvent être publiées], le **8 janvier 2018**, en prononçant à l'encontre de la société Darty une sanction de **100 000** euros.

(ii) Les sanctions pénales visées aux articles 226-16 et suivants du Code pénal

Malgré l'amélioration des politiques de sécurité des systèmes et des réseaux d'information, les entreprises sont régulièrement victimes de cyberattaques et de « vols » de données, faute de protection efficace de leurs systèmes.

Le constat d'un tel risque externe à l'entreprise conduit à faire peser, sur les sociétés, une obligation renforcée de protection des systèmes d'information et des données…

Ainsi, en cas de faille de sécurité ayant entraîné la destruction, la perte, la divulgation ou l'accès non autorisé à des données personnelles de clients ou de salariés traitées par l'entreprise, la responsabilité pénale de l'entreprise pourra être engagée.

L'origine de « ces détournements » de données personnelles peut être :

- illicite ou malveillante en cas, notamment, de cyberattaque ou de comportement malintentionné ou ;
- accidentelle : divulgation par erreur, par un salarié, de données, etc.

Ils ont pour dénominateur commun un manque dans la protection des systèmes d'information et des données.

Plusieurs infractions visent à sanctionner ce comportement défaillant d'une entreprise en matière de sécurisation de ses systèmes et de protection des données personnelles traitées. Elles sont prévues aux articles 226-16 et suivants du Code pénal :

- Ainsi, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites aux articles **24, 25, 30, 32** du RGPD ou au 6° de l'article **4** et aux articles 99 **à 101** de la loi Informatique et Libertés peut être sanctionné par une peine allant jusqu'à **cinq ans d'emprisonnement et 300 000 euros d'amende** (article 226-17 du Code pénal).
- Le fait, pour un fournisseur de services de communications électroniques ou pour un responsable de traitement, de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des articles **33 et 34** du RGPD ou des dispositions de l'article **83** et de l'article **102** de la loi informatique et liberté, peut être puni par cinq ans d'emprisonnement et **300 000 euros d'amende** (article **227-17-1** du Code pénal).
- Peut être puni des mêmes peines le fait, pour un sous-traitant, de ne pas notifier cette violation au responsable de traitement, en méconnaissance de l'article 33 du RGPD ou de l'article 102 de la loi informatique et liberté (article **226-17-1** alinéa **2** du Code pénal).

En cas de poursuites pénales pour défaut de protection des systèmes d'information et des données à caractère personnel, la société et son représentant légal pourront être poursuivis cumulativement ou uniquement l'un ou l'autre, selon le choix du procureur de la République.

En tout état de cause, en cas de poursuites dirigées contre le dirigeant de la société, ce dernier pourra s'exonérer de sa responsabilité pénale, en démontrant (si elle existe) la mise en œuvre effective d'une délégation de pouvoirs dans ce domaine précis.

Pour être valable, une délégation de pouvoirs devra réunir trois conditions cumulatives, à savoir que le délégataire devra être compétent, autonome et disposer des moyens nécessaires à l'accomplissement de sa mission.

Le délégataire qui disposerait d'une telle délégation de pouvoirs pourrait ainsi engager, en cas d'infractions pénales prévues aux articles **226-16** et suivants du Code pénal, non seulement sa propre responsabilité pénale, mais également celle de l'entreprise au même titre que le représentant légal.

Toutefois, il est important de rappeler que le principe général d'« accountability[43] » posé par le RGPD tend à **limiter les champs possibles de délégation de pouvoirs pour le dirigeant aux aspects uniquement opérationnels, et non stratégiques, de mise en œuvre des mesures prescrites par le RGPD ou la loi Informatique et Libertés**.

43. Obligation pour toutes les entreprises de mettre en œuvre un ensemble de mécanismes et de procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

FOCUS

PRÉCISIONS SUR LA DÉLÉGATION DE POUVOIRS EN MATIÈRE DE PROTECTION DE DONNÉES PERSONNELLES

Le délégué à la protection des données personnelles (DPO), dont la désignation est prévue par le RGPD, ne peut être responsable en cas de manquement au règlement.

De ce fait, le dispositif de délégation de pouvoir pénal n'est pas admis à l'égard du DPO, notamment parce que la délégation est incompatible avec l'indépendance du délégué et avec le fait que le responsable du traitement des données (qui, lui, peut bénéficier d'une délégation de pouvoirs) doit garantir l'absence d'un conflit d'intérêts avec le DPO (article 38.6 du Règlement).

Cette interdiction se déduit :

- des dispositions de l'article 38.6 du RGPD qui prévoit que les missions et tâches du délégué à la protection des données personnelles ne doivent pas entraîner de conflit d'intérêts ;
- des lignes directrices du G29 qui précisent que le délégué n'est pas responsable en cas de non-respect du règlement, et que **seul le responsable de traitement ou le sous-traitant peut être responsable** ;
- du guide de la CNIL *« Devenir délégué à la protection des données »*.

La CNIL avait déjà considéré, en application des dispositions de l'article 46 du décret d'application de la loi Informatique et Libertés, que l'ancien correspondant informatique et libertés (CIL) ne pouvait pas faire l'objet d'**une délégation pénale qui reviendrait alors à confondre sa fonction avec celle de responsable de traitement.**

Cette solution est, dès lors, transposable au nouveau délégué à la protection des données personnelles.

En cas de poursuites pénales envers la personne morale, c'est le représentant légal de la société ou le responsable du traitement de données, s'il bénéficie d'une délégation de pouvoirs, qui sera poursuivi, et non le DPO.

Pour pouvoir être exonéré de sa responsabilité, le représentant légal de la société devra **justifier de la mise en œuvre effective de cette délégation de pouvoirs au profit du responsable du traitement de données.**

Étant précisé que le principe général d'« *accountability* » posé par le RGPD tend à limiter les champs de délégation du dirigeant aux aspects opérationnels non stratégiques.

Ce qui laisse à penser que l**e DSI pourrait, dans une société, seulement être délégataire quant à la conformité opérationnelle des systèmes** et non s'agissant de la définition des politiques en matière de données personnelles.

En tout état de cause, en cas de délégation valable, le représentant légal pourra s'exonérer de sa responsabilité dans le domaine couvert par la délégation, sauf s'il a personnellement pris part à l'infraction.

(iii) Le cumul des sanctions

Rappelons, enfin, qu'un cumul est possible entre les sanctions administratives prononcées par la CNIL et les sanctions pénales, celles-ci étant de natures différentes.

En revanche, en vertu du principe de proportionnalité, en cas de cumul de ces sanctions, le montant global des sanctions prononcées ne pourra pas dépasser le montant le plus élevé de l'une des deux amendes encourues qui sont déjà très élevées.

(iv) Exemples de condamnations prononcées à l'encontre d'entreprises pour défaut de sécurité de leur STAD

• Sanctions prononcées en France

FOCUS

SANCTIONS PRONONCÉES PAR LA CNIL

À la suite d'un incident de sécurité survenu sur le site internet de l'association Alliance française Paris Île-de-France, les données des personnes inscrites aux cours sont devenues accessibles.

La CNIL a constaté que les mesures élémentaires de sécurité n'avaient pas été prises s'agissant de la procédure d'identification des utilisateurs du site internet et de prévisibilité des URL et a prononcé, le **6 septembre 2018**, une sanction de **30 000 euros**[44].

La société Dailymotion a également fait l'objet d'une sanction de la CNIL pour insuffisance de sécurisation des données des utilisateurs de sa plateforme d'hébergement de contenus vidéo.

44. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037435170/

Les hackers sont parvenus à obtenir les identifiants d'un compte administrateur de la base de données de la société à laquelle ils ont pu accéder par ce biais et extraire les données personnelles des utilisateurs.

Malgré la technicité de ce type d'attaque, la CNIL a considéré que celle-ci n'aurait pu aboutir si des mesures de sécurité suffisantes avaient été mises en place et a donc prononcé, le **24 juillet 2018**, une sanction pécuniaire de **50 000 euros** à l'encontre de la société Dailymotion[45].

Le **7 mai 2018**, la CNIL a prononcé, à l'encontre de la société Optical Center, une sanction de **250 000 euros** pour insuffisance de sécurisation de données de ses clients, estimant que la société avait manqué à son obligation de sécurité des données personnelles, en méconnaissance de l'article 34 de la loi Informatique et Libertés[46].

Le **28 mai 2019**, la CNIL a, dans le même sens, sanctionné la société Sergic par une amende d'un montant de **400 000 €**[47].

• Sanctions prononcées à l'étranger

En **2013**, la chaîne de supermarché « Target » a été victime d'un vol massif de données personnelles de ses clients, parmi lesquelles des données bancaires.

Plus de **80** poursuites judiciaires et actions collectives (*class actions*) ont été menées, y compris à l'encontre de ses dirigeants.

La dernière évaluation du coût de ces réclamations s'élevait, en octobre **2017**, à **65 millions d'USD** de frais de défense et d'investigation[48].

Dans le même sens, la société Yahoo a été condamnée à payer une amende de **35 millions d'USD** pour avoir caché un piratage massif de données personnelles d'utilisateurs en **2016**[49].

Le **25 octobre 2018**, la société British Airways annonce avoir été victime d'une cyberattaque. L'enquête menée par l'Information Commissioner's Office (ICO) a révélé que les données, notamment de paiement de **500 000 clients**, avaient été piratées. L'organisme britannique a infligé, en **juillet 2019**, une amende record de **206 millions d'euros** à la compagnie aérienne[50].

45. https://www.lemonde.fr/pixels/article/2018/08/02/la-cnil-sanctionne-dailymotion-pour-un-piratage-de-comptes-d-utilisateurs-en-2016_5338652_4408996.html
46. https://www.solutions-numeriques.com/rgpd-1ere-sanction-de-la-cnil-contre-optical-center/
47. https://www.cnil.fr/fr/sergic-sanction-de-400-000eu-pour-atteinte-la-securite-des-donnees-et-non-respect-des-durees-de
48. https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031
49. https://www.lesechos.fr/tech-medias/hightech/yahoo-indemnise-les-victimes-du-hack-du-siecle-142766
50. https://www.bbc.com/news/business-48905907

La mise en place d'un système de responsabilité de l'entreprise victime d'un incident cyber pour insuffisance de **sécurisation** des STAD par le règlement européen sur la protection des données personnelles (RGPD), ainsi que les sanctions administratives et pénales susceptibles d'être prononcées par la CNIL, **doivent inciter les entreprises à investir dans la prévention, notamment relative aux données personnelles, en mettant en place des mesures de sécurité au sein de leurs systèmes d'information.**

SECTION V
L'INDISPENSABLE MISE EN PLACE DE RÈGLES PRÉVENTIVES DE CYBERGOUVERNANCE DANS LE CADRE DU DISPOSITIF DE GESTION GLOBALE DES RISQUES DES ENTREPRISES

■ **25.** Aujourd'hui, le constat est double :

- le **risque zéro n'existe pas**, la question n'est pas de savoir si l'on risque d'être attaqué, mais quand et comment limiter ce risque ;
- il faut **assurer la sécurité des systèmes d'information** en optimisant, avec des moyens raisonnables, leur capacité à résister aux actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données et des services associés.

■ **26.** La diffusion d'une culture de cybersécurité sous l'impulsion des dirigeants, avec le concours du risk manager est, par conséquent, nécessaire dans toutes les entreprises et souvent indispensable à leur survie, et peut être requise par les assureurs comme préalable à tout contrat.

FOCUS ET CONSEILS

LES RÈGLES DE LA CYBERGOUVERNANCE DANS L'ENTREPRISE

I. Instaurer une gouvernance transversale des données et du patrimoine informationnel de l'entreprise :

- identifier les informations, ainsi que les données sensibles et stratégiques à protéger ;
- réaliser un audit des vulnérabilités ;
- définir une politique de sécurité des systèmes d'information ;
- désigner un ou plusieurs référents en charge de ces questions ;

- instaurer une procédure de gestion de crise, immédiatement opérationnelle en cas de survenance d'une cyberattaque, comprenant un plan de continuité et de reprise d'activité ;
- se mettre en conformité avec le RGPD ;
- élaborer une politique de protection des données à caractère personnel et notamment à la lumière de l'invalidation du *privacy shield*, et avoir les bonnes *binding rules* ;
- mettre en place des procédures pour identifier les incidents de sécurité et les notifications requises (à la CNIL et/ou à l'ANSSI, le cas échéant) ;
- sécuriser le recours au télétravail et, d'une manière générale, le travail à distance ;
- intégrer les règles de cybergouvernance dans le règlement intérieur ;
- rédiger une charte informatique.

II. Revoir les contrats :

- d'externalisation de données et de protection informatique avec les prestataires afin qu'ils soient conformes aux nouvelles règles de responsabilités entre responsable de traitement et sous-traitants ;
- d'assurance et plus particulièrement d'assurance cyber ;
- de travail en les mettant à jour par l'insertion de clauses types de protection des données ou tout autre moyen d'information des salariés et renforcer les clauses de confidentialité figurant dans les contrats de travail.

III. Former les collaborateurs de l'entreprise :

- réaliser un plan de formation et de communication relatif à la sécurité informatique, la valorisation des actifs informationnels et la gestion des données à caractère personnel, impliquant l'ensemble des métiers et les partenaires sociaux ;
- réaliser des tests au minimum deux fois par an.

IV. Disposer d'un plan de communication et de gestion de crise

- préparer les éléments de langage pour la communication interne et externe ;
- avoir les coordonnées à jour des interlocuteurs potentiels pouvant être joints à tout moment (l'ANSSI, services de police, agence de communication, avocat, huissier de justice).

27. Face à la menace grandissante et polymorphe des cyberattaques pour la sécurité nationale, l'économie, les collectivités territoriales, les hôpitaux, les citoyens et les entreprises, la sécurité du numérique est devenue une priorité en France. Parmi les outils de protection indispensables figurent, au premier rang, les moyens de cryptographie et notamment les technologies de chiffrement de l'information.

Ces outils permettent d'assurer une sécurité au juste niveau lors de la transmission, du stockage et de l'accès aux données numériques sensibles. Les applications sont très nombreuses : échanges couverts par le secret de la défense nationale, données de santé ou de professions réglementées, données techniques, commerciales et stratégiques des entreprises, données personnelles des citoyens…

28. Dans ce cadre, la loi française ne limite pas les moyens de cryptologie.

La loi n° 2004-575 du 21 juin 2004 *« pour la confiance dans l'économie numérique »* pose le principe de la liberté de l'utilisation de la cryptologie, mais en réglemente l'usage, notamment en exigeant des déclarations préalables *(L. n° 2004-575, 21 juin 2004, art. 30). On entend, par moyen de cryptologie, tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission des données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité (...) ».*

À cet égard, le RGPD présente de façon pertinente le chiffrement comme « *une garantie appropriée* ».

FOCUS

LES CYBERCRIMINELS FONT DES ÉTUDES DE MARCHÉ DE LEURS CIBLES. LORSQUE CELLES-CI ONT ATTEINT UN NIVEAU SUPÉRIEUR DE PROTECTION, ILS CONCOCTENT DES ATTAQUES SOPHISTIQUÉES *VIA* LEURS « INTERMÉDIAIRES » PLUS FRAGILES EN TERMES DE CYBERSÉCURITÉ. COMMENT LUTTER CONTRE CETTE FAILLE ?

PHILIPPE COTELLE
Head of Insurance Risk Management Airbus Defence and Space
Administrateur de l'AMRAE, président de la commission Système d'information

L'essor du digital pendant la période de confinement liée au Covid-19 a considérablement augmenté la surface d'attaque et créé une dépendance au digital.

Par conséquent, le bombardement d'attaques qui a eu lieu durant le premier semestre 2020 devrait malheureusement perdurer. Il convient donc de trouver rapidement des pare-feu, faute de quoi le cyber sera la pandémie de demain.

La nouvelle génération de cybercriminels procède à des études de marché qui ont donné lieu à une recrudescence de *big game hunting* avec l'obligation, pour les entreprises, de vérifier et de sécuriser toutes les étapes de la *supply chain*, ce qui nécessite que soient préalablement auditées la dépendance et la pénétration de chacun des sous-traitants dans l'organisation interne de l'entreprise.

En effet, pour faire face à cette menace réelle et pour rester compétitives, les entreprises doivent travailler avec des partenaires armés et attentifs.

Les cybercriminels font également des campagnes de *ransomware* « au chalut », qui visent les PME de manière indifférenciée. Ces campagnes nécessitent peu de ressources pour un gain substantiel.

Les PME sont donc très concernées, soit de façon indépendante dans le cadre de ces attaques, soit parce qu'elles sont la faille du système d'autres entreprises dont elles sont partenaires.

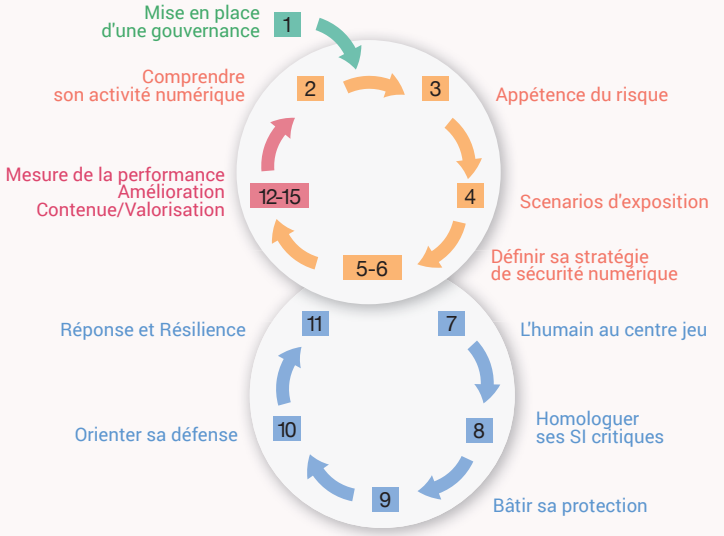
Pour autant, la plupart d'entre elles n'ont toujours pas conscience du risque qu'elles encourent, c'est-à-dire, très concrètement, de l'impossibilité de surmonter la perte financière et d'image engendrée par l'attaque.

Il est donc nécessaire que les petites entreprises sécurisent leur système d'information et protègent leur patrimoine en procédant aux investissements nécessaires, y compris en matière de formation, car ce sont celles qui auront su s'adapter qui survivront.

Quelle que soit la taille de l'entreprise, cette sécurisation nécessite de casser les silos et que soient définis, de façon transverse, les risques stratégiques qui peuvent affecter l'existence d'une entreprise.

En fonction du risque stratégique qui aura été défini et précisé sous l'angle du risque cyber, l'entreprise va donner la priorité aux protections à déployer pour s'en prémunir.

Le graphique ci-dessous, issu du rapport commun AMRAE/ANSSI intitulé « Maîtrise du risque numérique – L'atout Confiance », décrit cette démarche progressive qui a pour objectif de maximiser la résilience de l'entreprise en minimisant l'effort d'investissement.



La première de ces étapes, dans le cadre d'une politique de gestion du risque numérique, est la mise en œuvre d'une cybergouvernance et la création d'un comité des risques constitué de représentants des équipes business et sécurité, afin de constituer un regard transverse sur le patrimoine à protéger. L'objectif étant d'identifier et protéger les vulnérabilités de l'entreprise puisque le risque cyber est une menace susceptible de les affecter, et donc d'avoir un impact négatif majeur sur le business.

CHAPITRE II

LES INFRACTIONS CLASSIQUES DANS LE CYBERESPACE

Les actes classiquement réprimés par le Code pénal pouvant être commis dans l'espace numérique, il y a lieu d'étudier celles de ces infractions qui portent atteinte aux biens et à la réputation de l'entreprise.

SECTION I
LES ATTEINTES AUX BIENS

■ **29.** Si la criminalité visant les systèmes de traitement automatisés de données (STAD) est sanctionnée pénalement par des incriminations et des circonstances aggravantes spécifiques, en pratique, la cybercriminalité correspond à une liste d'infractions, ainsi qu'à une façon d'opérer.

Les qualifications classiques, telles que l'escroquerie notamment en bande organisée, l'abus de confiance, le blanchiment simple ou en bande organisée (C. pén., art. **324-1**) permettent, par ailleurs, de réprimer bon nombre d'actes frauduleux dans leur dimension numérique.

■ **30.** La liste des infractions par atteintes aux biens peut être ainsi synthétisée :

ESCROQUERIE PAR INTERNET 313-1 et ss	Fraudes aux noms de domaine	▸ *Typosquatting* : création d'un nom de domaine approchant pour tromper la victime (amendes-gouv.fr et amendes.gouv.fr) et la déterminer à une remise	C. pén., art. 313-1 : 5 ans d'emprisonnement 375 000 € (C. pén., art. 313-2, al ; 1er à 6 : 7 ans d'emprisonnement et 750 000 € en présence de diverses circonstances aggravantes, peines portées à 10 ans d'emprisonnement et 1 M € lorsque l'escroquerie est commise en bande organisée (C. pén., art. 313-2, dernier alinéa).
FAUX ET USAGE DE FAUX PAR INTERNET		▸ *Phishing* : envoi de mails frauduleux à des fins : - Publicitaires ou de ventes de produits prohibés - De recueil frauduleux de DCP (codes et coordonnées bancaires… pour *carding*… - D'infection par virus pour contrôler le système et commettre des escroqueries	Le commerçant devient victime de l'escroquerie et la banque règle le particulier de l'usage frauduleux de son numéro de carte bancaire dont il ne s'est pas départi (Code monétaire et financier). Mais l'action pénale survit pour le particulier et le commerçant.
	Fraude aux cartes bancaires	▸ *Carding* : piratage de n° carte bancaire revendu sur les sites du deep web inaccessibles aux policiers (sauf en criminalité organisée et en bande organisée).	
ESCROQUERIE suite		▸ *Skimming* : récupération de n° de carte bancaire par lecture de la piste dans des DAB. Escroqueries au logement, la location, etc., et en tous genres. Faux ordres de virement par manipulation informatique grâce à l'ingénierie sociale, plus rarement avec un malware préalable ou une prise de contrôle d'un ordinateur.	
	Fraudes aux PBX (standards téléphoniques), *phreaking*	Fraudes aux autocommutateurs téléphoniques, escroquerie de communications passées sur le compte d'une entreprise pour bénéficier de gains ou services *via* des numéros surtaxés.	

EXTORSION 312-1 et ss	Il s'agit d'infractions cyber stricto sensu de blocage d'ordinateurs par un malware, commises dans le but d'une infraction cyber au sens large, cf. l'ENTRAVE 323-2 et chiffrement des données.	- Contraindre à la remise de personnages de jeux vidéo ou d'unités de compte *via* internet pour débloquer l'ordinateur (bitcoin, Ethereum…). - Contraindre une entreprise à payer en bitcoins pour recouvrer l'accès à ses ordinateurs qui ont été chiffrés par un virus (entrave le système en sus).	Difficulté de l'élément matériel. La contrainte est un élément de l'infraction. 7 ans d'emprisonnement et 100 000 € (C. pén., 312-1, al. 2). 10 ans d'emprisonnement et 150 000 € en présence de diverses circonstances aggravantes, notamment la particulière vulnérabilité de la victime (C. pén., art. 312-2).
CHANTAGE 312-10 et ss	IDEM, mais menace de ruiner la réputation par des révélations, par la divulgation d'une vulnérabilité technique.	- Menacer de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération pour obtenir un secret, des fonds une remise de la part de la victime (chantage).	Distinction du chantage. La menace de révélation 5 ans et 75 000 € (C. pén., art. 312-10). Si exécution de la menace, 7 ans et 100 000 €.
ABUS DE CONFIANCE ABUS DE FAIBLESSE 314-1	*Via* internet.	Divers modes opératoires et blanchiment et recel de quelque chose, etc.	Jusqu'à 10 ans et 1 500 000 €.
Toute infraction commise par internet ou au moyen des technologies de l'information et de la communication a vocation à entrer dans le champ de la cybercriminalité au sens large. Aussi, ce tableau n'est pas exhaustif.			

SECTION II
L'USURPATION D'IDENTITÉ PORTANT ATTEINTE À LA REPUTATION DE L'ENTREPRISE

■ **31.** L'usurpation d'identité numérique, le vol d'identité en ligne ou l'usage de données de toute nature, peut prendre plusieurs formes et vise à se faire passer pour un autre (dirigeant, entreprise, administration) pour accéder à des données ou des comptes bancaires et détourner des fonds, ou porter atteinte à la réputation d'une entreprise ou de ses dirigeants ou commettre des escroqueries dites *« à la carambouille »*. (Un vrai fournisseur se fait leurrer par quelqu'un qui se fait passer pour son entreprise cliente et le livre dans une zone industrielle, il ne sera jamais payé…).

■ **32.** Les techniques le plus souvent utilisées pour soutirer des données permettant une usurpation d'identité sont le *phishing* ou l'utilisation de *keyloggers* (maliciels enregistrant les frappes de clavier).

L'usurpation d'identité a, notamment, été établie dans le cas de la création d'adresses e-mails, de faux profils Facebook et de fausses annonces dans le but de nuire à un dirigeant d'entreprise[51].

■ **33.** Face à l'augmentation de ces atteintes à l'identité *via* internet, le législateur a créé, par la loi du **14 mars 2011** dite « Loppsi[52] 2 », le délit d'usurpation d'identité[53] qui réprime d'un an et de 15 000 euros d'amende *« le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération »* (226-4-1 du CP).

Le rapporteur de la loi du **14 mars 2011** a souligné que le terme « identité » devait être compris comme *« recouvrant tous les identifiants électroniques de la personne, c'est-à-dire à la fois son nom, mais aussi son surnom ou son pseudonyme utilisé sur internet[54] »*.

■ **34.** L'élément matériel du délit d'usurpation d'identité consiste soit en l'usurpation de l'identité d'un tiers, soit en l'utilisation de données permettant l'identification d'un tiers. L'élément moral suppose, en plus d'un dol général, de vouloir troubler la tranquillité d'autrui ou de vouloir porter atteinte à son honneur ou à sa considération.

■ **35.** Le délit d'usurpation d'identité peut être invoqué par une personne morale. La jurisprudence considère en effet qu'en cas d'atteinte

51. CA Paris, 10 oct. 2014, n° 13/7387 : Comm. com. électr. 2015, comm. 9).
52. Loi d'orientation et de programmation pour la performance de la sécurité intérieure).
53. Article 226-4-1 du Code pénal.
54. E. Ciotti, Rapport AN n° 2271, 1re lecture, 27 janv. 2010, p. 112.

à sa réputation sur internet, l'entreprise, représentée par son dirigeant social, peut agir sur le fondement de l'usurpation de l'identité numérique. Ce texte peut éviter de porter le débat sur le terrain dérogatoire du droit commun, à savoir la loi de 1881 sur la presse avec, notamment, la diffamation plus difficile à caractériser et de courte prescription.

36. Toutes ces évolutions légales et réglementaires traduisent une véritable prise de conscience, extrêmement importante de la part des institutions, des enjeux liés à la sécurité numérique dans son ensemble, en ajustant le cadre juridique européen aux changements radicaux qu'elle introduit et en mettant en œuvre les mesures adaptées pour une transition numérique réussie.

Le risque est le nouveau concept clé du RGPD et de NIS. Ces deux textes nous éclairent aussi sur les méthodes susceptibles de limiter la survenance des risques et de les minimiser. À l'ère d'internet et du big data, le risque est omniprésent.

FOCUS

QUEL RÔLE POUR LES OPÉRATEURS TÉLÉCOMS EN MATIÈRE DE CYBERSÉCURITÉ ?

NICOLAS ARPAGIAN
Vice-président en charge de la stratégie et des affaires publiques, Orange Cyberdefense

Les pirates informatiques utilisent les réseaux de communication pour infecter les serveurs de données et les systèmes d'information de leurs cibles. La détection le plus en amont possible des équipements visés devient une condition d'une meilleure sécurité numérique globale. Un constat fait par Guillaume Poupard, le directeur général de l'Agence nationale des systèmes d'information (ANSSI) en octobre 2017[55] : *« À mon avis, le seul endroit où on peut agir de manière efficace, c'est au niveau des opérateurs qui transportent ces choses-là [les logiciels malveillants]. Eux ont probablement la capacité d'agir à ce moment-là »*.

Cette analyse a été mise en perspective dans la *Revue Stratégique de Cyberdéfense*[56] publiée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) en mars 2018, qui appelle les opérateurs télécoms à renforcer leur coopération avec l'État pour déceler les cyberattaques en cours. Sa déclinaison opérationnelle intervient dans le cadre de la Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025.

Son article 34 complète le Code des Postes et des Communications électroniques en établissant un article L. 33-14 qui explique la nature de cette coopération :

« Art. L. 33-14.-Pour les besoins de la sécurité et de la défense des systèmes d'information, les opérateurs de communications électroniques peuvent recourir, sur les réseaux de communications électroniques qu'ils exploitent, après en avoir informé l'autorité nationale de sécurité des systèmes d'information, à des dispositifs mettant en œuvre des marqueurs techniques croissants aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés.

« À la demande de l'autorité nationale de sécurité des systèmes d'information, lorsque celle-ci a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information, les opérateurs de communications électroniques ayant mis en œuvre les dispositifs prévus au premier alinéa procèdent, aux fins de prévenir la menace, à leur exploitation, en recourant, le cas échéant, à des marqueurs techniques que cette autorité leur fournit ».

« Par dérogation au II de l'article L. 34-1, les opérateurs de communications électroniques sont autorisés à conserver, pour une durée maximale de six mois, les données techniques strictement nécessaires à la caractérisation d'un événement détecté par les dispositifs mentionnés au premier alinéa du présent article.
Les données recueillies dans le cadre de l'exploitation de ces dispositifs autres que celles directement utiles à la prévention et à la caractérisation des menaces sont immédiatement détruites. »

« Lorsque sont détectés des événements susceptibles d'affecter la sécurité des systèmes d'information, les opérateurs de communications électroniques en informent sans délai l'autorité nationale de sécurité des systèmes d'information. »

« À la demande de l'autorité nationale de sécurité des systèmes d'information, les opérateurs de communications électroniques informent leurs abonnés de la vulnérabilité de leurs systèmes d'information ou des atteintes qu'ils ont subies.

« Les modalités d'application du présent article sont précisées par décret en Conseil d'État. Celui-ci détermine notamment les catégories de données pouvant être conservées par les opérateurs de communications électroniques. »

55. « L'ANSSI veut que les opérateurs protègent Internet des cyberattaques », *Nextinpact*, Guénaël Pépin, 12 octobre 2017 - https://www.nextinpact.com/news/105385-lanssi-veut-que-operateurs-protegent-internet-cyberattaques.htm
56. http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

Ce dispositif devrait permettre une meilleure anticipation des campagnes d'attaques et servir à renseigner utilement les réseaux de CERT (*Computer Emergency Response Teams*) qui servent aux praticiens de la cybersécurité pour échanger en toute confidentialité et selon des protocoles normés des informations sur les caractéristiques des logiciels malveillants détectés. La qualification technique de ces maliciels sera intégrée dans les bases de données des sondes de supervision des systèmes d'information, afin de repérer leur présence et de bloquer le plus tôt possible leur accès aux serveurs de l'entité visée.

Les opérateurs télécoms sont également en première ligne pour répondre aux campagnes d'attaques en déni de service (DDoS) qui conduisent à saturer l'accès à un site internet, empêchant les internautes (visiteurs ou clients) légitimes de se connecter au service. Des prestataires malhonnêtes proposent en effet des solutions clés en main, avec la mise à disposition de dizaines de milliers d'ordinateurs infectés qui peuvent, pour des sommes dérisoires, être sollicités en quelques clics et conduire à la non-disponibilité de sites internet marchands ou institutionnels. Les opérateurs peuvent, à la demande de leurs clients, filtrer le flux de connexions et ainsi restituer un libre usage du site mis en difficulté.

Une des forces d'un opérateur télécoms propriétaire de ses infrastructures, à l'instar d'Orange, dont les réseaux sont déployés à l'échelle planétaire, est de disposer de relais et de capteurs sur l'ensemble du globe. Alors que les attaquants appuient leurs dispositifs d'attaques à partir d'équipements interconnectés dans plusieurs pays, l'implantation internationale d'un prestataire en cybersécurité est un atout pour être informé en amont des modes d'intervention des pirates, afin de documenter rapidement les outils de détection. Idem pour la capacité de mobilisation d'équipes opérationnelles pour la réponse à incidents. Enfin, il est souhaitable que la prise en compte de la cybersécurité accompagne naturellement le déploiement des services numériques proposés par les opérateurs télécoms.

PARTIE II

CYBERATTAQUE : QUELLE RÉPONSE JUDICIAIRE ?

CHAPITRE I

LES ACTEURS ET LEUR CADRE INSTITUTIONNEL

SECTION I
LE SYSTÈME FRANÇAIS

La spécificité de la cybercriminalité et la technicité des modes opératoires des cyberdélinquants ont nécessité la création de services d'enquête dédiés, ainsi qu'une spécialisation progressive de l'institution judiciaire.

I-1.
LA SPÉCIALISATION DES SERVICES D'ENQUÊTE

■ **37.** Les plaintes au niveau local et les affaires simples sont prises en charge par les commissariats de police et les brigades de gendarmerie.

■ **38.** Les affaires nécessitant davantage d'investigations sont traitées par les sûretés départementales de police, les sections de recherche de la gendarmerie et les services de police judiciaire à Paris et dans la petite couronne.

■ **39.** Les procédures les plus complexes en raison de leur technicité et de leur dimension internationale, par exemple, sont de la compétence de services spécialisés centraux ou en assistance d'un service classique.

La création de ces services spécialisés a résulté de la nécessité d'adapter les dispositifs aux stratégies utilisées par les cyberdélinquants et s'est inscrite dans un contexte général de mobilisation des institutions publiques pour renforcer l'efficacité de la lutte contre la cybercriminalité.

Ces services spécialisés ont ainsi un rôle primordial au sein de cette lutte contre la cybercriminalité.

On peut ainsi citer :

▸ **la sous-direction de lutte contre la cybercriminalité (SLDC)** de la direction centrale de la police judiciaire, qui joue un rôle préventif et répressif : d'une part, elle définit les stratégies à mettre en œuvre dans les domaines de l'opérationnel, de la formation et de la prévention et, d'autre part, elle contribue à la recherche des preuves des infractions de cybercriminalité ;

▸ son office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) chargé :

- du traitement des contenus illicites de l'internet, de leur recoupement et de leur exploitation ;
- de centraliser, au bénéfice des enquêteurs, les informations utiles pour faciliter les échanges opérationnels avec les fournisseurs d'accès à internet ;
- de la répression des infractions liées aux atteintes aux systèmes de traitement automatisé de données, des fraudes aux opérateurs de communications électroniques, des escroqueries commises sur internet et des atteintes aux systèmes de paiement.

▸ à Paris et dans la petite couronne, pour le traitement du contentieux spécifique des infractions aux STAD et aux données :

- La Brigade de lutte contre la cybercriminalité (BLCC), anciennement Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), est compétente pour traiter principalement les actes relevant de l'accès ou du maintien frauduleux dans un système de traitement automatisé des données (infractions aux STAD). Par souci de cohérence, elle a absorbé le groupe de La Brigade des fraudes aux moyens de paiement (BFMP) pour lutter contre cette nouvelle délinquance économique et financière et, notamment, le cyberblanchiment réalisé par des transactions dématérialisées par le biais de cryptoactifs.

  Elle contribue à la diffusion d'une culture de cybervigilance et de cybersécurité auprès du grand public, des professionnels du secteur informatique et, plus globalement, du monde numérique. La Brigade de répression de la délinquance astucieuse (BRDA) traite des escroqueries, faux et abus de confiance en ligne.

- La Brigade de protection des mineurs traite des affaires de pédopornographies et de *grooming* (rendez-vous donné en ligne aux enfants sous des prétextes fallacieux et donnant souvent lieu à des infractions graves).

- La brigade de répression de la délinquance envers la personne traite des affaires de diffamation, d'apologie du

terrorisme, du droit pénal du travail *via* internet.

- Le centre de lutte contre les criminalités numériques (C3N) est chargé d'assurer le pilotage et l'appui spécialisé de l'action de la gendarmerie contre la cybercriminalité et les criminalités numériques, de mener ou coordonner les investigations d'ampleur nationale de la gendarmerie ayant trait à la cybercriminalité, et de réaliser une surveillance permanente de l'internet, pour y détecter et collecter les preuves des infractions qui peuvent y être commises. Le réseau d'enquêteurs spécialisés par niveau de la gendarmerie forme une chaîne globale et cohérente de 3 500 gendarmes. Seuls ses enquêteurs de Pontoise disposent d'une compétence nationale et sont formés à l'enquête sous pseudonyme sur internet.

- Les douanes, en particulier la direction nationale du renseignement et des enquêtes douanières (DNRED) dispose, depuis **2009**, d'une structure de lutte contre la cybercriminalité, appelée Service des cyberdouanes, ou encore cellule Cyberdouane. Le service recueille et exploite tous les renseignements utiles dans la lutte contre les fraudes sur internet en matière de trafics de marchandises prohibées, réglementées ou fortement taxées. Ses agents effectuent une veille sur internet afin d'établir des liens entre différents sites, forums ou mots-clés et de cartographier les fraudes complexes. Ils cherchent à identifier les personnes physiques ou morales qui se cachent derrière un site de vente en ligne, une adresse électronique ou un pseudonyme sur un site de petites annonces, un forum, un blog ou un réseau social. Ils mènent des enquêtes dans le cadre de cybercontrefaçon et des investigations, y compris dans le darknet.

■ **40.** Ces services se sont fortement mobilisés ces dernières années pour relever les défis relatifs à la connaissance du cyberdélinquant, au développement des ressources humaines de renseignement, à la coordination des réseaux d'information et d'innovation, à la formation des enquêteurs en plus grand nombre et à la coopération internationale.

FOCUS SUR LE C3N

“ RENCONTRE AVEC LA COLONELLE FABIENNE LOPEZ ET LE CAPITAINE PAUL-ALEXANDRE GILLOT

Basé à Pontoise (Val d'Oise), au sein du pôle judiciaire de la gendarmerie, le C3N est une unité de pointe de la gendarmerie dans la lutte contre la cybercriminalité. Ce service spécialisé, qui s'est illustré récemment dans l'opération EMMA95 contre le réseau de communication chiffré Encrochat, ou encore dans le démantèlement de plusieurs réseaux de machines infectées par le *botnet* Retadup à l'été 2019, est dirigé par la colonelle Fabienne LOPEZ.

Pouvez-vous nous présenter le C3N, son origine et son rôle ?
Créé en 2015, le C3N est historiquement l'héritier du département de lutte contre la cybercriminalité créé en 1998 au sein du Service technique de recherches judiciaires et de documentation, devenu par la suite le STRJD. Le C3N est une unité d'investigation à compétence nationale dont la mission principale est l'investigation en matière de cyberdélinquance, à savoir les atteintes aux systèmes de traitement automatisé de données, trafics sur le darknet ou à travers d'autres systèmes de communication (What's App, Telegram, SnapChat, etc.), escroqueries sous différentes formes (SPAM, *phishing*, ou encore faux supports techniques), etc.

Le C3N est composé de 42 personnes réparties sur 4 départements aux rôles bien définis :

- le département coordination, qui anime et coordonne la chaîne Cybergen, communauté de près de 3 500 gendarmes ;
- le département technique : recherche et développement, pôle de compétence rare au profit des enquêtes et appui en termes d'investigations numériques ;
- le département de conception et développement cyber, qui travaille à la création et au développement d'outils cyber que tous les enquêteurs pourront utiliser sur le terrain (recherche source ouverte) ;
- le département Enquêtes, qui est divisé en 5 groupes, mène les enquêtes du C3N, appuie et coordonne l'action des 11 antennes-C3N réparties sur le territoire national.

Le **département enquête du C3N**, qui a vocation à mener **les enquêtes les plus complexes en matière de cybercriminalité**, seul ou en co-saisine avec les unités territoriales, sur les **phénomènes d'ampleur nationale et internationale**, est dirigé par **le capitaine GILLOT**. À ce titre, le **C3N est notamment chargé, pour la gendarmerie, de la lutte contre :**

- les organisations criminelles utilisant, entre autres, des *botnets* (Retadup en 2019), des systèmes de communication chiffrés (Encrochat depuis 2017) ;
- les trafics illégaux sur le darknet, en particulier les ventes massives de produits stupéfiants et les trafics d'armes ;

- les atteintes aux STAD, notamment, sous la forme de rançongiciels. **Concernant les attaques par rançongiciel, la compétence du C3N pour mener les investigations dépendra du malware utilisé pour l'attaque.** En effet, les rançongiciels sont répartis par familles, elles-mêmes réparties entre les services spécialisés ;

- les escroqueries complexes comme celles des fausses réparations informatiques ;

- les atteintes sexuelles contre les mineurs sur internet ;

- les investigations impliquant tous les cryptoactifs. En effet, les cryptomonnaies sont au centre de toutes les affaires de cybercriminalité et deviennent une véritable thématique horizontale. L'enjeu majeur est la désanonymisation des criminels par le traçage des flux de cryptomonnaie et le *demixing* des transactions.

Toujours, en lien avec la section J3 du parquet de Paris, spécialisée dans la cybercriminalité, le C3N travaille en concertation avec les institutions internationales (Europol, Interpol, etc.), mais aussi avec de nombreuses sociétés privées, afin d'obtenir du renseignement (fournisseurs d'accès, opérateurs téléphoniques, développeurs d'antivirus, etc.). Le C3N vient également en appui technique des unités de terrain en termes de cybercriminalité, et participe à la formation des enquêteurs spécialisés sur certains volets spécifiques, comme l'enquête sous pseudonyme.

Pouvez-vous nous parler d'une enquête achevée et d'un réseau démantelé ?
Le C3N a récemment réussi à neutraliser le virus informatique international « Retadup ».

Créé en 2016, le *botnet* Retadup comptait 11 versions différentes et 20 noms de domaines embarqués. Sa capacité de nuisance était due notamment à un outil de prise de contrôle à distance (minage de cryptomonnaies), du vol massif de données personnelles (vol de données médicales d'un hôpital israélien, capture de mots de passe stockés) et l'exécution d'actions offensives coordonnées.

Au total, ce *botnet* contrôlait, à l'insu de leurs propriétaires, plus d'1,327 million de logiciels.

Le 25 mars 2019, la société d'antivirus Avast a signalé une vague d'infections sur 200 000 PC répartis dans le monde dont un serveur C&C en France, ce qui a permis au C3N d'être saisi par la section cybercriminalité du parquet de Paris pour mener l'enquête.

Sur réquisition judiciaire, une copie du serveur C&C est faite chez l'hébergeur et 11 versions du malware sont découvertes lors de son analyse. Une faille dans l'exécution du *botnet* Retadup a également été mise à jour, permettant au C3N de créer son propre serveur C&C en vue de remplacer celui de Retadup et de permettre ainsi la neutralisation des logiciels bots.

Le 1er juillet 2019, opérant en toute discrétion pour ne pas se faire repérer par les cybercriminels, le C3N a procédé au remplacement du serveur C&C par celui contrôlé par ses soins. Le FBI a appuyé leur action en prenant en charge la redirection des noms de domaine.

Le serveur du C3N a alors enregistré plus d'un To de logs, ce qui a permis de gérer en direct la désinfection progressive des 1,327 million de machines contrôlées par Retadup. Les investigations se sont poursuivies avec l'ouverture d'une information judiciaire au TGI de Paris.

Quel est votre avis sur la coopération internationale en matière de cybercriminalité ? A t elle progressé ces dernières années et en quoi est-elle primordiale pour lutter contre les cyberattaquants ?
Concernant le contentieux cyber, les derniers dossiers du C3N et des autres services spécialisés ont, plus que jamais, souligné les besoins exponentiels en matière de coopération internationale.

De nos jours, il est courant de se retrouver face à des adversaires qui ont une infrastructure répartie sur différents pays. La coopération internationale est donc primordiale, d'abord pour des aspects pratiques comme la nécessité d'obtenir rapidement une copie des serveurs avant que les preuves ne disparaissent. Sur le plan de l'enquête à proprement parler, si un autre service étranger enquête sur le même groupe, il s'agit d'effectuer en amont une déconfliction utile pour la suite des investigations..., voire de se répartir les tâches à effectuer.

De plus, dans le cadre de la planification d'une opération, il n'est pas rare, dans le contentieux cyber, que celle-ci se déroule de manière coordonnée en impliquant différents pays.

On note plusieurs modes de coopération :
- police to police en bilatéral ;
- dans le cadre d'une coopération plus approfondie impliquant Europol et/ou Interpol ;
- de manière plus complète dans le cadre d'une ECE.

En matière de lutte contre les rançongiciels, par exemple, la dernière famille prise en charge par le C3N a nécessité, dès le départ, une coopération avec 5 pays afin de recouper les éléments de l'attaque,

obtenir les copies des serveurs mis en lumière dans le temps de la négociation, puis procéder à une déconfliction sur l'enquête en elle-même. Alors que le premier fait en France remonte à septembre 2020, les premières réunions de coordination ont déjà eu lieu avec Europol et Interpol, au cours desquelles la France est en position de prendre le lead sur les investigations.

Les soit-transmis de la section J3 cybercriminalité du parquet de Paris mentionnent désormais systématiquement l'autorisation de partager les éléments de l'enquête avec Europol et ses États membres.

I-2. LA SPÉCIALISATION DES MAGISTRATS

■ **41.** La spécialisation des magistrats du siège et du parquet, quel que soit le degré de la juridiction, s'est également avérée nécessaire.

La loi n° 2016-731 du 3 juin 2016 a ainsi renforcé les dispositions du titre XXIV du livre IV du Code de procédure pénale.

L'article **706-72-1** du Code de procédure pénale confie ainsi au procureur de la République de Paris, au pôle de l'instruction, au tribunal judiciaire et à la cour d'assises de Paris une **compétence concurrente nationale** en matière d'atteintes aux STAD et d'atteintes aux intérêts fondamentaux de la nation (cybersabotage), pour les affaires complexes et étendues géographiquement.

La saisine du parquet et du tribunal judiciaire de Paris, fondée sur la compétence nationale concurrente pour les infractions relatives aux STAD, ne relève pas d'une initiative de la partie civile, mais uniquement de celle du parquet d'un autre tribunal territorialement compétent qui requerrait le dessaisissement au profit de la juridiction parisienne.

■ **42.** Cette spécialisation a été confortée par la loi n° **2019-222** du **23 mars 2019** qui a créé une nouvelle compétence au profit du tribunal judiciaire de Paris qui est devenu la juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO). Elle rassemble des magistrats spécialisés, chargés de conduire des enquêtes de grande ampleur, impliquant fréquemment des investigations à l'échelle nationale ou internationale, notamment en matière de cybercriminalité[57] [58].

57. Circulaire du 17 décembre 2019 relative à la compétence nationale concurrente du tribunal de grande instance et de la cour d'assises de Paris dans la lutte contre la criminalité organisée de très grande complexité et à l'articulation du rôle des différents acteurs judiciaires en matière de lutte contre la criminalité organisée.

58. Entretien avec R. Heitz, Gaz. Pal. 4 févr. 2020, n° 369 x 4, p. 10.

La création de la JUNALCO a entraîné également la réorganisation du parquet de Paris en 3 divisions par spécialisation, la J3 étant chargée de la lutte contre la cybercriminalité.

FOCUS

MYRIAM QUÉMÉNER
Avocat général près la cour d'appel de Paris

Que pensez-vous de la spécialisation des magistrats en matière de cybercriminalité ?

« Elle est à mon sens indispensable, non seulement pour avoir une vision et une connaissance des modes opératoires des délinquants qui sont de plus en plus sophistiqués, mais également pour gérer la dimension internationale et avoir des contacts aussi bien au sein d'Interpol, d'Europol que du FBI, par exemple.

Cette formation doit également mettre l'accent sur les techniques spéciales d'enquête harmonisées par la loi de 2019, qui sont très encadrées juridiquement et qu'il convient de sécuriser pour faire tenir les procédures. Il s'agit plus particulièrement de l'enquête sous pseudonyme, de la géolocalisation, de la captation de données à distance.

Compte tenu de l'évolution permanente de la matière et de l'imagination débordante des cyberdélinquants, cette formation doit être continue.

Elle devra comprendre un suivi de la jurisprudence des cours européennes et une veille juridique permanente.

Il serait également nécessaire que les magistrats soient intégrés à la communauté cyber et participent aux think tanks et aux divers événements incontournables sur le sujet rassemblant les professionnels de la matière.

Cela suppose également de créer, non seulement au parquet, mais également au siège et à chaque degré de juridiction, un département numérique et cyber étoffé, composé de magistrats et de cadres spécialisés en technique numérique. »

■ **43.** Le traitement de la cybercriminalité nécessite de connaître les modes opératoires évolutifs des cybercriminels, ce qui suppose de nouer des partenariats solides avec les acteurs essentiels intervenant en amont de la justice, en particulier avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui intervient en première ligne afin de constater les dégâts résultant des cyberattaques, et qui est en mesure de détecter, par exemple, quel *ransomware* a été utilisé par les cybercriminels.

FOCUS

RÉMI HEITZ
Procureur de la République de Paris

Comment le parquet de Paris est-il organisé pour faire face à l'accroissement du nombre et de l'ampleur des cyberattaques ?

*« Le parquet de Paris est un acteur central de la lutte contre la cybercriminalité puisqu'il dispose d'une compétence concurrente nationale en matière d'atteinte à un système de traitement automatisé de données. Il a donc vocation à se saisir des dossiers d'ampleur commis en France en matière de cybercriminalité et à centraliser les procédures en lien avec les parquets locaux sur le ressort desquels les attaques peuvent avoir lieu. Par conséquent, la multiplication récente des cyberattaques a des effets directs sur son activité. Pour l'année **2020**, par exemple, la section J3 dédiée à la cybercriminalité a enregistré au titre de sa compétence nationale **397** saisines, alors que ce chiffre n'était que de **62** en **2019**.*

*Pour répondre à ce phénomène d'ampleur nationale, cette section est intégrée, depuis le **1er février 2020**, au parquet de la Juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO). Cette organisation permet aux magistrats et fonctionnaires d'échanger avec les autres sections spécialisées dans la criminalité organisée de grande ampleur (grand banditisme, criminalité financière) pour établir d'éventuels liens et développer des synergies renforçant l'efficacité dans l'action. La section est également plus facilement identifiable, tant par les autres parquets que par ses partenaires étrangers. Les ramifications internationales de cette délinquance déterritorialisée nécessitent une collaboration internationale forte, et le parquet de Paris s'ouvre continuellement sur l'extérieur pour y répondre.*

*De surcroît, les trois magistrats de cette section sont désormais assistés, depuis la fin de l'année **2020**, d'un juriste assistant spécialisé dans l'entraide pénale internationale, d'un officier de liaison de la gendarmerie nationale et d'un assistant issu de la police nationale spécialisé dans le traitement des ransomwares.*

Au-delà des renforts en termes de personnel, dont l'augmentation devra se poursuivre dans les années à venir, il a été décidé de créer une permanence dédiée à la cybercriminalité le soir et le week-end. Des magistrats spécialisés peuvent donc désormais réagir immédiatement, à toute heure du jour et de la nuit, en cas de cyberattaque d'ampleur sur tout le territoire national. »

Quelle stratégie pénale mettez-vous en place pour lutter contre la cybercriminalité ?

« Pour lutter efficacement contre la cybercriminalité en tarissant le nombre d'attaques, nous devons établir les responsabilités pénales, démasquer les auteurs des attaques et les sanctionner. Nous n'avons pas affaire à des génies de l'informatique qui se joueraient des autorités, il s'agit avant tout de délinquants. Notre stratégie se doit donc d'être empreinte de réactivité, d'adaptabilité et de fermeté.

Afin de limiter l'ampleur des attaques, nous devons observer finement les techniques utilisées par les hackers. Pour ce faire, la centralisation des procédures est un réel atout. Le parquet de Paris se saisit notamment de toutes les procédures de ransomwares, de fraudes aux réparations informatiques et de jackpotting. Il en saisit pour enquête des offices centraux (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication – OCLCTIC – et Centre de lutte contre les criminalités numériques ou C3N). Cela permet de disposer d'une vue d'ensemble de ces réseaux de criminalité organisée, d'observer finement par recoupements les mécanismes mis en œuvre et de ne pas subir passivement les attaques. En cartographiant l'infrastructure technique des cybercriminels, nous pouvons remonter plus rapidement par le mode opératoire jusqu'aux auteurs lors de nouvelles résurgences d'une attaque. Le démantèlement récent du ransomware Egregor en Ukraine, avec la participation du parquet de Paris, nous confirme que ces efforts sont payants.

Pour faire face à une délinquance protéiforme et qui se renouvelle régulièrement, il faut également se former et informer. Nous avons, en ce sens, renforcé nos liens avec le secteur privé et le secteur de la recherche. Nous travaillons fréquemment avec les sociétés de remédiations à incidents pour obtenir leurs rapports d'intervention et les informations techniques en leur possession. Elles interviennent rapidement auprès de la victime pour mettre fin aux effets de l'attaque et ont donc un savoir-faire dont le partage nous aide dans nos enquêtes. Nous sommes également en contact avec une doctorante de l'École normale supérieure qui nous aide à repenser nos techniques d'enquête en matière de cybercriminalité. Cette ouverture au-delà des frontières traditionnelles du monde judiciaire est indispensable si nous voulons être efficaces et pouvoir juger de plus en plus de cybercriminels. Dans le but de faire profiter tous les acteurs de nos réflexions, nous allons diffuser, en 2021, un modèle de plainte et une fiche réflexe à destination de tous les services de police et de gendarmerie. Il est en effet primordial de pouvoir agir rapidement en effectuant, au plus près de l'attaque, des gels de données auprès des autorités étrangères.

Une fois les responsabilités individuelles établies, nous portons évidemment un message de fermeté. C'est le seul moyen de mettre un terme au sentiment d'impunité des cybercriminels. Notre fermeté s'exprime dans le déroulement des enquêtes ou des informations judiciaires d'abord. À ce stade, nous requérons régulièrement la saisie des avoirs criminels quand ils existent. Nous ne pouvons accepter que certains s'enrichissent par le biais de cette délinquance. À l'audience correctionnelle, ensuite, la même rigueur est de mise et des peines

d'emprisonnement sont requises. Toutefois, pour être suivis dans nos réquisitions, il est indispensable de faire œuvre de pédagogie devant le tribunal, car nous présentons essentiellement des dossiers techniques avec des criminels aguerris et des modes opératoires très complexes. »

Pensez-vous que le corpus juridique actuel est suffisant pour répondre à ce fléau ?

*« Les modes opératoires des cyberattaques sont multiples et sont en développement continu. Ils demandent une adaptation permanente de la justice, mais le cadre souple de la loi dite Godfrain du **5 janvier 1988**, qui a créé les infractions d'atteintes aux systèmes de traitement automatisé de données, nous permet d'appréhender les nouveaux phénomènes en matière de cybercriminalité. Elle réprime en effet toutes les actions susceptibles de porter atteinte à un système de traitement automatisé de données, sans en fixer une liste précise et contraignante.*

Cependant, face à l'accroissement de la cybercriminalité, les services de police et de gendarmerie ont dû adapter leurs techniques d'enquête. Certains procédés techniques ne sont pas disponibles en France. Par ailleurs, certaines autres techniques ne sont pas toujours prévues dans le Code de procédure pénale, faute pour le législateur d'avoir pu anticiper leur création. Nous sommes donc dans une forme de course à la technologie qui nécessite des moyens humains et matériels toujours plus performants. »

Quels conseils pouvez-vous donner aux entreprises dans ce domaine ?

« Le combat contre la cybercriminalité nécessite l'engagement de chacun, afin de réduire notre exposition au risque cybercriminel. Toutefois, si une entreprise subit une cyberattaque en dépit des mesures de précaution prises en interne, il convient, d'abord pour arrêter l'attaque, de limiter la surinfection du système touché en débranchant de son réseau et d'internet les machines infectées et en faisant appel à un informaticien, à une société de réponse à incidents informatiques ou à l'agence nationale de la sécurité des systèmes d'information (ANSSI), selon la taille du système touché.

Plus spécifiquement, pour assurer l'effectivité de la réponse pénale, il est fortement déconseillé de payer la rançon lorsqu'il s'agit d'une attaque par ransomware. En effet, ce paiement ne garantit pas la récupération des données, ne prémunit pas contre une nouvelle attaque, et participe au financement de l'écosystème cybercriminel. Il est également indispensable de conserver ou faire conserver les preuves par un professionnel, notamment un exemple de message piégé ou la note de rançon. Il convient, enfin, impérativement de déposer plainte auprès du service de police ou de gendarmerie territorialement compétent. Si l'attaque est massive, le parquet de Paris, qui aura été informé par le procureur initialement saisi de la procédure, pourra évoquer le dossier au titre de sa compétence concurrente nationale. »

I-3.
LE RÔLE DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DES AUTORITÉS ADMINISTRATIVES INDÉPENDANTES

■ **44.** L'ANSSI, autorité nationale de la sécurité des systèmes d'information, coordonne l'action gouvernementale en matière de protection des systèmes d'information et a renforcé les liens avec d'autres autorités administratives indépendantes telles que l'AMF, depuis **février 2018**, laquelle met en garde sur les risques, pour les marchés financiers et boursiers, de la cybercriminalité. Dans son plan stratégique **2018-2022**, L'AMF rappelle l'enjeu important qu'est devenue la cybercriminalité, ainsi que sa volonté de développer de nouvelles expertises pour y répondre.

■ **45.** Un accord du **19 janvier 2018**, conclu entre l'ANSSI et l'ACPR (Autorité de contrôle prudentiel et de résolution), prévoit également un échange régulier d'informations concernant les incidents affectant la sécurité des systèmes d'information, ainsi qu'une collaboration dans la gestion des crises éventuelles et, de façon plus générale, en matière de sécurité du numérique.

■ **46.** TRACFIN, service administratif de traitement du renseignement financier, dispose d'une cellule « cybercriminalité » dont l'activité est essentiellement consacrée aux *blockchains*, au darknet et à la pédopornographie.

SECTION II
LA COOPÉRATION POLICIÈRE ET JUDICIAIRE INTERNATIONALE

■ **47.** **La cybercriminalité, par essence mondiale et sans frontières, impose une coopération internationale.**

II-1.
LES ACTEURS AU NIVEAU EUROPÉEN ET INTERNATIONAL

■ **48.** Les États doivent établir des contacts et collaborations avec :

Au niveau européen, **Europol**, l'agence européenne spécialisée dans la répression de la criminalité, qui soutient les 27 États membres de l'Union européenne dans leur lutte contre la cybercriminalité à travers la mise en place d'un canal d'information entre elle et les États membres.

En **2013** a été créé le Centre européen de la lutte contre la cybercriminalité (EC3) pour faciliter une coopération opérationnelle et analytique européenne entre les services répressifs, le milieu universitaire et le secteur privé.

Europol a adapté, fin **2019**, sa stratégie dite « 2020+ » qui comprend plusieurs axes relatifs à la cybercriminalité : renforcement de la capacité d'analyse de l'agence, gestion de l'information, définition d'une stratégie d'innovation, création d'un laboratoire d'innovation et des technologies émergentes, qui permettra de mettre en contact des experts des services répressifs, du milieu universitaire et du secteur privé.

Le travail d'Europol a permis, en **janvier 2021**, de démanteler le réseau Safe Inet, l'un des plus importants réseaux privés virtuels du monde (VPN).

Ce réseau était utilisé par des cybercriminels, notamment pour des attaques par rançongiciel et de piratage de données de cartes bancaires. Les forces de l'ordre, sous le commandement de la police de Rentlingen, dans le sud de l'Allemagne, ont confisqué, lundi **11 janvier 2021**, ce service de VPN Safe Inet en désactivant ses serveurs actifs depuis plus d'une décennie. Safe Inet était utilisé par certains des plus grands cybercriminels au monde, responsables d'attaques par rançongiciel, de piratages de données, de cartes bancaires et d'autres formes de cybercrime.

■ **49.** Au niveau international, **Interpol** fournit une plateforme de coopération permettant aux autorités de police de travailler directement avec leurs homologues.

Par exemple, l'unité de cybercriminalité d'Interpol a adressé en **décembre 2020** un message d'avertissement à ses **194** pays membres, les appelant à se préparer à des actions du crime organisé centrées sur les vaccins contre le coronavirus. Dans une notice Orange d'alerte sécurisée, l'organisation de coopération policière internationale, basée à Lyon, avait prévenu d'une « potentielle activité criminelle liée à la contrefaçon, au vol et à la promotion illégale de vaccins contre la Covid-19 ». Aujourd'hui, les sites vendant ces faux vaccins se sont multipliés.

■ **50.** Un accord de coopération entre Interpol et Europol a été signé en **2001** et approuvé par le Conseil de l'Union européenne le **27 juin 2001**, et par l'Assemblée générale d'Interpol lors de sa 70e session qui s'est tenue à Budapest, le **26 septembre 2001**, organisant une coopération dans la lutte contre la criminalité internationale, notamment en ce qui concerne l'échange d'informations.

Et Interpol pour l'innovation (CMII), spécialisé dans la lutte contre la cybercriminalité, a été créé en **avril 2015** à Singapour et œuvre pour l'amélioration des compétences techniques des services d'enquête et le développement des outils transnationaux.

II-2.
LES TEXTES ACTUELLEMENT EN DISCUSSION

■ **51.** E-evidence

La Commission européenne a présenté, le **17 avril 2018**, un projet de règlement et de directive sur l'accès transfrontalier aux preuves électroniques en matière pénale : « E-evidence ».

Ce projet de règlement vise à faciliter l'obtention de preuves électroniques (telles que des mails ou autres documents situés dans le cloud), nécessaires pour les enquêtes menées par les autorités judiciaires. Ayant un effet d'extraterritorialité, il apparaît comme une réponse à la promulgation du « Cloud Act », en **mars 2018**.

Le projet de directive « E-evidence » pose les bases d'une coopération entre l'UE et les États Unis et constitue un modèle de coordination pour l'accès à des preuves électroniques. Elle a créé l'obligation de désignation de représentants légaux sur le territoire européen pour les personnes morales établies à l'extérieur de l'UE.

II-3.
LE 2e PROTOCOLE DE LA CONVENTION DE BUDAPEST

■ **52.** Les négociations relatives à la conclusion d'un deuxième protocole additionnel à la convention de Budapest du **27 novembre 2001** ont débuté en **juin 2017**, et devraient se conclure prochainement [59].

■ **53.** L'objectif de ce protocole est de renforcer la coopération internationale entre les **67** pays signataires, notamment en ce qui concerne l'accès aux preuves électroniques, l'amélioration de l'entraide judiciaire et l'organisation d'enquêtes communes par des mesures visant à améliorer :

- la coopération internationale entre les services répressifs et les autorités judiciaires, y compris l'entraide juridique entre les autorités ;
- la coopération entre les autorités et les fournisseurs de services dans d'autres pays ;
- les conditions et les garanties d'accès à l'information pour les autorités d'autres pays ;
- les conditions relatives à la protection des données.

59. La convention de Budapest sur la cybercriminalité est le premier traité international permettant, notamment, de nouer une coopération policière internationale pour obtenir des données détenues dans un autre pays.

FOCUS

L'ACTION INTERNATIONALE CONTRE LA CYBERCRIMINALITÉ ORGANISÉE DOIT ÊTRE PRIORITAIRE

par BERNARD BARBIER[60], JEAN-LOUIS GERGORIN[61] et ÉDOUARD GUILLAUD[62]

La France, comme les autres démocraties, est confrontée à une croissance exponentielle de la cybercriminalité organisée.

Celle-ci est fondée sur l'existence de groupes mafieux établis dans des pays parfaitement identifiés n'ayant pas ratifié la Convention de Budapest sur la cybercriminalité. Ces groupes n'ont aucune difficulté à recruter des informaticiens talentueux naturellement attirés par le core business de la grande cybercriminalité, les attaques par rançongiciel (*ransomware*), qui constituent probablement l'activité criminelle la plus rémunératrice et la moins risquée de l'histoire.

En effet, ces groupes au minimum tolérés par les autorités des pays concernés, bénéficient d'une impunité quasi totale. La conséquence en est un écosystème où les grands groupes cybercriminels, confortablement installés dans les pays sanctuaires, développent des maliciels de plus en plus sophistiqués qu'ils proposent, avec les accès *ad hoc*, sous forme de « *ransomware as a service* » aux attaquants directs.

Dans ce contexte, il n'est pas étonnant que seule une proportion infinitésimale des grands cybercriminels internationaux soit traduite en justice. Face à l'explosion de cette cyberpiraterie, nous préconisons une action internationale volontariste aux niveaux national ou européen pour inciter les États sanctuaires à mettre fin à l'impunité des groupes cybercriminels. Cette politique devrait s'accompagner d'un volet dissuasif consistant à expliciter dans la doctrine française de cyberdéfense, et à mettre en œuvre, le cas échéant, la possibilité de riposter informatiquement contre les auteurs de cyberattaques contre le potentiel économique ou de survie de la nation, comme cela est théoriquement prévu par l'article L. 2321-2 du Code de la défense. Il est intéressant de noter, à cet égard, que le Royaume-Uni a récemment créé une National Cyber Force pour riposter numériquement contre non seulement les États, mais aussi les cybercriminels s'attaquant numériquement au « *Realm* ».

60. Bernard Barbier est ancien directeur technique de la DGSE et ancien directeur du Laboratoire d'Électronique et de technologies de l'information (LETI). Il est membre de l'Académie des technologies.
61. Jean-Louis Gergorin chargé de cours à Sciences Po, ancien chef du Centre d'analyse et de prévision du Quai d'Orsay, est coauteur de « Cyber La guerre permanente » (Éditions du Cerf 2018).
62. L'amiral Édouard Guillaud est ancien chef d'État—Major des Armées. Il est membre de l'Académie de marine.

Enfin, l'explosion des cybermenaces nous paraît justifier la création, auprès du président de la République, d'un coordinateur national Cyber, à l'instar du coordinateur national du renseignement et de la lutte contre le terrorisme qui a démontré son efficacité[63].

CHAPITRE II

LA MISE EN ŒUVRE DE L'ACTION PUBLIQUE ET LES MOYENS DE PREUVE

SECTION I
LA PLAINTE

I-1.
LE DÉPÔT DE PLAINTE

■ **54.** La plainte simple est l'étape préalable à l'ouverture d'une enquête judiciaire.

Toute personne physique ou morale, ou toute organisation victime d'une cyberattaque, peut déposer plainte, que l'auteur de l'attaque soit identifié ou non. Dans ce dernier cas, la plainte est déposée contre X.

■ **55.** La majorité des infractions liées à des cyberattaques étant des délits, la plainte, pour être recevable, doit être déposée dans un délai maximum de 6 ans à compter de la date de commission des faits, mais en réalité, elle doit être déposée dans les délais les plus brefs, car en matière de cyberdélinquance, il est essentiel d'aller vite et d'être réactif.

Une plainte déposée rapidement entraîne l'ouverture d'une enquête qui, elle-même, permet la préservation des preuves, le recours à des prestataires et à des experts techniques par les enquêteurs, le déploiement d'une coopération internationale, etc.

63. *Le Monde* 5/01/2021 « La cyber coercition doit être combattue par une stratégie nationale et globale »

(i) Auprès d'un commissariat ou d'une gendarmerie

FOCUS

DÉPÔT DE PLAINTE

Pour déposer **plainte auprès des forces de l'ordre**, il suffit de se rendre au service de police ou de gendarmerie le plus proche de l'entreprise ou du lieu de constatation des faits. Pour rappel, les officiers et agents de police judiciaire ou gendarmes sont obligés de recevoir les plaintes, même si les faits ne relèvent pas de leur zone géographique de compétence. La plainte ne sera qu'exceptionnellement déposée auprès d'un service spécialisé adapté à la cyberattaque.

Au sein de ces services, des investigateurs sont généralement spécialisés dans la lutte contre la cybercriminalité et, à défaut, ils vont orienter l'entreprise vers le service spécialisé, cf. titre **I.1**.

Le représentant de l'entreprise, si possible muni d'un extrait de KBIS de moins de 3 mois et d'un pouvoir s'il n'est pas le dirigeant, va pour déposer plainte, décrire les faits constatés et évoquer, avec un maximum de précision, le mode opératoire éventuellement repéré.

Si l'entreprise dispose de ressources dédiées à la protection numérique, soit en interne, soit *via* un prestataire, il est important que ces professionnels assistent au dépôt de plainte et fournissent des éléments techniques établissant les faits. Il peut ainsi être opportun de venir accompagné du responsable de la sécurité informatique ou de la personne désignée pour la gestion de l'incident.

Les informations à produire peuvent être :

- le descriptif précis de l'incident ;
- les coordonnées de l'ensemble des intervenants ou prestataires susceptibles d'apporter des informations aux enquêteurs ;
- l'ensemble des éléments techniques qui ont pu être collectés : traces informatiques de l'attaque (exemple : logs de connexion), l'adresse précise de la ou des machines attaquées (préciser s'il s'agit d'un poste de travail professionnel, d'un mobile ou encore d'une attaque du site internet, du serveur hébergé auprès d'un fournisseur d'accès internet) ;
- les mails en lien avec l'infraction, l'organigramme de la société, la liste du personnel, les coordonnées des différents **prestataires** (hébergeur, société de sécurité).

Il est primordial, à la découverte de l'infraction, de préserver (ou faire préserver par tout prestataire, notamment un huissier de justice) toute trace de l'attaque, et notamment une copie de l'état des serveurs et réseaux.

■ **56.** Il est également possible de déposer une plainte auprès du procureur de la République du tribunal judiciaire du ressort territorial du siège social de l'entreprise par courrier **(ii)** ou en ligne **(iii)**.

(ii) Auprès du parquet du procureur de la République territorialement compétent (TC) pour enquêter sur la cyberattaque, la plainte étant formalisée par le dépôt sur place ou l'envoi d'un courrier avec AR.

Cette démarche se fait généralement par l'intermédiaire d'un avocat qui rédigera et documentera la plainte avant dépôt en main propre auprès du parquet.

Après l'enregistrement de la plainte, le procureur saisira le service d'enquête adapté.

(iii) La plainte en ligne

La loi n° **2019-222** du **23 mars 2019** de programmation et de réforme pour la justice a introduit **la possibilité de déposer une plainte simple en ligne**[64] pour certaines infractions[65].

Le 1er procureur de la République (PR) réputé compétent est celui de Nanterre (lieu de réception de la plainte en ligne). Au vu des premières investigations menées par l'OCLCTIC, le procureur de Nanterre transmettra au procureur territorialement compétent pour poursuivre l'enquête.

(iv) La plainte avec constitution de partie civile

Une plainte avec constitution de partie civile auprès du doyen des juges d'instruction pourra être déposée à l'issue de trois mois d'enquête sans effet après le dépôt d'une plainte simple (art. 85 du CPP) ou si la plainte simple a été classée sans suite.

Cela entraînera la désignation d'un juge d'instruction qui devra faire rapatrier le dossier, en prendre connaissance. Parfois, il devra attendre les réponses aux réquisitions préalablement lancées dans le cadre de l'enquête préliminaire.

64. Article 15-3-1 du Code de procédure pénale.
65. http://www.textes.justice.gouv.fr/art_pix/Article_14_Plainte_en_ligne_190324_V1.pdf

I-2.
LE TRAITEMENT DE LA PLAINTE

■ **57.** Dès le dépôt de plainte, l'infraction commise ou tentée est portée à la connaissance du procureur de la République qui apprécie la suite judiciaire à donner.

Lorsque les investigations requièrent une technicité particulière et/ou lorsque le préjudice est important, le procureur peut décider de confier l'enquête à un service spécialisé, ou que les investigations soient effectuées en collaboration avec un enquêteur spécialisé en cybercriminalité.

■ **58.** Les enquêteurs peuvent être amenés à se déplacer dans les locaux de l'entreprise et à solliciter un accès aux ordinateurs des salariés avec leur accord (notamment pour déceler une infection par *malware*), réaliser une copie des supports numériques ayant un intérêt pour l'enquête ou accéder à certains lieux ou bureaux de l'entreprise, notamment lorsque l'attaque ou l'infraction a été commise par une personne de l'entreprise ou un sous-traitant.

Ils peuvent également convoquer, pour les auditionner, des personnes qualifiées (techniciens informatiques, responsable de la sécurité des systèmes d'information…), des témoins ou éventuellement, des suspects.

I-3.
L'ENQUÊTE

■ **59.** Le Code de procédure pénale prévoit que les investigations peuvent être menées dans trois cadres juridiques qui confèrent des pouvoirs coercitifs différents aux enquêteurs :

- la flagrance, lorsque les faits sont révélés dans un temps très proche de leur réalisation ;
- l'enquête préliminaire, lorsque les conditions de la flagrance ne sont pas réunies ;
- la commission rogatoire par le magistrat, juge d'instruction qui aura été désigné).

■ **60.** Le procureur de la République et le juge d'instruction peuvent délivrer respectivement une demande d'entraide pénale internationale (DEPI), une commission rogatoire internationale pour faire des investigations à l'étranger ou une demande d'enquête européenne (DEE). Les échanges auront alors lieu notamment entre les services français, l'ANSSI, Europol, Interpol, les polices étrangères, et/ou les magistrats étrangers.

I-4.
LES SUITES JUDICIAIRES POSSIBLES DE L'ENQUÊTE

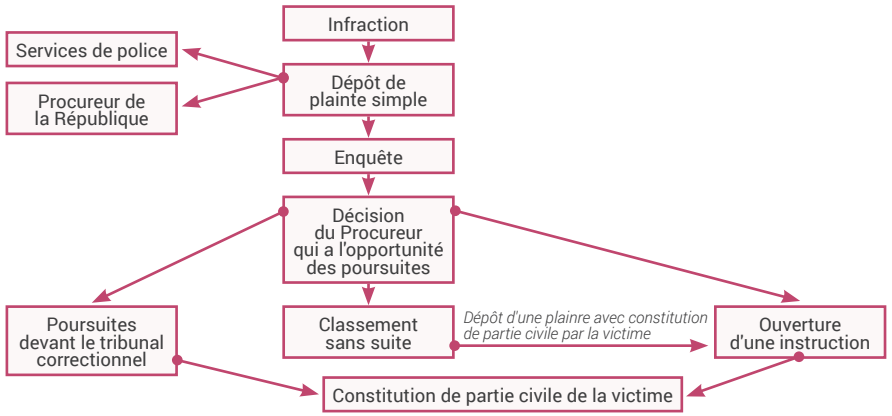
■ **61.** À l'issue des investigations, l'ensemble du dossier d'enquête est transmis au procureur de la République qui décide de l'orientation de l'affaire, car il dispose de l'opportunité des poursuites.

■ **62.** Il pourra ainsi décider :

- le **classement sans suite de l'affaire**, et ce, pour différents motifs tels que :
  - absence d'infraction (les faits ne peuvent recevoir qualification pénale)
  - infraction insuffisamment caractérisée
  - auteur non identifié
  - faits prescrits
  - motifs d'opportunité (préjudice faible et réparé, etc.) ;
- des mesures alternatives aux poursuites ;
- la **poursuite de l'auteur devant le tribunal correctionnel** ;
- l'**ouverture d'une instruction** et la désignation d'un magistrat instructeur dans les cas où la complexité, notamment technique, de l'affaire ou sa médiatisation le nécessitent.

En cas de classement sans suite, la victime peut le contester par un recours auprès du procureur général (40-3 du CPP) ou en déposant une plainte avec constitution de partie civile auprès du juge d'instruction. Cette possibilité est également offerte au plaignant si aucun acte d'enquête n'a été effectué dans un délai de trois mois ou si le procureur n'a pas pris de décision dans le même délai.

■ **63.** En cas de poursuite devant le tribunal ou d'ouverture d'une instruction, la victime pourra se constituer partie civile, simplement pour soutenir l'action publique, ou pour faire valoir une demande de dommages et intérêts.



FOCUS

ANNE SOUVIRA
Commissaire divisionnaire, ancien chargé de mission aux questions relatives à la cybercriminalité au sein du cabinet du préfet de Police de Paris ;
chef de la nouvelle Mission « Cyber » de la préfecture de Police depuis 2021 à la Direction de l'innovation, de la logistique et des technologies

Pensez-vous que les entreprises sont suffisamment informées et savent comment réagir en cas de cyberattaque ?
« Les entreprises, bien que certaines aient progressé, souvent les plus importantes, ne sont pas suffisamment informées ni préparées pour réagir en cas de cyberattaque. Elles sont encore sous-équipées techniquement en cybersécurité faute de budgets dédiés, ainsi qu'en formation/sensibilisation des dirigeants et salariés, les deux piliers techniques et humains de la cybersécurité.

Toutes sujettes aux cybermenaces, les entreprises doivent apprendre à anticiper et envisager leur réaction en fonction des types d'attaques qu'elles peuvent subir. En effet, un mail de phishing qui permet d'introduire d'un clic un ransomware chiffreurs de données qui met tout le système à plat et donc l'activité, ce n'est pas la même chose que le mail de phishing pour une escroquerie au fournisseur dans lequel il est demandé à une entreprise de changer les coordonnées du compte bancaire sur lequel doit être payée une facture, ou encore que de faux ordres de virement par une fraude dite au président toujours en vogue.

Il faut une véritable prise de conscience des entreprises, qui doivent réaliser des analyses du risque cyber (sur les données et les réseaux) et intégrer la cybersécurité dans leur business plan. Cela signifie être prêt à financer les moyens techniques, organisationnels et humains nécessaires pour anticiper et gérer l'attaque qui aura lieu. Aucun système n'est inviolable et les attaques peuvent être directes ou également indirectes en passant par des prestataires, des fournisseurs de l'entreprise ou des personnes ayant accès à l'extranet, autant de portes d'entrée pour les attaquants (NotPetya, dommage collatéral parti d'Ukraine, ou une mise à jour légitime embarquant un code modifié par des hackers telle que l'affaire Solarwinds, l'imagination est sans limite) ».

Quelles sont les informations qui vous sont le plus souvent demandées par les entreprises victimes de cyberattaques ?
« Le plus souvent, les entreprises veulent savoir auprès de qui elles doivent déposer plainte.

Pour le dépôt de plainte, c'est généralement le système des guichets uniques qui va s'appliquer, c'est-à-dire que les victimes vont s'adresser à la brigade de gendarmerie ou au commissariat qui leur convient le mieux, lequel avise le procureur de la République qui choisit le service d'enquête.

Parfois, un traitement un peu différent peut être réservé à certaines cyberattaques. Par exemple, pour les ransomwares, leur nombre est tel qu'ils ont été répartis par types entre différents services spécialisés de la police nationale (OCLCTIC et BL2C ancienne BEFTI de la préfecture de Police) et de la gendarmerie nationale (C3N). Donc, en fonction du nom du rançongiciel concerné (Egregor, Ryuk, M88P…), la plainte sera prise par le service spécialisé déjà saisi sur le même ransomware.

Le parquet près le tribunal judiciaire de Paris, section cybercriminalité (J3) à compétence concurrente nationale, procède à la répartition et suit les enquêtes.

Il est toujours possible d'adresser sa plainte directement au procureur de la République qui saisira le service d'enquête.

À noter que pour les opérateurs d'importance vitale, la section judiciaire de la DGSI sera systématiquement saisie. Les entreprises entrant dans ce cadre ont normalement un correspondant à la DGSI qui les orientera pour leur plainte. »

Selon vous, le système répressif actuel et les techniques d'enquête existants sont-ils adaptés à la lutte contre la cybercriminalité ?
« Oui, le système répressif en tant que tel est adapté à la répartition et aux attributions des forces du simple vers le plus complexe. Malgré son ancienneté, ce domaine apparaît comme récent et réservé aux techniciens. C'est plus la formation de techniciens du droit pénal spécial qui mérite d'être améliorée et promue, également auprès des magistrats. J'ai l'impression que tout le monde se fait une montagne de la matière, ce qui nuit à l'appétence et donc à son maniement.

Il y a eu du progrès puisque maintenant, il existe le pôle cybercriminalité au sein du tribunal judiciaire de Paris, qui vient d'être renforcé à trois magistrats spécialisés qu'il conviendra encore d'étoffer. La police met également à la disposition des magistrats du parquet comme du siège, des assistants spécialisés leur apportant une aide et favorisant les liaisons et le travail avec les services spécialisés ou non.

Concernant la législation et les techniques d'enquête, l'arsenal juridique existe : il comprend des techniques classiques comme les réquisitions, les perquisitions, les auditions, les transports sur les lieux, ou encore l'enquête sous pseudonyme, qui permet au fonctionnaire de police formé, qualifié et habilité, sur proposition de son directeur par le procureur général, d'aller dans le darknet pour constater des infractions commises par la voie des communications électroniques et recueillir des éléments de preuve.

La seule limite, en revanche, concerne à mon sens la conservation des données personnelles par les opérateurs de services électroniques et l'accès à la preuve numérique, qui ne sont pas stabilisés sur le plan européen après l'arrêt Télé2sverige de la CJUE interdisant la conservation des données de manière générale et indifférenciée. Seule la conservation de données ciblées pour l'avenir est possible. Cela ne permet pas aujourd'hui d'enquête de qualité, la preuve pouvant n'avoir jamais existé. On ne peut remonter la chaîne d'une donnée dont on ignore si on en aura besoin… Il ne faut pas s'attendre à des miracles. »

SECTION II
LA PREUVE ET SES LIMITES

■ **64.** En matière de preuve numérique, droit et techniques s'associent afin de garantir une efficience procédurale, conditionnée par la recherche d'un équilibre indispensable entre la préservation de la vie privée et la protection de l'ordre public.

En effet, des difficultés sont récurrentes pour obtenir une preuve numérique :

- sa localisation dématérialisée et extraterritorialisée ;
- l'absence de conservation des données ou l'utilisation de Virtual Private Networks (VPN) ou de TOR, destinés à préserver l'anonymat des utilisateurs du réseau. Ces moyens d'anonymisation, ainsi que les outils de chiffrement, obligent les enquêteurs à multiplier les actes d'enquête pour retrouver l'auteur des faits.

II-1.
LES PROCÉDURES D'ACCÈS À LA PREUVE NUMÉRIQUE

Les enquêteurs peuvent classiquement obtenir des preuves par le biais d'une réquisition **(i)**, de perquisitions et de saisies informatiques **(ii)**, ou d'une enquête sous pseudonyme **(iii)** ou encore accéder aux correspondances stockées (iv).

(i) Les réquisitions classiquement utilisées pour la recherche des preuves numériques

■ **65.** Le procureur de la République, le juge d'instruction ou, sur autorisation de ceux-ci en enquête préliminaire ou sur commission rogatoire, l'officier de police judiciaire et, sous son contrôle, l'agent de PJ, peuvent ainsi requérir de toute entreprise qui détient des documents liés à l'enquête de lui remettre des données, ou de conserver des données de contenus, y compris de ceux issus d'un système informatique ou d'un traitement de données normatives (articles 60-1 et 60-2, 77-1-1, 77-1-2, 99-3 et 99-4 du Code de procédure pénale).

Les réquisitions permettent d'obtenir les données de souscription, de connexion et parfois de contenus consultés, qui sont souvent des informations déclaratives, financières et techniques adressées aux opérateurs de télécommunications ou à des sociétés (identité, domicile, numéro de téléphone, moyens de paiement), ainsi que des données permettant d'identifier un système de traitement automatisé de données en particulier, tel un ordinateur, et sa localisation.

(ii) Les perquisitions et les saisies informatiques de données

■ **66.** Les officiers de police judiciaire effectuant une perquisition peuvent, dans le cadre de l'enquête de flagrance prévue par l'article 57-1 du Code de procédure pénale, accéder, par un système informatique implanté, dans les lieux où se déroule la perquisition, ou à partir de leur bureau, aux données intéressant l'enquête et qui sont stockées sur ce système ou sur un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

La perquisition permet alors l'accès aux données stockées sur l'ordinateur ou, sous réserve qu'on ne sache pas préalablement que les données sont situées à l'étranger, aux données se trouvant en ligne ou sur un autre ordinateur, à la condition qu'elles soient accessibles à partir de l'ordinateur perquisitionné.

■ **67.** La loi n° 2014-1353 du 13 novembre 2014, relative à la lutte contre le terrorisme, a étendu les prérogatives des enquêteurs en ajoutant la possibilité d'accéder, par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie, à des données intéressant l'enquête en cours et stockées dans un autre système informatique.

■ **68.** L'ensemble de ces dispositions est également applicable à tous les cadres d'enquête.

■ **69.** Les données recueillies originales sont placées sous main de justice après avoir éventuellement été copiées sur tout support, lequel peut faire l'objet d'un placement sous scellé après analyse par les enquêteurs spécialisés ou un expert. Préservant l'intégrité des données originales, le scellé garantit l'authenticité et le caractère inaltéré des données analysées. Une nouvelle copie des

données originales permettra, en outre, la réalisation d'une contre-expertise en cas de contestation de la validité des éléments de preuves obtenus.

(iii) L'enquête sous pseudonyme

■ **70.** En application de l'article 230-46 du Code de procédure pénale issu de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, cette procédure est désormais applicable aux infractions d'atteintes aux systèmes de traitement automatisé de données et limitée *« aux seules fins de constater les crimes et les délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques »*.

Cette enquête permet de réaliser les actes suivants :

- *« participer sous un pseudonyme aux échanges électroniques »*,
- être en contact, par la voie électronique, avec les suspects des infractions,
- extraire ou conserver, par cette voie, les éléments de preuve et données sur les suspects,
- acquérir tout contenu, produit, substance, prélèvement ou service, y compris illicite,
- transmettre une réponse en demande expresse à des contenus illicites.

■ **71.** L'enquête sous pseudonyme ne doit pas, à peine de nullité, constituer une incitation à la commission d'infractions.

(iv) L'accès aux correspondances stockées

■ **72.** Jusqu'à la loi n° 2019-222 du 23 mars 2019, l'accès aux correspondances stockées était **limité à la délinquance et à la criminalité organisées**. Le législateur permettait au parquet, avec l'autorisation préalable du juge des libertés et de la détention, et au juge d'instruction, de récupérer, à distance et à l'insu de la personne visée, les correspondances électroniques stockées et accessibles au moyen d'un identifiant informatique[66].

■ **73.** Le législateur a **étendu le champ d'application** des articles 706-95-1 et 706-95-2 du Code de procédure pénale à **tous les crimes**.

66. Circulaire du 2 décembre 2016 de présentation des dispositions de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relative au renforcement du dispositif en matière de lutte contre la délinquance et la criminalité organisées NOR : JUSD1635582C

C'est ainsi que le juge des libertés et de la détention (art. 706-95-1 CPP) ou le juge d'instruction (art. 706-95-2 CPP), ou l'officier de police judiciaire peut autoriser l'accès, à distance et à l'insu de la personne visée, aux correspondances électroniques stockées pour tout type de crime.

II-2. LA CONSERVATION DES DONNÉES PAR LES OPÉRATEURS

■ **74.** L'obligation de conservation des données, imposée en France pendant un an aux opérateurs de télécommunication, constitue un moyen d'obtenir des éléments de preuve. Toutefois, les règles de conservation des données numériques varient en fonction de la législation des États, ce qui rend chaotique la coopération internationale.

■ **75.** La directive 2006/24 du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, prévoit une durée minimale de conservation des données de 6 mois.

L'article 15 de cette directive prévoit que les États membres peuvent adopter des mesures limitant les droits et obligations prévus par la directive *« lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour […] assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales »*.

■ **76.** La marge de manœuvre laissée par les textes européens aux États membres a pour effet des approches diverses en matière de conservation des données.

S'agissant de la législation française, la durée de conservation des données techniques est fixée à un an[67].

■ **77.** Certains États ne prévoient une durée de conservation que de quelques semaines, et ce, pour protéger les données personnelles de leurs citoyens, au détriment des procédures et donc des victimes.

Étant précisé que par un arrêt du 8 avril 2014 « Digital Rights Ireland », la cour de justice semble ôter toute portée normative à l'article 15 puisqu'elle a jugé qu'une législation prévoyant *« la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits » ne* pouvait être justifiée que par la lutte

67. Article L. 34-1, III du Code des postes et des communications électroniques.

contre la criminalité grave et donc, pour l'avenir, personne ne pouvant savoir qu'il aura besoin de telles ou telles données, et pour une infraction grave pas encore connue…

■ **78.** Ainsi, cet arrêt révèle l'insécurité juridique en matière de durée de conservation des données puisque sa portée est interprétée différemment par les législations des États membres.

■ **79.** Aux États-Unis, il n'existe pas d'obligation générale de conservation minimale des données pour une utilisation éventuelle par les services de police ou de justice.

Malgré les coopérations du groupe de contact permanent entre le ministère de l'Intérieur, de la Justice et les divers opérateurs de ces services, le traitement des demandes (liées par exemple aux GAFAM Google, Amazon, Facebook, Apple, Microsoft), adressées par les autorités judiciaires françaises aux autorités judiciaires américaines, prennent parfois plusieurs semaines, hormis en cas d'urgence vitale, et peuvent ne pas aboutir, notamment lorsque la liberté d'expression, moins restrictive que l'analyse juridique de la France, est en jeu.

II-3.
LES MOYENS D'ACCÈS AUX DONNÉES CHIFFRÉES

Les autorités judiciaires peuvent requérir de toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition. Ces dispositions, introduites en 2014, permettent également aux enquêteurs de **demander à des tiers, détenteurs des codes verrouillant l'accès au contenu informatique**, de leur remettre les informations permettant d'accéder à ces données. Cela s'inscrit dans le but de parer à l'absence du détenteur d'un contenu informatique ou à son refus de fournir ces codes.

Sur ce point, il est intéressant de rappeler que l'article 434-15-2 du Code pénal sanctionne de 3 ans d'emprisonnement et de **270 000 €** d'amende *« le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de la remettre aux autorités judiciaires ou de la mettre en œuvre »*, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du Code de procédure pénale.

En pratique, il s'avère que cette infraction est parfois retenue en cas de refus des personnes interpellées de donner le code d'accès de leur téléphone portable. Cette interprétation de l'article 434-15-2 du Code pénal apparaît en l'état erronée et a conduit à l'annulation de plusieurs procédures. En effet, l'infraction vise les moyens de cryptologie comme certaines applications (Signal ou Telegram, par ex., L. n° 2004-575, 21 juin 2004, art. 29), ce que n'est pas un code d'accès à un téléphone, qui correspond à un mécanisme d'authentification et non de cryptologie. Le droit se heurte, en ce domaine, à la technique qui est particulièrement évolutive et constitue donc une source d'insécurité juridique.

■ **80.** **En outre, le recours à des experts judiciaires** est prévu par le Code de procédure pénale qui permet aux autorités judiciaires, aux fins de *« mettre au clair des données chiffrées »,* de recourir à une **expertise « externe »** pour effectuer les opérations techniques permettant l'accès à des données chiffrées, à leur version en clair ou à la convention secrète de déchiffrement.

Par exemple, il s'agit de faire appel à un « expert en chiffrement », afin de « déchiffrer » des informations en leur disposition.

PARTIE III

10 PRÉCONISATIONS POUR FAIRE AVANCER LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Les préconisations suivantes visent, après celles concernant l'assurance cyber objet du tome I, à améliorer le traitement juridique des cyberattaques qui doivent faire l'objet d'une réponse judiciaire globale et transversale.

FOCUS

QUELLES ÉVOLUTIONS EN MATIÈRE D'ASSURANCE DU RISQUE CYBER DEPUIS LA PUBLICATION DU TOME I DE CE RAPPORT, EN JANVIER 2018 ?

CHRISTOPHE DELCAMP
Directeur adjoint des assurances de biens et responsabilité à la FFA

Les évolutions récentes liées aux risques cyber démontrent toute la pertinence de traiter de manière pluridisciplinaire ce risque. Cette méthode de travail avait permis au tome I du rapport du Club des juristes, dédié à l'assurance cyber, de poser les enjeux clés de l'assurabilité de ces risques.

Trois ans après, où en sommes-nous ?

Le contexte de l'assurance cyber a évolué de manière positive, mais n'a pas encore dissipé toutes les menaces qui pèsent sur son développement.

Le 12 novembre 2019, l'ACPR a publié un communiqué de presse attirant l'attention des assureurs sur l'insuffisance de la mesure de leur exposition à ce risque, notamment au travers des garanties implicites contenues dans les contrats de RC et de dommages aux biens. Les préconisations 2 et 6 du tome I avaient anticipé ce sujet. Depuis lors, les principaux assureurs ont effectué un travail en profondeur d'analyse de leur exposition à ce risque. Il appartiendra à chaque assureur de faire évoluer ou non son offre sur la base de ce travail.

Le 7 juin 2019 le Conseil de l'Union européenne a adopté le règlement européen « Cybersecurity Act ». Ce règlement vise le renforcement de l'Agence européenne pour la cybersécurité (ENISA) et la mise en place d'un cadre unique européen de certification de cybersécurité.

Le 18 février 2021, Cybermalveillance.gouv.fr a annoncé le lancement du label ExpertCyber. Ce label permet aux TPE/PME/Collectivités d'identifier rapidement un prestataire informatique reconnu en matière d'accompagnement des victimes dans les domaines des sites internet et de systèmes d'information des professionnels.

Les préconisations 4 et 7 appelaient de leurs vœux cet encadrement technique, tant à destination des grandes entreprises que de plus petites structures à un niveau européen et national, afin de permettre d'infuser auprès de tous les acteurs économiques de vrais outils de prévention et remédiation.

Le 18 février 2021, le président de la République, Emmanuel Macron, a présenté un plan de 1 milliard d'euros d'ici à 2025, visant à renforcer la cybersécurité du pay, dont 720 millions de financements publics.

La préconisation 10 soulignait la nécessité d'orienter les plans d'investissements publics pour favoriser le développement de filières d'excellence dans le domaine de la cybertechnologie, seule manière d'anticiper les défis futurs et de ne pas être distancé par d'autres pays.

Le 16 juillet 2019, Michel Van Den Berghe, directeur général d'Orange Cyberdefense, recevait sa lettre de mission du Premier ministre Édouard Philippe, pour mettre en place un campus cyber en France. Dans son rapport de janvier 2020, Michel Van den Berghe identifiait le partage de la donnée comme un des défis que ce campus devait relever.

La préconisation 5 mettait en exergue ce besoin de partage de la donnée pour les assureurs.

Si ces mesures participent à une évolution positive de l'assurabilité de ces risques, de nombreuses menaces pèsent encore sur le bon transfert de ces risques aux assureurs.

La conjonction de la survenance de la crise de la Covid-19, de la multiplication des attaques d'ampleur, et de graves sinistres affectant les sites de stockage de données (Solarwinds en décembre 2020, Microsoft Exchange et OVHCloud en mars 2021), font craindre « qu'une pandémie » puisse affecter les systèmes d'information.

L'absence d'éclaircissement sur l'assurabilité des rançons et des amendes administratives, déjà identifiée dans le tome I, ne permet pas la transparence nécessaire auprès des acheteurs d'assurance.

Le manque de culture du risque cyber des TPE/PME/collectivités locales, mais également de professionnels de l'assurance, ne permet pas une prise de conscience salutaire pour développer la prévention contre ces risques et leur transfert auprès des assureurs.

L'année 2021 sera marquée par la course entre le temps court des renouvellements annuels des contrats d'assurance et de réassurance et le temps long de la mise en place des fondations au bon traitement de ces nouveaux risques.

PRÉCONISATIONS À L'ATTENTION DU GOUVERNEMENT

PRÉCONISATION 1 :

Faire de la lutte contre la cybercriminalité une cause nationale pour 2022

- Lancer des campagnes récurrentes d'information et de sensibilisation ciblées par le biais des médias et réseaux sociaux, notamment avec le soutien des chambres de commerce, des compagnies et ordres professionnels.
- Conclure un protocole entre le ministère de la Justice et la plateforme Cybermalveillance.gouv.fr à cet effet.

PRÉCONISATIONS À L'ATTENTION DU MINISTÈRE DE LA JUSTICE

PRÉCONISATION 2 :

Promouvoir la spécialisation des magistrats du siège et du parquet et leur formation continue

- Créer une filière de cybermagistrats, au besoin par le biais d'une formation diplômante (DU Cyber, par exemple).
- Renforcer le pôle Cyber au niveau du parquet de Paris.
- Renforcer la spécialisation d'une chambre du tribunal judiciaire en matière de droit du numérique et cybercriminalité.
- Créer un département Numérique et Cyber au niveau de la cour d'appel de Paris, composé de magistrats du siège et du parquet.
- Accentuer les formations communes ENM/EFB et PN/GN/Douanes sur le droit du numérique et la lutte contre la cybercriminalité, avec des stages pratiques dans les services spécialisés.
- Désigner un référent cyber par cour d'appel en actualisant régulièrement la liste.

PRÉCONISATION 3 :

Renforcer la coopération public/privé et orienter l'investissement public et privé vers l'émergence d'une filière française et européenne d'excellence en cybertechnologie

- Les plans d'investissements publics français et européens devraient favoriser le développement d'une filière européenne d'excellence dans le domaine de la cyberprotection et accompagner les efforts du marché en faveur d'une réduction de la menace cyber.

  Cette recommandation, déjà formulée dans le tome I, est également valable pour le traitement juridique de la menace cyber puisqu'elle vise à la réduire.

  Elle vise également, afin d'éviter leur expatriation, à aider les chercheurs à devenir des entrepreneurs dans la lignée du campus cyber et des investissements du « *défi cyber William Levat* ».

PRÉCONISATION 4 :

Étoffer les services de la justice en matière de lutte contre la cybercriminalité

- Recruter des cadres et assistants spécialisés en matière de cybersécurité, tant au niveau du tribunal judiciaire que de la cour d'appel de Paris.
- Développer des échanges réguliers avec les compagnies des experts judiciaires.
- Revoir la nomenclature des experts judiciaires, afin d'introduire une spécialité sur le numérique et la cybersécurité.
- Signer des protocoles Justice/Barreau/Intérieur sur ces problématiques de cybersécurité et cybercriminalité, et prévoir le partage d'informations entre chaque responsable.

PRÉCONISATION 5 :

Simplifier les procédures d'enquête sous pseudonyme dans le « darknet »

- Donner des moyens réalistes aux enquêteurs qui doivent les mener.

PRÉCONISATIONS À L'ATTENTION DES INSTANCES EUROPÉENNES

PRÉCONISATION 6 :

Adoption d'un régime européen de conservation des données permettant de répondre aux besoins opérationnels des services répressifs et judiciaires

- Ce régime devra prévoir de permettre les enquêtes par la prise en compte de données conservées un an au plus.

PRÉCONISATIONS À L'ATTENTION DE L'ANSSI

PRÉCONISATION 7 :

Inciter les États sanctuaires à mettre fin à l'impunité des groupes cybercriminels

- L'objectif est de mettre un terme à l'installation confortable des grands groupes cybercriminels dans les pays sanctuaires en développant la solidarité entre les États pour obliger les États sanctuaires à prendre les mesures juridiques et économiques à cette fin.

PRÉCONISATION 8 :

Signature de protocoles avec l'ensemble des agences et autorités administratives indépendantes concernées

- Cette préconisation vise toutes les agences et autorités administratives indépendantes, afin de les inciter à systématiser les procédures de signalement.

  Cette préconisation est en lien avec la préconisation 5 du tome I : mutualiser les données résultant d'incidents cyber et avec la création du campus cyber.

PRÉCONISATIONS À L'ATTENTION DES ENTREPRISES

PRÉCONISATION 9 :

Investir dans la prévention contre les cyberattaques

- Ces investissements s'intègrent dans le cadre du dispositif de gestion globale des risques.

  Ils doivent être humains (par exemple, formation à la cybersécurité), techniques (investissement dans des logiciels, outils de sauvegarde, audits, etc.), organisationnels (mise en place d'une cybergouvernance) et assurantiels.

PRÉCONISATION 10 :

En cas de cyberattaque, déposer immédiatement plainte

- La plainte permet à tous les services mentionnés dans le livret d'être saisis et de pouvoir remonter les filières, notamment pour démanteler les réseaux.

> *« Ces 10 propositions concrètes, qui visent à renforcer la protection des entreprises et des citoyens, sont autant d'instruments supplémentaires au service des libertés. Elles sont aussi les conditions, pour la France, de disposer des atouts essentiels de compétitivité et de souveraineté de notre pays dans le contexte des développements technologiques engagés au XXIe siècle sur la voie du digital et de l'intelligence artificielle. Il est rare que des enjeux d'une telle importance ne requièrent pas des investissements hors de portée. Ces propositions sont à notre portée sur le plan financier. Il leur reste à pouvoir s'appuyer sur une réelle volonté politique. »*
>
> **Bernard Spitz**

COMPOSITION DE LA COMMISSION

■ PRÉSIDENT :

Bernard Spitz, président du pôle International et Europe du MEDEF, ancien président de la Fédération française de l'assurance (FFA)

■ SECRÉTAIRE GÉNÉRALE :

Valérie Lafarge-Sarkozy, avocate associée, cabinet Altana

■ MEMBRES :

Nicolas Arpagian, VP Strategy & Public Affairs, Orange Cyberdefense

Brigitte Bouquot, ancienne présidente de l'Association pour le management des risques et des assurances de l'entreprise (AMRAE), VP scientifique

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense, Airbus Defence and Space, Administrateur de l'AMRAE, président de la commission Systèmes d'information

Christophe Delcamp, directeur adjoint des assurances de dommages et responsabilité, FFA

Émilie Dumérain, déléguée juridique, Syntec Numérique

Agathe Lepage, professeur, université Panthéon-Assas (Paris II)

Charles-Henry Madinier, Director of Consulting Solutions, Marsh Advisory

Alexandre Menais, Executive Vice President and Group Head of M&A, Strategy & Development, Atos

Séverine Oger, chargée de mission / état-major de la sous-direction Opérations, ANSSI

Martin Pailhes, responsable de l'équipe juridique « Information Technology – Intellectual Property », BNP Paribas

Christian Poyau, président Micropole, président de la commission Transformation numérique du MEDEF

Myriam Quéméner, avocat général près la cour d'appel de Paris

Anne Souvira, commissaire divisionnaire, chargée de mission aux questions relatives à la cybercriminalité au sein du cabinet du préfet de police de Paris

François Weil, conseiller d'État

Leigh Wolfrom, Policy analyst, Directorate for Financial and Entreprise Affairs, OCDE

■ ONT CONTRIBUÉ À LA RÉDACTION :

Valérie Lafarge-Sarkozy, avocate associée, cabinet Altana

Myriam Quéméner, avocat général près la cour d'appel de Paris

Anne Souvira, commissaire divisionnaire, chargée de mission aux questions relatives à la cybercriminalité au sein du cabinet du préfet de police de Paris

Laetitia Daage, avocate counsel, cabinet Altana

■ AVEC LES INTERVIEWS ET PARTICIPATIONS DE :

Nicolas Arpagian, VP Strategy & Public Affairs, Orange Cyberdefense

Bernard Barbier, ancien directeur technique de la DGSE – membre de l'Académie des technologies,

Mariette Bormann, directrice du pôle Juridique, Conformité, Fiscal, Distribution de la FFA (Fédération française de l'assurance)

Brigitte Bouquot, ancienne présidente de l'Association pour le management des risques et des assurances de l'entreprise (AMRAE), VP scientifique

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense, Airbus Defence and Space, Administrateur de l'AMRAE, président de la commission Systèmes d'information

Christophe Delcamp, directeur adjoint des assurances de dommages et responsabilité, FFA

Jean-Louis Gergorin, ancien chef du centre d'analyse et de prévision du Quai d'Orsay,

Paul-Alexandre Gillot, chef du département enquête du C3N Amiral

Édouard Guillaud, ancien chef d'état-major des armées – membre de l'Académie de marine

Rémy Heitz, procureur de la République près le tribunal judiciaire de Paris

Agathe Lepage, professeur université Panthéon-Assas (Paris II)

Fabienne Lopez, colonelle, cheffe du C3N

Haritini Matsopoulou, professeur, université Paris-Sud

Séverine Oger, chargée de mission / état-major de la sous-direction Opérations, ANSSI

Guillaume Poupard, directeur général de l'ANSSI

Élisabeth Rolin, conseiller juridique à la Gendarmerie nationale

le club
des juristes

4, rue de la Planche 75007 Paris
Tél. : 01 53 63 40 04

leclubdesjuristes.com

RETROUVEZ-NOUS SUR