N° 613

SÉNAT

SESSION EXTRAORDINAIRE DE 2019-2020

Enregistré à la Présidence du Sénat le 9 juillet 2020

RAPPORT D'INFORMATION

FAIT

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) et de la commission des affaires européennes (2) sur la **lutte contre** *la* **cybercriminalité**,

Par Mme Sophie JOISSAINS et M. Jacques BIGOT,

Sénateurs.

(1) Cette commission est composée de : M. Philippe Bas, *président ;* MM. François-Noël Buffet, Jean-Pierre Sueur, Mme Catherine Di Folco, MM. Jacques Bigot, André Reichardt, Mme Sophie Joissains, M. Arnaud de Belenet, Mme Nathalie Delattre, MM. Pierre-Yves Collombat, Alain Marc, *vice-présidents ;* M. Christophe-André Frassa, Mme Laurence Harribey, M. Loïc Hervé, Mme Marie Mercier, *secrétaires ;* Mmes Catherine André, Esther Benbassa, MM. François Bonhomme, Philippe Bonnecarrère, Mmes Agnès Canayer, Maryse Carrère, Josiane Costes, MM. Mathieu Darnaud, Marc-Philippe Daubresse, Mme Jacky Deromedi, MM. Yves Détraigne, Jérôme Durain, Mme Jacqueline Eustache-Brinio, MM. Jean-Luc Fichet, Pierre Frogier, Mmes Françoise Gatel, Marie-Pierre de la Gontrie, M. François Grosdidier, Mme Muriel Jourda, MM. Patrick Kanner, Éric Kerrouche, Jean-Yves Leconte, Henri Leroy, Mme Brigitte Lherbier, MM. Didier Marie, Hervé Marseille, Jean Louis Masson, Thani Mohamed Soilihi, Alain Richard, Simon Sutour, Mmes Lana Tetuanui, Claudine Thomas, Catherine Troendlé, M. Dany Wattebled.

(2) Cette commission est composée de : M. Jean Bizet, *président ;* MM. Philippe Bonnecarrère, André Gattolin, Didier Marie, Mme Colette Mélot, MM. Cyril Pellevat, André Reichardt, Simon Sutour, Mme Véronique Guillotin, MM. Pierre Ouzoulias, Jean-François Rapin, *vice-présidents ;* M. Benoît Huré, Mme Gisèle Jourda, MM. Pierre Médevielle, René Danesi, *secrétaires ;* MM. Pascal Allizard, Jacques Bigot, Yannick Botrel, Pierre Cuypers, Mme Nicole Duranton, M. Christophe-André Frassa, Mme Joëlle Garriaud-Maylam, M. Daniel Gremillet, Mmes Pascale Gruny, Laurence Harribey, MM. Claude Haut, Olivier Henno, Mmes Sophie Joissains, Mireille Jouve, Claudine Kauffmann, MM. Guy-Dominique Kennel, Claude Kern, Pierre Laurent, Jean-Yves Leconte, Jean-Pierre Leleux, Mme Anne-Catherine Loisier, MM. Franck Menonville, Jean-Jacques Panunzi, Michel Raison, Claude Raynal, Mme Sylvie Robert.

SOMMAIRE

Pages

L'ESSENTIEL

En mai 2019, les rapporteurs ont présenté un rapport d'information sur la coopération judiciaire en matière pénale et la mise en œuvre du Parquet européen[1] et ont pris l'initiative d'une proposition de résolution européenne sur ce sujet[2]. À cette occasion, ils ont pu se rendre compte combien **le Parquet européen constituait une avancée conceptuelle majeure**, permettant à l'Union européenne de conduire des enquêtes pénales transfrontières, et illustrant par conséquent un fonctionnement beaucoup plus intégré de la coopération judiciaire, **mais n'exercerait qu'une compétence limitée**, réduite aux infractions portant atteinte aux intérêts financiers de l'Union européenne.

Par ailleurs, en leur qualité de représentants du Sénat au sein du Groupe de contrôle parlementaire conjoint d'Europol[3], ils ont été marqués, lors de l'une des réunions semestrielles de ce Groupe, par l'**importance croissante que prend la cybercriminalité dans le paysage des menaces qui affectent l'Union européenne et ses États membres**, ce qui conduit Europol et les services répressifs nationaux à renforcer sans cesse leurs réponses.

Les rapporteurs ont dès lors souhaité étudier plus avant la façon dont la France s'est organisée pour réduire ce risque informatique, y compris dans un cadre européen, voire plus large, et dans ses relations avec les autres États membres, et **engager une réflexion sur la façon dont l'Union européenne pourrait davantage aider les États membres à poursuivre les cybercriminels, le cas échéant, en mobilisant ce nouvel outil de coopération judiciaire qu'est le Parquet européen**. **Traiter de la cybercriminalité conduit logiquement à s'intéresser aussi à la cybersécurité**, c'est-à-dire à la façon de sécuriser les systèmes informatiques. La France est d'ailleurs pionnière en Europe dans ce domaine, en particulier grâce à l'action de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au Secrétariat général de la défense et de la sécurité nationale.

Cette double approche, nationale et européenne, a conduit les rapporteurs à travailler à la fois au nom de la commission des lois et de la commission des affaires européennes, dont ils sont tous deux membres.

---

[1] *Rapport d'information n° 509 (2018-2019) du 16 mai 2019.*

[2] *Devenue la résolution européenne n° 117 (2018-2019) du 21 juin 2019.*

[3] *Établi par l'article 51 du règlement de 2016 réformant le mandat d'Europol, en application de l'article 88 du traité sur le fonctionnement de l'Union européenne, le groupe de contrôle parlementaire conjoint assure le contrôle politique des activités d'Europol dans l'accomplissement de sa mission, y compris en ce qui concerne leur incidence sur les libertés et les droits fondamentaux des personnes physiques.*

Compte tenu du contexte marqué par la crise sanitaire occasionnée par la pandémie de Covid-19, ils ont mené l'intégralité de leurs travaux par audioconférences. Au cours de 15 auditions à distance, ils ont entendu 22 personnes, à la fois des acteurs nationaux et européens, publics et privés.

La cybercriminalité – les juristes préfèrent le terme de cyberdélinquance – **recouvre une réalité protéiforme et mal cernée**. Il n'existe en effet **aucune définition conventionnelle ou légale unanimement admise** de la cybercriminalité. Celle-ci peut se concevoir comme toute action illégale dont l'objet est de perpétrer des infractions pénales sur ou au moyen d'un système informatique interconnecté à un réseau de télécommunications.

La cybercriminalité vise :

- soit des infractions spécifiques à Internet, pour lesquelles les technologies de l'information et de la communication sont l'objet même du délit, par exemple les atteintes aux systèmes de traitements automatisés des données, les infractions en matière de fichiers ou de traitement informatique ou encore le domaine de la cryptologie : il s'agit d'**infractions nouvelles spécifiques à Internet**, relevant du piratage informatique, c'est-à-dire l'intrusion non autorisée dans les systèmes informatiques et le sabotage informatique de ceux-ci ;

- soit des infractions de droit commun dont Internet permet la commission : il s'agit dans ce cas de formes traditionnelles de criminalité ou d'infractions de droit commun préexistant à Internet, mais qui se sont développées grâce à lui, la pédopornographie par exemple.

Quoique non définie, la cybercriminalité présente toutefois plusieurs caractéristiques : il s'agit d'une **criminalité organisée, mondialisée et transnationale par nature**. Non seulement, les frontières n'arrêtent pas les cyberdélinquants, mais elles leur permettent d'échapper aux poursuites.

La menace que constitue aujourd'hui la cybercriminalité devrait encore s'accentuer dans les années à venir. La numérisation croissante de l'économie et de la société multiplie les opportunités de cybercrimes – on l'a vu récemment lors de la crise sanitaire qui a été propice à de nombreuses cyberattaques[1]. Et les derniers développements technologiques vont mettre la cybersécurité sous une pression encore plus forte. C'est le cas de la 5G. Celle-ci va engendrer des millions de connexions supplémentaires, des objets domestiques les plus simples, tels que le grille-pain, aux systèmes critiques les plus complexes tels que ceux du secteur aérospatial. Les potentialités de cyberattaques vont donc croître de façon exponentielle. L'enjeu de sécurité des réseaux informatiques sera d'autant plus stratégique.

---

[1] *Sur ce point, voir le rapport d'information n° 502 (2019-2020) du 10 juin 2020 sur le suivi de la cybermenace pendant la crise sanitaire, établi par Olivier Cadic et Rachel Mazuir, au nom de la commission des affaires étrangères, de la défense et des forces armées.*

Face à ce phénomène transnational, l'efficacité de la lutte contre la cybercriminalité exige une coopération européenne, voire internationale poussée. L'Union européenne s'est progressivement dotée d'un dispositif d'ensemble pour lutter contre la cyberdélinquance, qui repose sur une réglementation applicable par les États membres, et qui mobilise l'action de différentes agences telles qu'Europol, Eurojust et l'ENISA. **Afin de compléter ce dispositif, et pour le rendre plus efficace, une réflexion est nécessaire sur le rôle que pourrait jouer le Parquet européen dans la poursuite des cybercriminels.**

À l'issue de leurs investigations, les rapporteurs ont présenté une proposition de résolution européenne afin que le Sénat prenne une position politique sur ce sujet important qui prendra une place croissante à l'avenir.

Liste des principales recommandations

• Mieux connaître le phénomène de la cybercriminalité en modernisant les outils statistiques de la police et de la justice et en encourageant les signalements et dépôts de plainte

• Renforcer les moyens des services enquêteurs spécialisés dans la lutte contre la cybercriminalité

• Augmenter considérablement les moyens de la section du parquet de Paris spécialisée dans la lutte contre la cybercriminalité et consolider le réseau de référents cyber dans les parquets locaux

• Approfondir les liens entre les services enquêteurs, l'autorité judiciaire et les acteurs privés du numérique afin de favoriser une meilleure connaissance mutuelle et de faciliter les investigations

• Sensibiliser l'opinion publique, et notamment les plus jeunes, aux enjeux de la cybersécurité, grâce à des campagnes d'information et en mobilisant l'éducation nationale

• Élaborer dans les meilleurs délais un cadre réglementaire européen relatif à la preuve numérique (durée de conservation des données, accès aux preuves hébergées à l'étranger) compatible avec les règles relatives à la protection des données personnelles

• Inviter l'ensemble des États membres de l'Union européenne à utiliser pleinement les outils de coopération policière et judiciaire Europol et Eurojust et renforcer l'implication d'Europol dans la lutte contre la cybercriminalité par de nouveaux outils techniques et par la création d'un laboratoire d'innovation

• Inciter l'ensemble des États membres à ratifier la convention de Budapest sur la cybercriminalité et conclure les négociations sur le deuxième protocole additionnel à cette convention afin de rendre l'entraide judiciaire internationale plus efficace

• Veiller à ce que le futur partenariat entre l'Union européenne et le Royaume-Uni instaure une coopération étroite dans les domaines de la cybersécurité et de la lutte contre la cybercriminalité

• Poursuivre la réflexion sur un éventuel élargissement, à long terme, des compétences du Parquet européen à la lutte contre la cybercriminalité

I. LA CYBERCRIMINALITÉ, UNE DÉLINQUANCE PROTÉIFORME ET EN EXPANSION

Le numérique étant devenu omniprésent dans la vie économique et dans la vie quotidienne des Français, nul ne saurait se considérer comme étant à l'abri de la cybercriminalité, qui revêt des formes variées.

A. LES MULTIPLES VISAGES DE LA CYBERCRIMINALITÉ

Sans prétendre à l'exhaustivité, les rapporteurs ont souhaité pouvoir illustrer la diversité des infractions relevant de la cybercriminalité, en insistant sur les tendances émergentes. Beaucoup d'infractions sont désignées par des termes anglais difficilement traduisibles, ce qui atteste du caractère international et évolutif de cette criminalité.

1. Les tentatives d'extorsion

Une première évolution préoccupante consiste dans la diffusion des « rançongiciels » (ou *ransomware*), que les cybercriminels utilisent pour pirater un ordinateur afin d'exiger le versement d'une rançon.

En pratique, le pirate informatique introduit un virus dans un ordinateur pour prendre le contrôle du système informatique et chiffrer l'ensemble des données, qui deviennent inexploitables ; la victime doit verser une rançon pour retrouver la maîtrise de son système informatique. Une autre variété de rançongiciels, dits «*locker*», ne chiffre pas les fichiers, mais empêche la victime d'accéder à son ordinateur ; le cybercriminel demande alors une rançon pour déverrouiller l'appareil.

Parmi les rançongiciels qui ont eu le plus fort impact ces dernières années, on peut citer : *CryptoLocker*, apparu pour la première fois en 2007 et qui s'est propagé *via* des pièces jointes infectées, jusqu'à contaminer 500 000 ordinateurs à travers le monde ; *Petya*, apparu pour la première fois en 2016, et qui a ressurgi en 2017 sous le nom de *GoldenEye* : il s'est répandu dans les services de ressources humaines des entreprises, *via* un courriel de candidature factice contenant un lien infecté, pour chiffrer l'ensemble du disque dur de la victime ; *Jigsaw*, apparu en 2016, qui supprimait progressivement les fichiers de la victime jusqu'à ce que la rançon soit payée ; ou encore *WannaCry*, qui s'est répandu dans 150 pays en 2017 grâce à l'exploitation d'une vulnérabilité dans *Windows*.

Une autre pratique en vogue est désignée sous le terme de « sextorsion » : une fenêtre affiche sur l'écran de l'ordinateur un message indiquant que le pirate a enregistré des images intimes de la victime pendant qu'elle visionnait un film pornographique et qu'il va les diffuser si une

rançon ne lui est pas versée. Ce type d'attaque a connu un nouvel essor à partir de 2018 dans le sillage de la diffusion du rançongiciel *GandCrab*.

Les victimes font parfois l'objet de tentatives d'extorsion sans que leur système informatique ait été paralysé, par exemple si des données confidentielles leur ont été volées et que le pirate menace de les divulguer ; ou encore si le délinquant menace de diffuser sur les réseaux sociaux des images intimes échangées dans un cadre privé. Au mois de mai 2020, le cabinet d'avocats américains *GSM Law*, qui compte parmi ses clients des stars du *show-biz* (Madonna, Lady Gaga, U2, Mariah Carey, etc.), ainsi que de grandes entreprises comme Facebook ou Samsung, a ainsi reconnu que ses fichiers informatiques avaient été dérobés et qu'il faisait l'objet d'une demande de rançon, dont le montant n'a pas été rendu public.

2. Les contenus illégaux frauduleux en ligne

Les contenus pédopornographiques, les appels à la haine ou encore l'incitation au terrorisme ne sont pas apparus avec Internet, mais le numérique a facilité leur diffusion. Cette forme de cybercriminalité utilise Internet comme le support de contenus illégaux, sans porter atteinte à l'intégrité d'un système informatique.

À la différence de l'Internet classique, qui utilise des protocoles de communication tendant à optimiser la transmission des données, le *dark web* utilise des protocoles visant à assurer l'anonymat de ses usagers. Ces protocoles procèdent au chiffrement de paquets de données afin de masquer l'adresse IP et *in fine* l'identité de l'utilisateur.

Numériquement, c'est surtout la **pédopornographie** qui mobilise les enquêteurs. Le *dark web*[1] constitue le terrain privilégié d'échange de contenus pédopornographiques, voire de ventes de prestations pédopornographiques en ligne. Dans une interview donnée en 2019[2], le directeur de l'Office central de répression des violences aux personnes estimait à 90 le nombre de ressortissants français impliqués dans des enquêtes pour des viols à distance en *streaming*. Le 13 janvier 2020, un ressortissant français a été condamné par le tribunal correctionnel de Paris pour avoir commandité l'agression sexuelle de petites filles aux Philippines, qu'il souhaitait visionner en direct sur Internet.

Comme l'a expliqué la directrice générale de Tracfin aux rapporteurs, la détection de ces violences sexuelles sur mineurs est parfois opérée par les banques qui repèrent des prélèvements forfaitaires réguliers

---

[1] *Le* dark web *(ou web sombre) désigne une portion du web qui n'est pas accessible par les moteurs de recherche classiques, mais uniquement* via *des logiciels anonymisant l'origine des connexions comme Tor. Il est possible de naviguer sur le* dark web *dans des conditions d'anonymat dont peuvent tirer parti par exemple les opposants à un régime autoritaire pour communiquer sans crainte. Mais cet anonymat favorise aussi l'essor d'activités criminelles en ligne.*

[2] Cf. Le Parisien*, 17 juin 2019.*

sur le compte de leur client, les versements étant généralement effectués dans des pays d'Asie du Sud-Est.

3. Des infractions classiques se sont déplacées vers l'univers numérique

Les personnes entendues par les rapporteurs ont souligné que des actes de délinquance classique avaient tendance à se déplacer dans le monde virtuel.

a) Les trafics en ligne

Le *dark web* constitue un espace virtuel propice au déroulement de divers trafics (d'armes, de faux papiers, de stupéfiants, etc.), les trafiquants et leurs clients ayant le sentiment de prendre moins de risques que lorsqu'ils interagissent physiquement.

Sur certains sites, se développent des modes de fonctionnement inspirés de ceux observés dans les sites commerciaux légaux, les clients commentant la qualité du produit fourni ou la ponctualité des livraisons, comme ils le feraient sur *TripAdvisor*... Tel était le mode de fonctionnement de la plateforme *Black Hand* (La Main noire), forum populaire du *dark web* francophone jusqu'à son démantèlement par les services des douanes en 2018. La Main noire ressemblait à un site de commerce classique, dans lequel vendeurs et acheteurs s'attribuaient des notes et pouvaient atteindre le statut « gold » ou « platine » en fonction du nombre de transactions effectuées. Au terme d'une année de surveillance, l'administratrice du site a pu être identifiée et interpellée à son domicile.

Le *dark web* permet également d'acquérir aisément des actifs plus immatériels, tels que des virus informatiques ou des coordonnées bancaires volées sur Internet, **ce qui permet à des individus qui ne disposent pas au départ d'un haut niveau d'expertise technique de mener des attaques informatiques assez sophistiquées**.

La place croissante des *blockchains* et des cryptoactifs

La croissance des trafics sur le *dark web* est favorisée par l'essor des *blockchains* et des cryptomonnaies[1] qui facilitent le blanchiment des capitaux et leur fuite vers l'étranger.

Dans son rapport publié en décembre 2018, la mission d'information commune de l'Assemblée nationale sur les usages des chaînes de blocs et autres technologies de certification de registre[2] donnait la définition suivante de la *blockchain* : une *blockchain* est un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la **cryptographie**.

Historiquement, la technologie *blockchain* s'est développée pour soutenir des transactions portant sur des cryptomonnaies ou des crypto-actifs (dont les *bitcoins* sont la forme la plus connue), qui ont comme caractéristique de ne pas dépendre d'un organisme centralisateur (comme une banque centrale) et d'être internationales.

Ce fonctionnement décentralisé complique la surveillance de la *blockchain*. Les transactions s'y effectuent en quelques secondes ou en quelques minutes, le temps nécessaire à la validation de chaque bloc, si bien qu'il est difficile pour les services enquêteurs de retracer l'ensemble de ces mouvements financiers réalisés en toute discrétion, sous une identité fictive. Ceci explique que les auteurs de tentatives d'extorsion au rançongiciel réclament généralement que la rançon leur soit versée en cryptomonnaie.

b) Les escroqueries en ligne

Une infraction très répandue relève de la pratique du « hameçonnage » (ou *phishing*) : elle consiste à reproduire un site légitime (une banque, un commerce en ligne) pour escroquer les consommateurs ou pour récupérer leurs coordonnées bancaires dans le but d'effectuer ensuite un virement frauduleux.

Le cybercriminel établit le contact avec ses victimes par l'envoi massif de courriels non sollicités (*spams*) qui invitent leurs destinataires à cliquer sur un lien les amenant sur le site frauduleux. Même si une très faible proportion des destinataires se laisse abuser et même si le préjudice individuel est généralement limité (quelques centaines d'euros), l'envoi de centaines de milliers de messages

[1] *Le développement des cryptomonnaies a d'ailleurs conduit à l'apparition d'un nouveau type d'infraction, qui se déroule souvent à l'insu de la victime, consistant à voler une partie de la puissance de calcul de son ordinateur, afin de générer de la cryptomonnaie.*

[2] *Rapport n° 1501 (XV^e législature) fait par Laure de La Raudière et Jean-Michel Mis, députés, au nom de la mission d'information commune sur les chaînes de blocs (blockchains).*

frauduleux rend l'opération lucrative pour le cybercriminel. Pendant la crise sanitaire, de nombreuses tentatives de hameçonnage ont consisté à proposer à la vente l'achat de masques ou d'autres matériels médicaux, qui n'étaient évidemment jamais livrés après que la victime en avait effectué le règlement, ou encore à inviter les victimes à faire un don en faveur de la recherche médicale.

D'autres infractions moins sophistiquées exploitent la crédulité de victimes souvent âgées.

Parfois, une fenêtre s'ouvre sur l'écran de l'ordinateur et informe son utilisateur qu'il doit contacter le service après-vente de Microsoft pour réparer le *bug* informatique que le programme vient de détecter ; la victime appelle le numéro qui lui est indiqué, un faux prestataire informatique lui répond et fait mine de corriger, à distance, le problème qui a soi-disant été détecté ; puis la victime reçoit une facture qu'elle règle en pensant avoir bénéficié d'une véritable assistance technique…

Les « escroqueries à la romance », qui impliquent souvent des ressortissants de pays d'Afrique de l'Ouest, sont également répandues : faisant croire à la victime qu'une relation amoureuse est en train de se nouer, l'escroc demande le virement de sommes d'argent de plus en plus importantes pour finalement ne plus donner signe de vie.

4. Des infractions mixtes

Certaines infractions combinent moyens informatiques et délinquance de rue. C'est le cas du *jackpotting*, ou piratage de distributeurs automatiques de billets (DAB).

La commission de l'infraction suppose la présence sur le terrain de délinquants chargés d'ouvrir le distributeur automatique, pour y introduire un dispositif informatique qui va permettre à leurs commanditaires, situés à l'étranger, de prendre à distance le contrôle du DAB pour le vider de l'ensemble des billets qu'il contient.

Les personnes impliquées dans ces opérations sont souvent originaires de l'ancien espace soviétique. En avril 2019, un groupe composé d'un Géorgien, d'un Lituanien et d'un Biélorusse, soupçonné d'avoir commis une dizaine d'attaques, a par exemple été arrêté dans l'Est de la France et déféré au parquet de Paris. En mai 2020, deux individus, également russophones, soupçonnés d'avoir commis dix-neuf infractions pour un préjudice estimé à près de 280 000 euros, ont été arrêtés à Rennes, au terme d'une enquête menée conjointement par la section de recherche de la gendarmerie et par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Dans son dernier rapport annuel, l'Observatoire de la sécurité des moyens de paiement indiquait avoir recensé, en 2018, 125 cas de piratages de DAB, contre seulement 76 en 2017, qualifiant toutefois ce niveau de « relativement modéré » par rapport à ceux constatés avant 2017.

B. UNE AMPLEUR DIFFICILE À ÉVALUER

Les rapporteurs se sont interrogés sur le montant du produit de la cybercriminalité pour rapidement constater qu'il était aujourd'hui impossible d'en fournir une évaluation rigoureuse.

1. Des données parcellaires

Le ministère de l'intérieur et le groupement d'intérêt public (GIP) Acyma, chargé d'apporter une assistance aux victimes d'actes de cybermalveillance, publient chaque année un rapport qui contient des données intéressantes, mais incomplètes, sur la cybercriminalité.

a) Les données du ministère de l'intérieur

Depuis sa création en 2017, la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, rattachée au ministère de l'intérieur, publie un rapport annuel sur l'**état de la menace numérique**. Son dernier rapport, datant de mai 2019, contient des informations détaillées qui reflètent l'activité des services de police et de gendarmerie.

Il est à noter que leur outil statistique répertorie les faits qualifiés de crime ou de délit **en fonction de la nature de l'infraction** commise, ce qui pose une vraie difficulté pour cerner l'ensemble des faits de cybercriminalité.

Certaines infractions relèvent par nature de la cybercriminalité. C'est le cas notamment des délits d'accès, d'altération du fonctionnement et de modification des données d'un système de traitement automatisé de données (STAD). C'est également le cas du délit de consultation habituelle de sites pédopornographiques, pour lequel une incrimination spécifique existe dans le code pénal. Ces infractions sont répertoriées dans les outils statistiques du ministère de l'intérieur.

Il en va différemment pour les infractions qui peuvent exister dans l'univers numérique comme dans le monde réel. Une escroquerie en ligne sera par exemple décomptée parmi les autres escroqueries, sans possibilité d'isoler les infractions commises au moyen d'un système informatique.

La gendarmerie a toutefois surmonté cette difficulté en donnant la possibilité au gendarme qui rédige un compte rendu de cocher la case « cyberespace » pour indiquer le lieu de l'infraction lorsqu'elle a été commise sur Internet. Les données de la gendarmerie fournissent donc une vision plus précise des contours de la cybercriminalité.

Concernant tout d'abord les atteintes aux systèmes de traitement automatisé de données (STAD), la police et la gendarmerie ont enregistré 9 970 infractions en 2018, chiffre en baisse par rapport à 2017 (- 6,6 %) et à 2016 (- 9,8 %). La délégation ministérielle insiste cependant sur le fait que « cette tendance statistique est difficilement interprétable en raison d'un faible taux de plainte ». La grande majorité de ces infractions (71 %) consiste en des accès frauduleux au système informatique, devant des atteintes aux données (22 % du contentieux).

Les services de police et de gendarmerie ont également enregistré, en 2018, un total de 390 atteintes au secret des correspondances émises par la voie électronique, chiffre en baisse de 2,5 % par rapport à l'année précédente.

La même année, 888 infractions sexuelles sur mineurs commises par l'intermédiaire d'un service en ligne ont été recensées, chiffre là aussi en baisse par rapport à 2017 (- 8 %).

D'autres infractions correspondent à des violations de la loi « Informatique et Libertés », par exemple la divulgation illégale de données à caractère personnel ou la collecte de données personnelles par un moyen frauduleux : 1 435 infractions ont été comptabilisées en 2018, contre 1 256 en 2017.

L'examen des statistiques de la gendarmerie donne une vision plus complète des faits de cybercriminalité **en englobant aussi les infractions qui se déroulent dans l'univers cyber**.

En 2018, 67 890 infractions relevant du champ cyber ont été traitées par la gendarmerie, chiffre en hausse de 7 % par rapport à 2017 après une progression de 32 % en 2016. Les trois quarts de ces infractions sont des escroqueries. Deux phénomènes saisonniers ressortent à la lecture des statistiques : des escroqueries à la location de courte durée pendant les vacances scolaires ; et des escroqueries variées à la période de Noël (*phishing* « remboursement des impôts », vente de produits contrefaits, etc.).

Deux autres sources de données exploitées par le ministère de l'intérieur sont les signalements effectués sur les plateformes **Pharos** et **Perceval**.

La plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) recueille les signalements des internautes qui repèrent sur le web des **comportements ou des contenus publics qu'ils estiment illégaux**. En 2018, les policiers et gendarmes en charge de la plateforme ont reçu et traité 163 723 signalements (en hausse de 6,6 % par rapport à 2017). Il s'agit en majorité (55 %) de signalements en lien avec des affaires d'escroquerie ou d'extorsion, ce qui est cohérent avec les données de la gendarmerie, qui mettent également en lumière la place majeure des escroqueries. Les atteintes aux mineurs (pédopornographie, prédation sexuelle, etc.) représentent 12,6 % des signalements et les faits d'apologie ou de provocation à des actes terroristes 2,8 % du total.

Lancée en 2018, la plateforme Perceval vise à recueillir les signalements relatifs aux **usages frauduleux de la carte bancaire**. Sur la période de dix mois comprise entre son lancement et la sortie du rapport, Perceval avait enregistré 100 000 signalements, correspondant à 400 000 usages frauduleux.

b) Les données du GIP Acyma

Le groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance, ou GIP Acyma, gère le site www.cybermalveillance.gouv.fr, qui s'adresse aux particuliers, aux entreprises et aux collectivités (à l'exception des opérateurs d'importance vitale et des opérateurs de services essentiels).

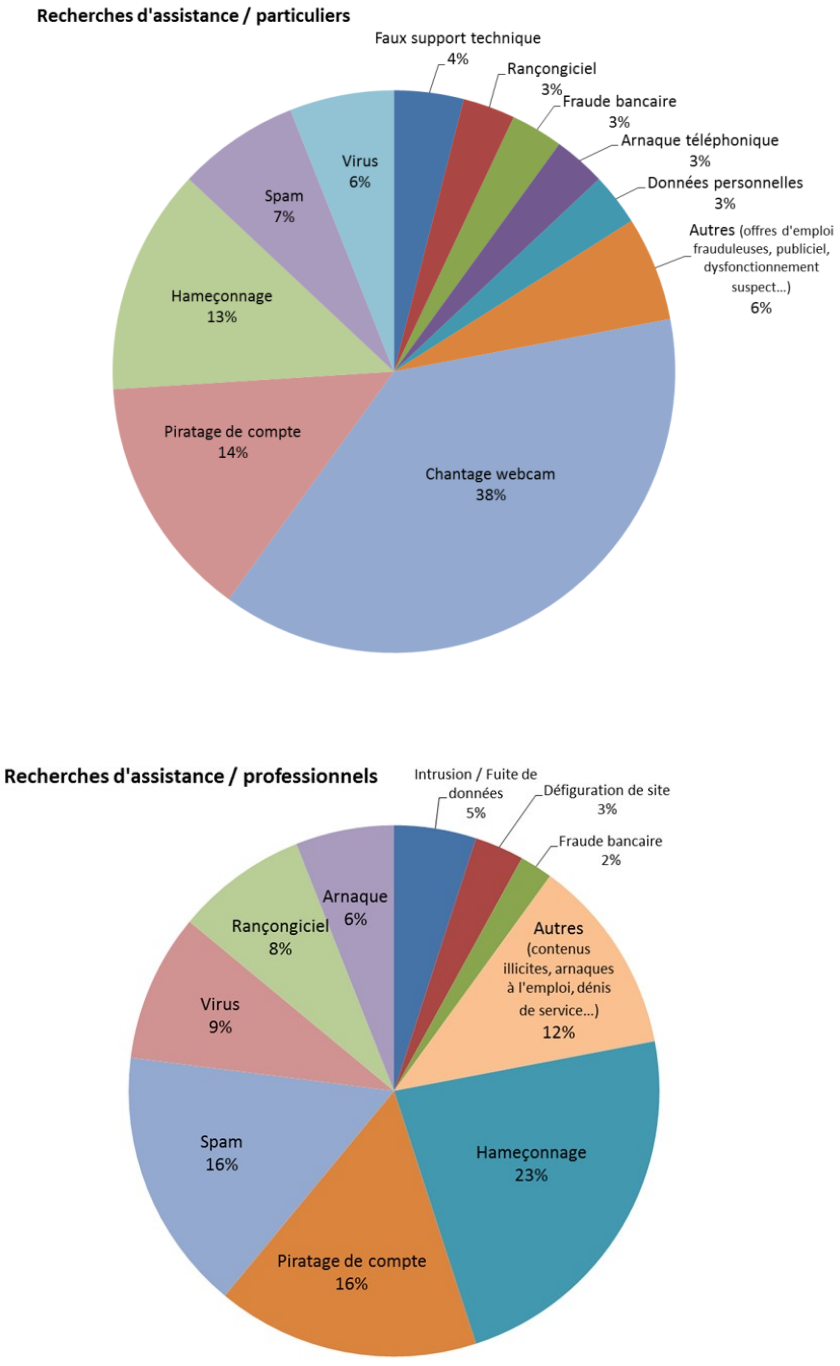
Cybermalveillance.gouv.fr ambitionne de devenir le site de référence vers lequel se tournent les victimes ou les personnes à la recherche de conseils en matière de prévention.

Le GIP rend publiques des statistiques élaborées à partir des demandes qui lui sont adressées[1]. Il indique dans son dernier rapport d'activité que plus de 90 000 victimes ont cherché de l'assistance sur la plateforme en 2019, contre seulement 28 000 en 2018. Il faut cependant y voir davantage le signe que les efforts pour faire connaître le dispositif ont porté leurs fruits plutôt qu'un indicateur de l'évolution sous-jacente de la cybercriminalité. Un pic de demandes d'assistance a été observé au début de l'année 2019, en lien avec différentes vagues de chantage à la *webcam* prétendument piratée.

Les deux diagrammes présentés en page suivante précisent sur quoi portaient les demandes d'assistance adressées à www.cybermalveillance.gouv.fr. Concernant les particuliers, les demandes d'assistance ont principalement porté sur le chantage à la *webcam* (38 %), suivi du piratage de compte en ligne (14 %) et du hameçonnage (13 %). Pour les professionnels (entreprises, collectivités et associations), le hameçonnage arrive en tête (23 %), devant le piratage de compte en ligne (16 %) et le *spam* (16 %).

[1] Cf. *le rapport d'activité 2019*.

Répartition des menaces par types de publics



Source : rapport d'activité 2019 du GIP Acyma

c) Les obstacles à une connaissance précise du phénomène

Les données publiées par le ministère de l'intérieur sont établies à partir des plaintes et des signalements auxquels procèdent les victimes. Or beaucoup de victimes ne portent pas plainte.

Certaines, comme cela a été indiqué, n'ont même pas conscience d'avoir été victimes d'une arnaque en ligne ou d'une intrusion dans leur système informatique. Par ailleurs, lorsqu'ils constatent qu'une infraction a été commise, les particuliers considèrent souvent que le préjudice subi, généralement de l'ordre de quelques centaines d'euros, est trop modeste pour justifier un dépôt de plainte, dont le résultat paraît aléatoire.

Concernant les entreprises, le préjudice est généralement plus important, mais la victime préfère parfois s'abstenir de déposer plainte afin de **préserver sa réputation** : l'image de l'entreprise risque d'être altérée s'il apparaît qu'elle n'est pas en mesure de se prémunir contre les cyberattaques et ses clients peuvent craindre que des informations les concernant soient rendues publiques, affaiblissant la confiance nécessaire à la poursuite de leur relation d'affaires. Seuls les opérateurs d'importance vitale ont l'obligation de signaler à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) les attaques dont ils font l'objet.

L'**inadaptation des outils statistiques**, développés à une époque antérieure à l'apparition de la cybercriminalité, constitue un autre obstacle à la connaissance fine du phénomène. Si la gendarmerie a innové pour appréhender l'ensemble des faits de délinquance et de criminalité cyber, le ministère de la justice apparaît plus en retrait : l'outil statistique Cassiopée utilisé pour suivre l'activité pénale repose entièrement sur les codes NATINF, qui renvoient à la nature de l'infraction, sans indication sur le lieu où elle a été commise. Ces statistiques ne permettent donc pas de distinguer par exemple si une escroquerie a été commise en ligne ou en dehors de l'univers numérique.

2. L'évaluation incertaine du produit de la cybercriminalité

Compte tenu de la difficulté de recenser l'ensemble des infractions, l'évaluation du produit de la cybercriminalité demeure nécessairement entourée d'une grande incertitude.

Les rares évaluations disponibles émanent de sociétés spécialisées dans la sécurité informatique. La société McAfee a ainsi estimé, dans un rapport publié en 2018, que la cybercriminalité coûtait aux entreprises un montant proche de 600 milliards de dollars par an, soit 0,8 % du PIB mondial, montant en hausse de 35 % par rapport à une précédente estimation (445 milliards) réalisée en 2014.

En 2017, l'entreprise Norton a réalisé une enquête dans vingt pays, totalisant 3,1 milliards d'habitants, dont 57 % disposaient d'un accès à Internet. Elle en a conclu que 53 % des utilisateurs d'Internet avaient été confrontés à la cybercriminalité ou que quelqu'un dans leur entourage l'avait été, et elle a évalué le montant global du préjudice lié à cette cybercriminalité à 172 milliards de dollars, soit 142 dollars en moyenne par victime. Pour la France, la perte est estimée à 7,1 milliards de dollars.

L'ampleur des écarts entre ces évaluations conduit à les envisager avec prudence.

Le rapport précité sur l'état de la menace liée au numérique mentionne des évaluations du préjudice subi par les entreprises pour certaines infractions : le coût moyen d'un détournement de données serait de 3,62 millions de dollars ; le coût estimé d'une violation de sécurité serait en moyenne de 330 000 euros pour les entreprises comptant au plus 1 000 salariés et atteindrait 1,3 million pour les entreprises de plus de 5 000 salariés. Concernant les particuliers, le rapport rappelle que le montant global de la fraude liée aux cartes de paiement s'élevait à 467 millions d'euros en 2017, dont 290,5 millions réalisés sur des transactions par Internet.

Outre le fait que de nombreuses infractions ne sont pas recensées, certains préjudices sont particulièrement difficiles à évaluer : lorsqu'une entreprise se fait voler des données confidentielles qui vont ensuite être exploitées par un concurrent et vont lui faire perdre des parts de marché, comment apprécier la perte subie ? Cela suppose de formuler des hypothèses fragiles sur ce qu'auraient été les positions respectives de chaque entreprise en l'absence de ce vol de données.

Les personnes entendues par les rapporteurs ont cependant toutes insisté sur le fait que **la cybercriminalité était un phénomène en expansion**, ce qui ne surprend guère dans un contexte où le numérique occupe une place croissante dans l'économie. Les délinquants perçoivent la cybercriminalité comme une activité moins risquée que la délinquance classique, et potentiellement très rémunératrice, ce qui favorise leur réorientation vers l'univers numérique.

3. L'intérêt d'une meilleure connaissance du phénomène

Dans la mesure où l'on ne combat efficacement que ce que l'on connaît, des initiatives pourraient être prises afin de tenter de mieux cerner les contours de la cybercriminalité.

La première pourrait consister à **faire évoluer les outils statistiques** de la police et de la justice afin qu'ils permettent de suivre, comme pour la gendarmerie, les infractions commises dans le cyberespace lorsque leur qualification juridique ne suffit pas à les identifier comme telles.

Il convient ensuite de faire encore mieux connaître les plateformes Pharos et Perceval afin que **les victimes acquièrent le réflexe de procéder à un signalement en ligne en cas d'infraction**. Le même effort de communication devra être mis en œuvre au moment du lancement de la **plateforme Thesee** (traitement harmonisé des enquêtes et signalements pour les e-escroqueries) qui permettra aux particuliers de déposer plainte en ligne

en cas d'escroquerie sur Internet[1]. Lorsque le préjudice est faible, la victime peut être réticente à se déplacer au commissariat ou à la brigade de gendarmerie la plus proche : la plainte en ligne est donc adaptée à ce type de situation. Les organisations d'employeurs, les chambres de commerce et d'industrie pourraient sensibiliser les entreprises à l'importance du dépôt de plainte en faisant valoir que leur souci de discrétion peut empêcher les enquêtes d'aboutir.

Au-delà de son intérêt sur le plan statistique, l'augmentation du nombre de signalements est indispensable pour aider les enquêteurs à recueillir des informations, opérer des rapprochements entre des faits de cybermalveillance qui semblent isolés de prime abord et reconstituer ainsi les différents aspects d'une affaire. En début d'année 2019, les magistrats spécialisés du parquet de Paris ont observé une amplification des campagnes de chantage à la webcam prétendument piratée. Ils ont élaboré un modèle-type de lettre pour le dépôt de plainte, mis à disposition du public sur www.cybermalveillance.gouv.fr. Cette initiative a permis à 28 000 personnes de formaliser leur plainte et de partager avec les enquêteurs des données techniques qui leur ont permis d'identifier deux personnes suspectées d'être les auteurs de l'infraction, interpellées en septembre 2019 puis en décembre 2019.

C. UNE GRANDE DIVERSITÉ DE PROFILS IMPLIQUÉS

Il n'existe pas un « profil-type » du cybercriminel, pas plus d'ailleurs que de « profil-type » de la victime de la cybercriminalité.

1. Du côté des auteurs

a) Des particuliers

Comme l'a souligné au cours de son audition le commandant de police Pierre Penalba, auteur de l'ouvrage *Cyber crimes*[2], « *le cybercriminel, c'est monsieur tout-le-monde* ».

Au cours de sa carrière de policier spécialisé dans la lutte contre la cybercriminalité, le commandant Penalba a été amené à interpeller des adolescents au profil de *geek*, des ingénieurs informatiques, mais aussi un caissier qui revendait des numéros de carte bancaire... La cybercriminalité ne concerne donc pas uniquement des personnes possédant une grande expertise dans le domaine informatique. Des particuliers, qualifiés de

[1] *Dans le détail, le projet Thesee devrait permettre le dépôt de plainte en cas d'escroquerie à la petite annonce et à la romance, de chantage à la webcam, de faux site de vente, d'usurpation de boîte mail et d'extorsion.*

[2] Cyber crimes : un flic 2.0 raconte, *par Pierre et Abigaelle Penalba, Albin Michel, Paris, janvier 2020.*

« mules » acceptent parfois de voir transiter sur leur compte des sommes de provenance frauduleuse en espérant en percevoir un pourcentage.

La facilité avec laquelle des logiciels malveillants ou des coordonnées bancaires peuvent être acquis sur le *dark web* favorise la diffusion de la cybercriminalité à des profils diversifiés.

b) Des organisations criminelles

Entendue par les rapporteurs, la magistrate Myriam Quémeneur a insisté sur la reconversion vers la cybercriminalité de certaines organisations criminelles, notamment des mafias russophones.

En 2019, les entreprises Thalès et Verint ont publié un annuaire mondial des groupes de pirates informatiques les plus dangereux. Il liste une soixantaine d'organisations, divisées en quatre familles d'attaquants en fonction de leurs motivations et de leur objectif final :

- 49 % sont parrainées par des États ; elles visent des cibles présentant un intérêt sur le plan géopolitique et volent des données sensibles ;

- 26 % sont décrites comme des « hacktivistes » ; leur motivation est idéologique, ils vont chercher à prendre le contrôle du site Internet d'un organisme officiel ou à en empêcher l'accès ;

- 20 % sont des cybercriminels au sens strict, animés par une motivation pécuniaire ;

- 5 % enfin sont des groupes terroristes qui vont chercher à propager leurs idées ou à détériorer les systèmes informatiques de leurs cibles.

Les groupes terroristes demeurent encore peu présents dans l'univers cyber. Le directeur général de l'ANSSI, Guillaume Poupard, a indiqué aux rapporteurs qu'aucune cyberattaque à caractère terroriste n'avait eu jusqu'ici un impact significatif. L'ANSSI veille cependant à la sécurité des réseaux électroniques et des réseaux de communications ou de transports qui pourraient être la cible de telles attaques.

c) Des services étatiques

Comme le montre cette classification, la cybercriminalité présente donc souvent une dimension politique : des attaques peuvent être lancées par des groupes sponsorisés par un État ou menées directement par des services de renseignement étrangers.

La **Russie** est régulièrement mise en cause en cas de cyberattaque. Dans son rapport rendu public en 2019, le procureur spécial américain Robert Mueller a accusé le service de renseignement militaire russe, le GRU, d'avoir piraté les boîtes mail de plusieurs responsables de la campagne présidentielle démocrate de 2016, afin de diffuser ensuite leurs messages sur *Wikileaks*. Il a également reproché à la Russie d'avoir mené sur les réseaux

sociaux une campagne de grande ampleur de dénigrement de la candidate Hillary Clinton.

À plusieurs reprises, l'Ukraine a également rendu la Russie responsable, soit directement, soit par l'intermédiaire de *hackers*, de cyberattaques qui ont touché ses entreprises et ses infrastructures. En décembre 2015 puis en décembre 2016, le réseau d'approvisionnement électrique ukrainien a fait l'objet d'attaques qui ont provoqué des coupures de courant pendant plusieurs heures.

En juin 2017, le pays a été fortement touché par la cyberattaque *NotPetya*. Le logiciel utilisé pour les déclarations fiscales a été infecté et a servi à diffuser la charge virale. Celle-ci a eu pour effet de supprimer le système de lancement des ordinateurs infectés, les rendant inutilisables. Cette attaque a provoqué des perturbations majeures : les chemins de fer, le métro et l'aéroport de Kiev ont été contraints de limiter leurs opérations, de même que des entreprises publiques de premier plan comme la poste ou l'opérateur de télécommunications UkrTelecom ; les distributeurs de billets ne fonctionnaient plus à Kiev, des banques et des magasins ont été contraints de fermer leurs portes, des chaînes de télévision et des stations de radio ont dû rendre l'antenne, tandis que les ordinateurs de plusieurs ministères ont été paralysés.

Cette attaque a été analysée comme une manifestation de la « guerre hybride » menée par la Russie contre l'Ukraine dans le but de déstabiliser ses institutions et d'affaiblir son économie.

La **Chine** est une autre puissance qui dispose des moyens techniques et des ambitions géopolitiques qui peuvent motiver des cyberattaques.

En juin 2020, à l'occasion d'un sommet Chine-Union européenne par téléconférence, la présidente de la Commission européenne, Ursula von der Leyen, a accusé la Chine d'être à l'origine d'une série de cyberattaques ciblant les hôpitaux européens pendant la pandémie. Elle a également reproché à la Chine d'avoir mené en Europe une campagne de désinformation relative à la crise sanitaire.

Le même mois, l'Australie a été la cible d'une importante cyberattaque que le Premier ministre, Scott Morrison, a attribuée à des pirates agissant pour le compte d'un acteur étatique sophistiqué. La plupart des observateurs considèrent que la Chine en est à l'origine, dans le but de faire pression sur l'Australie dans un contexte de tensions diplomatiques et commerciales. Le gouvernement australien a annoncé, le 30 juin 2020, que le pays allait investir plus de 800 millions d'euros au cours des dix prochaines années pour renforcer sa cybersécurité.

2. Du côté des victimes

a) Les particuliers

Personne n'est à l'abri de la cybercriminalité qui concerne, comme on l'a vu, un grand nombre de particuliers : **ils ont représenté l'an passé 90 % des victimes qui se sont tournées vers le dispositif Cybermalveillance.gouv.fr**.

Les personnes âgées, moins familières de l'univers du numérique, apparaissent particulièrement vulnérables, de même que les plus jeunes qui, quoiqu'étant des *digital natives*, manquent de maturité pour repérer certains comportements suspects.

Très présents sur Internet, les plus jeunes constituent en particulier des proies faciles pour les prédateurs sexuels. La pratique du *grooming* consiste pour un adulte à gagner la confiance d'un mineur, et parfois aussi de ses parents, afin d'en abuser sexuellement. Les réseaux sociaux, les forums de discussion, les jeux vidéo en ligne offrent de multiples occasions de contacts entre les victimes et leurs futurs agresseurs qui se font parfois passer eux-mêmes pour des enfants ou des adolescents pour obtenir un rendez-vous avec le mineur.

Le mode opératoire retenu est parfois fort simple : en 2017, le tribunal correctionnel de Poitiers a par exemple condamné un pédocriminel de 28 ans qui entrait en relation avec ses victimes en proposant ses services en tant que baby-sitter dans des petites annonces postées sur le site Le Bon Coin. Ses méfaits ont été interrompus lorsqu'une jeune victime a expliqué à ses parents ce qu'elle avait subi.

b) Les entreprises et les administrations

Des grandes entités publiques et privées sont également la cible de cybercriminels, occasionnant parfois un préjudice considérable, comme le montre l'actualité récente.

Au mois de février 2020, Bouygues Construction, la filiale de BTP du groupe éponyme, a été la victime d'un rançongiciel qui a bloqué son système informatique pendant plusieurs semaines. Les *hackers* ont exigé une rançon de dix millions de dollars et ont menacé de rendre publiques les données qu'ils avaient cryptées s'ils n'obtenaient pas satisfaction.

Le mois suivant, c'est la ville de Marseille et la Métropole Aix-Marseille-Provence qui ont été victimes d'une attaque, à la veille du premier tour des élections municipales. Les perturbations ont été telles que la municipalité s'est demandé si elle serait en mesure d'imprimer les listes d'émargement nécessaires à l'organisation du scrutin ! La tenue de l'état-civil, la comptabilité, différents services aux habitants ont été affectés de

manière prolongée, le retour à la normale n'étant intervenu qu'au cours du mois de mai.

En novembre 2019, c'est le système informatique du CHU de Rouen qui a été paralysé pendant plusieurs jours, entraînant des perturbations dans son fonctionnement administratif. Si la réactivité du personnel hospitalier a évité que la santé des patients soit mise en danger, la présence d'un nombre croissant d'**appareils connectés** dans les hôpitaux ne permet pas d'écarter totalement le risque que la continuité des soins aux patients soit un jour menacée par une attaque informatique.

c) Les opérateurs d'importance vitale

Une attention particulière est portée à la sécurité des **opérateurs d'importance vitale** (OIV), compte tenu de leur rôle dans la continuité de la vie de la Nation.

Le code de la défense précise que les opérateurs d'importance vitale sont des opérateurs publics ou privés qui gèrent ou utilisent, au titre de leur activité, un établissement, un ouvrage ou une installation dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement, d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

Une liste de deux cents OIV, gardée confidentielle pour des raisons de sécurité, a été établie, couvrant les secteurs de l'alimentation et de l'approvisionnement en eau, des transports, de l'énergie, de la santé ou encore de la défense.

Le dispositif de sécurité des OIV intègre une dimension de cybersécurité, placée sous la responsabilité de l'ANSSI (*cf. infra*).

II. UN DISPOSITIF NATIONAL DE LUTTE QUI APPARAÎT INSUFFISAMMENT DOTÉ NOTAMMENT SUR SON VERSANT JUDICIAIRE

A. UN ARSENAL LÉGISLATIF GLOBALEMENT ADAPTÉ

Les personnes entendues par les rapporteurs ont jugé le cadre juridique de la lutte contre la cybercriminalité satisfaisant, qu'il s'agisse du droit matériel ou de la procédure pénale, même si des améliorations restent possibles, notamment en ce qui concerne la sécurisation des éléments de preuve numérique.

1. Le droit matériel

Un grand nombre d'incriminations pénales peuvent être utilisées pour réprimer les faits de cybercriminalité. Certaines sont propres à l'univers cyber, tandis que d'autres sont de portée plus générale, beaucoup de faits pouvant d'ailleurs faire l'objet d'une double qualification.

a) Sur les atteintes aux systèmes informatiques

Beaucoup de faits de cybercriminalité sont poursuivis sur le fondement des articles 323-1 et suivants du code pénal, relatifs aux **atteintes aux systèmes de traitement automatisé de données**, souvent qualifiés « d'infractions STAD ».

Ces infractions sont anciennes, puisqu'elles sont issues de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite loi Godfrain, du nom de l'ancien député Jacques Godfrain qui en est à l'origine.

En dépit des évolutions technologiques considérables observées depuis plus de trente ans, **ces incriminations pénales ont été rédigées en des termes suffisamment larges pour pouvoir s'appliquer aux formes contemporaines de la cybercriminalité**.

Une actualisation a toutefois été opérée en 2004 afin de sanctionner la **vente d'équipements ou de logiciels permettant d'attaquer un système informatique**, ce qui est très utile pour réprimer certaines transactions observées sur le *dark net*.

Les atteintes aux systèmes de traitement automatisé de données

L'article 323-1 du code pénal punit de deux ans d'emprisonnement et de 30 000 euros d'amende le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système automatisé de traitement de données (STAD).

La peine est portée à trois ans d'emprisonnement et à 45 000 euros d'amende lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système.

L'article 323-2 punit de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait d'entraver ou de fausser le fonctionnement d'un STAD.

L'article 323-3 punit des mêmes peines le fait d'introduire frauduleusement des données dans un STAD ou de supprimer ou modifier frauduleusement les données qu'il contient.

L'article 323-3-1, issu de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, punit 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 prévues par les articles 323-1 à 323-3 ; la peine est identique à celle prévue pour ladite infraction.

L'article 323-4 punit la participation à une bande organisée en vue de commettre l'une des infractions visées aux articles précédents.

L'article 323-5 prévoit des peines complémentaires (privation des droits civiques, interdiction d'exercer certaines fonctions, fermeture de l'établissement, exclusion des marchés publics, confiscation de l'objet qui a servi à commettre l'infraction, etc.).

L'article 323-6 dispose que les personnes morales peuvent également être poursuivies.

L'article 323-7 prévoit enfin que la tentative des délits est punie des mêmes peines que les délits eux-mêmes.

Des faits de cyber-espionnage dans le réseau informatique d'une entreprise, l'attaque d'un *hacker* qui défigure un site Internet institutionnel ou la compromission de données sont autant d'actes de délinquance qui peuvent être poursuivis sur le fondement des infractions STAD.

b) Sur les atteintes aux personnes

Le code pénal a été complété, soit par la création d'infractions spécifiques, soit par la création de circonstances aggravantes, afin de tenir compte de l'utilisation d'Internet pour porter atteinte aux personnes, et notamment aux mineurs.

(1) Des infractions spécifiques

En 2004, 2006 et 2007, l'article 227-23 du code pénal a ainsi été modifié afin de mieux réprimer les faits de **pédopornographie**. Cet article punit désormais de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait d'enregistrer ou de transmettre la représentation à caractère pornographique d'un mineur en vue de sa diffusion. Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsque cette diffusion est effectuée *via* un réseau de communications électroniques.

Le même article punit de deux ans d'emprisonnement et de 30 000 euros d'amende[1] le fait de consulter des images pédopornographiques en ligne ou de conserver ces images par quelque moyen que ce soit, sur le disque dur d'un ordinateur par exemple.

Les peines prévues à cet article sont portées à dix ans d'emprisonnement et à 500 000 euros d'amende lorsque les faits sont commis en bande organisée.

En 2011, un nouvel article 226-4-1 a été introduit dans le code pénal afin de réprimer le fait d'**usurper l'identité d'un tiers**, y compris lorsque l'infraction est commise sur un réseau de communication au public en ligne.

Plus récemment, la loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes a introduit dans le code pénal un nouvel article 226-3-1 afin de réprimer la pratique de l'*upskirting* qui consiste à filmer ou photographier à son insu les parties intimes d'un individu, souvent dans le but de diffuser ensuite les images sur Internet. Les peines sont de deux ans d'emprisonnement et 30 000 euros d'amende lorsque les images ont été enregistrées ou transmises.

(2) Des circonstances aggravantes

Afin de dissuader les prédateurs sexuels de rechercher leurs victimes sur Internet, des **circonstances aggravantes** ont été introduites à différents articles du code pénal afin de réprimer plus sévèrement certains faits lorsque l'auteur est entré en contact avec la victime *via* un réseau de communication électronique :

- à l'article 222-24 concernant le viol ;

- à l'article 222-28 relatif aux agressions sexuelles ;

- à l'article 225-12-2 sur l'achat de prestations sexuelles à une personne mineure ou vulnérable ;

- à l'article 227-22 sur la corruption de mineurs.

---

[1] *Ces peines devraient être prochainement portées à cinq ans d'emprisonnement et à 75 000 euros d'amende comme le prévoit la proposition de loi visant à protéger les victimes de violences conjugales en cours de navette.*

Une circonstance aggravante a également été introduite à l'article 227-26 du code pénal relatif au harcèlement moral.

c) Les infractions de portée générale

Beaucoup de faits de cybercriminalité sont poursuivis sur la base d'incriminations pénales générales, parfois associées à des infractions STAD.

Les **attaques au rançongiciel** peuvent ainsi être poursuivies au titre des atteintes au STAD, mais aussi sur le fondement des articles 312-1 et 312-6-1 du code pénal, qui répriment l'extorsion simple ou en bande organisée.

Les articles 313-1 à 313-3 du code pénal, qui répriment l'**escroquerie**, simple ou en bande organisée, peuvent être mobilisés pour réprimer les escroqueries à la fausse amitié ou à la romance, les escroqueries à l'investissement en ligne, les escroqueries au faux site de vente en ligne ou encore l'arnaque au faux site administratif. Les escroqueries au faux ordre de virement ou aux images érotiques fictives peuvent aussi être poursuivies au titre des atteintes au STAD.

La publication de contenus illicites en ligne peut être poursuivie en faisant appel à une grande diversité de qualifications pénales, qui vont dépendre de la nature du contenu considéré : un fait de *revenge porn* pourra être réprimé sur le fondement de l'article 226-2-1 du code pénal sur les atteintes à la vie privée ; d'autres contenus seront réprimés au titre de l'apologie du terrorisme, de la provocation à la haine, à la discrimination ou à la violence, ou encore en tant que diffamation ou injure.

Les cybercriminels qui recrutent des mules sur Internet ou qui proposent sur le *dark web* du matériel pour réaliser une cyberattaque peuvent être poursuivis sur le fondement des articles 450-1 à 450-5 du code pénal, relatifs à la participation à une association de malfaiteurs. Le blanchiment réalisé grâce à des cryptoactifs peut être poursuivi en tant que blanchiment aggravé (article 324-2 du code pénal), tandis que la vente illicite de données personnelles peut être poursuivie sous la qualification de recel (article 321-1).

Cette présentation des principales qualifications pénales utilisées montre que **l'arsenal législatif est étoffé** : **il n'existe pas de faits de cybercriminalité qui ne pourraient être poursuivis faute d'incrimination adaptée.**

Comme le notait Marc Robert dans son rapport de février 2014, *Protéger les internautes*, la **jurisprudence de la Cour de cassation contribue également à faciliter la poursuite des faits de cybercriminalité** en allant « dans le sens d'une "dématérialisation" des éléments constitutifs de certains délits, par exemple lorsqu'elle admet que le délit de vol est constitué par le simple fait de s'approprier, à l'insu de son propriétaire, un document, quel qu'en soit le support, pour la seule durée nécessaire pour le copier, ou celui d'abus de confiance par le détournement d'un bien "quelconque" pour

d'autres usages que ceux pour lesquels il a été confié, ou encore celui d'escroquerie par l'utilisation d'un code de carte bancaire ».

2. La procédure pénale

Les enquêteurs et magistrats entendus par les rapporteurs se sont également déclarés satisfaits du cadre procédural dans lequel ils opèrent, après qu'il a été réformé par la loi de programmation 2018-2022 et de réforme pour la justice du 23 mars 2019. Deux techniques d'investigation sont particulièrement utiles en matière de lutte contre la cybercriminalité.

a) L'enquête sous pseudonyme

Créée en 2007, la technique des enquêtes sous pseudonyme, ou « cyberpatrouilles » se conçoit comme une **infiltration numérique** : dès lors que diverses infractions sont commises au moyen d'Internet, il convient de permettre à des officiers de police judiciaire d'enquêter en ligne, sous pseudonyme, afin de recueillir des preuves.

Les enquêteurs, spécialement habilités à cette fin, peuvent notamment :

- participer sous pseudonyme aux échanges électroniques ;

- extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs des infractions ;

- extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites (sauf pour certaines infractions).

À peine de nullité, ces actes ne peuvent constituer une incitation à la commission d'une infraction, ce qui signifie que l'enquêteur ne doit pas inciter autrui à commettre une infraction sous peine que l'acte soit annulé et ne puisse plus figurer dans la procédure.

Le champ d'application de cette technique, d'abord limité aux infractions de nature sexuelle ou en matière de traite des êtres humains, a été progressivement étendu à l'apologie du terrorisme, à l'ensemble des infractions de la délinquance et de la criminalité organisées, mentionnées aux articles 706-73 et 706-73-1 du code de procédure pénale, mais également aux délits d'atteintes aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'État, commis en bande organisée, ainsi qu'à certaines infractions du code de la santé publique ou du code de la consommation.

La loi du 23 mars 2019 a **unifié le régime de l'enquête sous pseudonyme**, désormais défini dans un nouvel article 230-46 du code de procédure pénale, alors qu'il était auparavant dispersé entre plusieurs articles dudit code. Surtout, elle a élargi le champ d'application de cette

technique en l'autorisant pour **toute infraction punie d'une peine d'emprisonnement commise par un moyen de communication électronique**. L'acquisition de tout contenu, produit, substance, prélèvement ou service, y compris illicite, est mieux encadrée puisque soumise à l'autorisation du procureur de la République ou du juge d'instruction, l'autorisation étant mentionnée au dossier de la procédure.

b) L'interception des communications électroniques

Au cours des investigations, il est possible de recourir aux interceptions de correspondances émises par la voie des communications électroniques[1], communément appelées « écoutes judiciaires ».

Légalisées en 1991, les interceptions judicaires relevaient initialement du seul juge d'instruction qui peut les prescrire « lorsque les nécessités de l'instruction l'exigent », en matière criminelle et correctionnelle si la peine encourue est égale ou supérieure à deux ans d'emprisonnement. Depuis 2004, le juge des libertés et de la détention (JLD) peut également autoriser des interceptions de correspondances pendant une enquête de flagrance ou préliminaire relative à la délinquance ou à la criminalité organisée, ces interceptions étant ordonnées pour une durée maximale d'un mois, renouvelable une fois.

Le projet de loi de programmation 2018-2022 et de réforme pour la justice avait pour ambition d'étendre le champ d'application des interceptions de correspondances émises par la voie des communications électroniques, durant l'enquête de flagrance et l'enquête préliminaire, à tous les crimes et à tous les délits punis d'au moins trois ans d'emprisonnement, sans exiger qu'ils relèvent de la délinquance ou de la criminalité organisée. La commission des lois du Sénat s'était opposée à cette extension qui lui avait semblé porter une atteinte disproportionnée aux libertés individuelles, notamment au regard des capacités de contrôle du JLD.

Le Conseil constitutionnel a partagé cette analyse puisqu'il a censuré cette disposition[2]. Il a considéré que les infractions visées n'étaient pas d'une particulière complexité et que l'autorisation du JLD, qui ne dispose pas de tout le dossier de la procédure, n'était pas une garantie suffisante.

Les professionnels entendus par les rapporteurs n'ont pas souhaité que le débat soit rouvert sur ce point, ce qui conduit à penser que l'extension considérable envisagée par le Gouvernement n'était sans doute pas indispensable.

---

[1] *Selon l'article 32 du code des postes et communications électroniques (CPCE), les communications électroniques correspondent à « toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques ». Est donc concernée l'interception des correspondances émises ou reçues sur des différents supports tels que les téléphones fixes ou mobiles, les tablettes ou les ordinateurs.*

[2] *Décision n° 2019-778 DC du 21 mars 2019.*

3. Des améliorations possibles

a) La preuve numérique

Le principal obstacle rencontré par les magistrats et par les enquêteurs réside dans la **difficulté à accéder à la preuve numérique**.

Le recueil de la preuve numérique dépend de la durée de conservation des données par chaque hébergeur, qui n'obéit à aucune norme commune, mais aussi de la garantie que pourront apporter les enquêteurs que la preuve n'a pas été falsifiée. Comme l'a souligné Myriam Quémener[1], avocate générale près la cour d'appel de Paris, « la matière pénale renforce les exigences sur les enquêteurs qui devront pouvoir démontrer son origine et son authenticité aux avocats et aux magistrats. Le respect de la procédure d'accès à la preuve numérique est d'une importance fondamentale car elle permet de démontrer l'intégrité des données électroniques et d'expliquer la manière dont elles ont été obtenues en conformité avec les droits des parties ».

Des négociations sont actuellement en cours au niveau de l'Union européenne, dans le cadre du paquet « e-evidence », afin d'harmoniser les règles applicables à l'échelle européenne (*cf. infra*).

La question de l'accès à la preuve numérique dépasse d'ailleurs le cadre de la lutte contre la cybercriminalité : dans les affaires d'une certaine complexité, quelle qu'en soit la nature, les enquêteurs ont souvent comme premier réflexe d'exploiter des données de téléphonie mobile, de vidéosurveillance ou de solliciter des expertises informatiques, ce qui témoigne de la nécessité de sécuriser ces données.

b) La question de la responsabilité des hébergeurs

Les rapporteurs ont concentré leurs investigations sur la lutte contre la cybercriminalité par l'autorité judiciaire et par les services enquêteurs. Ils n'ont pas étudié la question de la responsabilité des hébergeurs, qui reste aujourd'hui en débat. Deux développements récents soulignent la complexité de ce sujet.

D'abord, la censure par le Conseil constitutionnel de la proposition de loi présentée par la députée Laetitia Avia, sur laquelle le Sénat avait multiplié les mises en garde.

Ce texte avait pour ambition d'imposer le retrait dans des délais extrêmement brefs de certains contenus illicites. Il aurait obligé certains opérateurs de plateforme en ligne, sous peine de sanction pénale, à retirer ou à rendre inaccessibles, dans un délai de vingt-quatre heures, des contenus illicites en raison de leur caractère haineux ou sexuel, sur la base d'un simple signalement par un utilisateur. Il aurait également imposé aux hébergeurs ou

[1] *Cette citation est extraite de la contribution écrite que Mme Quémener a adressée aux rapporteurs.*

aux éditeurs d'un service de communication en ligne de retirer, dans un délai d'une heure, les contenus à caractère terroriste ou pédopornographique notifiés par l'autorité administrative. Le non-respect de ces obligations aurait été passible d'une lourde sanction pénale.

Saisi par plus de soixante sénateurs, dont le rapporteur Sophie Joissains, le Conseil constitutionnel a estimé, par sa décision n° 2020-801 DC du 18 juin 2020, que ces dispositions portaient une atteinte disproportionnée à la liberté d'expression et de communication et qu'elles devaient donc être déclarées contraires à la Constitution. Elles auraient accordé un pouvoir considérable à l'administration pour décider des contenus à retirer et fait peser une forte contrainte sur les opérateurs qui auraient été tentés de retirer tous les contenus signalés pour se mettre à l'abri de poursuites pénales, compte tenu de la difficulté de procéder à un véritable examen des contenus litigieux dans le délai court qui leur était imparti.

Par ailleurs, la Cour des comptes a publié, en février 2020, un rapport sur la lutte contre les contrefaçons dans lequel elle suggère de **renforcer les obligations juridiques des plateformes du commerce en ligne** afin de mieux lutter contre le commerce de contrefaçons.

La Cour des comptes estime que « les plateformes numériques sont relativement passives dans la lutte contre la contrefaçon au motif qu'elles ne sont que des intermédiaires sans obligation de vigilance particulière. Ce régime de responsabilité limitée résulte de la directive commerce électronique 2000/31/CE qui dispense les plateformes du contrôle général des contenus qu'elles hébergent. C'est seulement en cas d'inaction à la suite d'une notification que l'intermédiaire peut, le cas échéant, voir sa responsabilité engagée ».

Sans aller jusqu'à imposer aux plateformes (moteurs de recherche, réseaux sociaux, places de marché) un devoir de surveillance générale *a priori* de la totalité des contenus, produits et services qu'ils référencent, la Cour suggère de définir de nouvelles obligations de vigilance renforcée, qui les obligeraient notamment à vérifier l'identité des vendeurs et à communiquer cette information aux consommateurs, à suivre les flux permettant d'identifier les étapes de la chaîne de distribution et à mettre en place une procédure de notification des contenus contrefaisants, avec un délai de retrait homogène et rapide.

Compte tenu du grand nombre d'infractions constatées dans l'univers cyber, il est vraisemblable qu'une meilleure régulation d'Internet par ses principaux acteurs, dans un cadre défini par les États ou, mieux, par l'Union européenne, se révèlera nécessaire pour compléter les efforts de la police et de la justice.

c) Les interrogations soulevées par certaines interventions à distance

En 2019, le centre de lutte contre la criminalité numérique (C3N) de la gendarmerie nationale a réalisé, en partenariat avec l'entreprise de sécurité informatique Avast, une opération spectaculaire tendant à mettre fin à l'activité d'un vaste *botnet*[1] dans le cadre de l'affaire dite Retadup.

Retadup est le nom d'un logiciel malveillant (ou *malware*) qui a principalement contaminé des ordinateurs basés aux États-Unis et en Amérique latine. Les ordinateurs contaminés ont formé un *botnet*, soit un réseau de centaines de milliers d'ordinateurs piratés pour générer de la cryptomonnaie à l'insu de leurs propriétaires.

À cette fin, les ordinateurs contaminés se connectent régulièrement à un serveur « *command and control* » qui leur donne des instructions. L'entreprise Avast a repéré que ces connections les reliaient à un serveur basé en région parisienne. Elle a pris contact avec le C3N, et le parquet de Paris a ouvert une enquête. Le serveur a été localisé chez un hébergeur qui a fait l'objet d'une perquisition.

Avast et le C3N ont repéré une faille dans le protocole utilisé par les pirates informatiques. **Cette faille a été exploitée pour nettoyer à distance les ordinateurs infectés**.

Ce serveur a été remplacé par un serveur de la gendarmerie auquel les ordinateurs contaminés se sont connectés : le nouveau serveur leur a donné l'ordre d'exécuter une commande vide ayant pour effet de désactiver le logiciel malveillant.

Cette affaire illustre l'excellence technique du C3N. **Elle pose aussi des questions nouvelles sur le plan juridique : est-il permis d'apporter une modification, sans l'accord de leur propriétaire ni des États concernés, à des ordinateurs situés à l'étranger ?** En l'espèce, le C3N n'a pas porté atteinte à un STAD puisque ce sont les ordinateurs contaminés qui se connectaient au serveur présent sur le territoire national, sans qu'il leur soit ordonné de réaliser de codes supplémentaires. Mais serait-il envisageable que des données plus intrusives soient envoyées vers les ordinateurs de particuliers ou d'entreprises à l'étranger, sans les en informer, dans le but de « nettoyer » ces machines, voire dans le but de neutraliser un *botnet* à distance ?

Une réflexion européenne et internationale mériterait d'être conduite dans les prochaines années afin de définir les pratiques qui sont juridiquement acceptables et de prévoir des règles de bonne conduite dans les relations entre États.

---

[1] *Un* botnet *est un réseau de robots composé d'un grand nombre d'ordinateurs dont un logiciel malveillant a pris possession.*

B. DES SERVICES SPÉCIALISÉS À ÉTOFFER

La forte dimension technique de la cybercriminalité a conduit à spécialiser certains services enquêteurs et certains magistrats. D'un bon niveau technique, ces services gagneraient toutefois à être étoffés, notamment sur le versant judiciaire qui apparaît particulièrement sous-doté.

1. La spécialisation des services enquêteurs

Les administrations en charge de la répression des infractions pénales, fiscales ou douanières se sont chacune dotées de leur service spécialisé.

a) Au sein de la police judiciaire

Depuis 2014, la direction centrale de la police judiciaire (DCPJ) du ministère de l'intérieur[1] s'est dotée d'une **sous-direction en charge de la lutte contre la cybercriminalité** (SDLC).

Pôle de compétence nationale, la sous-direction emploie environ 130 personnes, dont une dizaine d'ingénieurs et de techniciens. Elle comprend notamment un bureau de coordination stratégique, un bureau de l'Internet, un bureau de la formation à la lutte contre la cybercriminalité, une division de l'anticipation et de l'analyse, ainsi que l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Elle travaille en partenariat avec les autres administrations du ministère de l'intérieur et avec d'autres administrations centrales, telles que la direction générale de la concurrence, de la consommation et de la répression des fraudes ou la direction générale des douanes et des droits indirects. Elle constitue une entité aisément identifiable par ses partenaires institutionnels, par les acteurs de l'économie numérique et par les particuliers.

La SDLC joue un rôle important en matière de formation - 610 investigateurs ont déjà été formés à la lutte contre la cybercriminalité - et d'animation du **réseau de « référents cybermenaces »** qui s'est constitué au sein de la police judiciaire. Elle apporte de l'information aux services qui enquêtent sur le terrain et les aide à nouer des contacts avec les acteurs de l'Internet grâce à son répertoire de contacts réservés.

La SDLC est aussi une source d'expertise grâce à ses **seize laboratoires d'investigation du numérique** présents sur le territoire et grâce à sa section d'assistance technique, de recherche et de développement,

[1] *La DCPJ concourt à l'exercice des missions de police judiciaire sur l'ensemble du territoire, ainsi qu'à la prévention et à la répression des formes spécialisées, organisées ou transnationales de la délinquance et de la criminalité.*

chargée d'aider les services à exploiter les supports numériques et à concevoir de nouveaux outils d'investigation numérique. La division de la preuve numérique peut envoyer en renfort un groupe d'appui pour travailler sur les traces numériques.

La SDLC contribue aussi au développement d'outils tournés vers le grand public. À parité avec la gendarmerie, la SDLC gère la plateforme Pharos, qui recueille les signalements des internautes qui repèrent sur le web des comportements ou des contenus publics qu'ils estiment illégaux, et pilote le projet Thesee qui a vocation à recueillir des signalements et des plaintes en ligne. Elle dispose également d'une plateforme téléphonique chargée d'orienter les victimes d'escroquerie, qui a reçu 66 000 appels en 2019.

Sur certains dossiers complexes, la SDLC joue un **rôle pleinement opérationnel**. L'OCLCTIC comporte ainsi trois brigades chargées respectivement de la répression des atteintes aux systèmes de traitement automatisé de données (STAD), des escroqueries commises sur Internet et des atteintes aux systèmes de paiement. Lors de son audition par les rapporteurs, la sous-directrice, Catherine Chambon, a indiqué que la SDLC était saisie de 275 dossiers. Elle a précisé que la SDLC se saisissait systématiquement, soit seule, soit en cosaisine, des affaires de rançongiciel.

La brigade sur les fraudes aux technologies de l'information de la préfecture de police

Au sein de la préfecture de police de Paris existe également une unité de police judiciaire spécialisée dans la lutte contre la cybercriminalité : la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI). Elle se saisit d'affaires relevant de l'accès ou du maintien frauduleux dans un système de traitement automatisé des données (STAD).

Créée en février 1994, la BEFTI emploie aujourd'hui vingt-cinq policiers spécialisés. Compétente sur le ressort de Paris et de la petite couronne, elle est composée de trois groupes « enquêtes et initiative » et d'un groupe d' « assistance ».

Elle apporte une assistance technique et matérielle aux autres services de la police judiciaire et aux commissariats du ressort. Elle contribue également à la diffusion d'une culture de cybervigilance et de cybersécurité auprès du grand public et des professionnels du secteur informatique.

b) Au sein de la gendarmerie

Au sein de la gendarmerie, c'est le **centre de lutte contre les criminalités numériques** (C3N) qui est chargé de piloter la lutte contre la cybercriminalité. Il est l'héritier du département de lutte contre la

cybercriminalité, créé en 1998 au sein du service technique de recherches judiciaires et de documentation de la gendarmerie.

Le C3N assume d'abord une mission de pilotage et d'appui spécialisé de l'action de la gendarmerie dans le domaine de la lutte contre la cybercriminalité.

Il peut également mener lui-même, ou coordonner, des investigations d'ampleur nationale. Lors de son audition, le général Jean-Philippe Lecouffe a indiqué que le C3N suivait une soixantaine d'affaires. Il traite en moyenne une centaine de dossiers chaque année et revendique un taux d'élucidation de 54 %, chiffre en baisse depuis la prise en compte des dossiers de rançongiciel, qui restent un point noir en matière d'élucidation.

Le C3N exerce également un rôle de veille en surveillant en permanence l'Internet pour détecter les infractions qui y sont commises et collecter des preuves. Il centralise les comptes rendus de police judiciaire émis par les unités de gendarmerie, ce qui lui permet d'évaluer les menaces et de procéder à des regroupements d'affaires traitées localement.

Le C3N est aussi en mesure d'apporter une assistance 24 heures sur 24 aux unités territoriales de la gendarmerie grâce à son guichet unique qui facilite les relations entre les enquêteurs et les opérateurs de téléphonie ou les fournisseurs d'accès à Internet.

Le C3N emploie actuellement 33 militaires. En 2020, l'effectif autorisé a été porté à 56 militaires (12 officiers et 44 sous-officiers), ce qui autorisera prochainement de nouvelles affectations. Le C3N anime un réseau de correspondants en technologie numérique (réseau CyberGend), qui compte aujourd'hui 5 300 gendarmes capables de conseiller leurs collègues et de procéder à certaines expertises, l'analyse d'un téléphone portable par exemple. Il s'appuie également sur 102 sections opérationnelles qui disposent, dans chaque département, d'enquêteurs en technologie numérique et de spécialistes des systèmes d'information. Il dispose enfin de neuf groupes régionaux pour traiter les cas les plus complexes ou les plus graves et envisage d'en créer deux supplémentaires pour compléter son implantation sur le territoire.

Au total, environ 5 500 gendarmes bénéficient d'une expertise en matière de cybercriminalité ; l'objectif de la gendarmerie est de faire passer ce chiffre à 7 000 d'ici à 2022.

Est par ailleurs rattaché au C3N le **centre national d'analyse des images de pédopornographie** (CNAIP) : il centralise, pour le compte de la police et de la gendarmerie, les fichiers saisis au cours des enquêtes, travaille à l'identification des victimes et des auteurs de ces contenus et fournit, le cas échéant, des images illicites aux agents habilités à réaliser des enquêtes sous pseudonyme.

c) Au sein du ministère de l'économie

Les services chargés à Bercy de la lutte contre la fraude contribuent aussi à la lutte contre la cybercriminalité.

(1) Les douanes

Au sein des douanes, la direction nationale du renseignement et des enquêtes douanières (DNRED) dispose, depuis 2009, de sa propre structure de lutte contre la cybercriminalité, appelée service des cyberdouanes ou encore cellule Cyberdouane. Ce service a remplacé le centre de recueil et d'analyse de l'Internet douanes (CRAIDO), créé en 1998. Il s'est notamment fait connaître auprès du grand public en septembre 2014 en démantelant un trafic de cannabis sur Internet et en récupérant une centaine de plants entreposés à Laval.

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-clefs 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.

Comme le notaient Albéric de Montgolfier et Philippe Dallier dans un rapport au titre de la commission des finances du Sénat de 2013, Cyberdouane mène donc une véritable « action sur l'offre », là où les contrôles douaniers plus classiques cherchent à agir sur les flux[1].

Lorsque les constatations douanières effectuées par Cyberdouane débouchent sur une enquête judiciaire, le parquet peut saisir le service national des douanes judiciaires (SNDJ) pour mener les investigations. Dirigé par un magistrat, ce service emploie des officiers de douane judiciaire (ODJ) habilités à mener des enquêtes sur l'ensemble du territoire.

(2) Tracfin

Depuis 2006, le service de traitement du renseignement et d'action contre les circuits financiers (Tracfin) est un service autonome à compétence nationale, compétent en matière de renseignement financier. Si sa mission porte majoritairement sur les circuits financiers clandestins, le blanchiment et le financement du terrorisme, il peut aussi être saisi dans des dossiers en lien avec la cybercriminalité.

---

[1] *Voir le rapport d'information n° 93 (2013-2014)* « Les douanes face au commerce en ligne : une fraude fiscale importante et ignorée », *d'Albéric de Montgolfier et Philippe Dallier au nom de la commission des finances.*

Tracfin reçoit des déclarations de soupçon adressées par des banques, des notaires, des agents immobiliers, etc., par d'autres administrations ou par ses homologues étrangers. Il peut procéder à une transmission judiciaire afin que des poursuites soient diligentées lorsqu'un dossier dont il est saisi présente un aspect pénal.

La cellule spécialisée sur la cybercriminalité au sein de Tracfin demeure de dimension modeste (trois agents, qui devraient bientôt être renforcés par un quatrième) au regard de l'effectif total du service (170 agents). Son activité porte surtout sur les *blockchains*, le *dark net* et la pédopornographie.

Lors de son audition, Maryvonne Le Brignonen, directrice générale de Tracfin, a souligné la qualité des relations entre son service et le système bancaire, tout en notant que le produit de la cybercriminalité s'échappe souvent très vite dans des pays moins régulés, rendant plus difficile le suivi de ces mouvements financiers frauduleux.

(3) Le service national des enquêtes

Institué en 2009, le service national des enquêtes (SNE) dépend de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

Il mène des enquêtes visant à la recherche et à la constatation des infractions au droit national et communautaire ainsi qu'à la collecte d'informations économiques en matière de qualité et de sécurité des biens et services, de loyauté des transactions, de protection des intérêts des consommateurs, de bon fonctionnement des marchés et d'équilibre des relations commerciales entre entreprises.

Le SNE comprend un centre de surveillance du commerce électronique, doté de près de soixante-dix agents, et une unité de renseignement. Ses efforts se concentrent surtout sur la surveillance des secteurs de la vente de billets d'avion en ligne et de la réservation d'hôtel en ligne.

2. Du côté de l'autorité judiciaire

Au sein de l'appareil judiciaire, la nécessité d'une spécialisation s'est également imposée : depuis l'entrée en vigueur 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, l'article 706-72-1 du code de procédure pénale confie au procureur de la République, au pôle de l'instruction, au tribunal correctionnel et à la cour d'assises de Paris une **compétence concurrente nationale** en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et

d'atteintes aux intérêts fondamentaux de la Nation (ce qui peut couvrir des hypothèses de cyber-sabotage).

Au sein du parquet, cette compétence est confiée à la **section J3**, anciennement dénommée section F1, ou section cybercriminalité.

Ce changement de dénomination est la conséquence de la réorganisation décidée par le procureur de la République de Paris, Rémi Heitz, au début de l'année 2020. Autrefois rattachée à la deuxième division du parquet chargée de l'action publique spécialisée, la section cybercriminalité est désormais intégrée à la troisième section qui traite les affaires relevant de la juridiction interrégionale spécialisée (JIRS) ou de la juridiction nationale de lutte contre la criminalité organisée (Junalco), c'est-à-dire des affaires se caractérisant, respectivement, par leur grande ou par leur très grande complexité dans le domaine de la criminalité organisée ou financière[1].

Au titre de sa compétence nationale, la section J3 peut se saisir des affaires de cybercriminalité complexes, où qu'elles se produisent sur le territoire, les parquets locaux demeurant compétents pour le reste du contentieux. Elle est seule compétente pour les infractions commises dans le ressort du parquet de Paris.

En pratique, elle exerce sa compétence nationale dans quatre hypothèses :

- en cas de pluralité d'auteurs ou de victimes sur le territoire, de manière à éviter la conduite d'enquêtes parallèles par plusieurs parquets locaux ;

- lorsque l'affaire présente une dimension internationale forte, la section J3 étant rompue aux procédures de coopération judiciaire européenne et internationale ;

- en raison de la technicité ou de la complexité du mode opératoire ;

- eu égard à la qualité de la victime, par exemple s'il s'agit d'un opérateur d'importance vitale, d'un ministère ou encore d'un sous-traitant de l'armement.

À ce jour, la section J3 a ouvert 249 enquêtes sur le fondement de cette compétence nationale, dont 225 sont toujours en cours. Ces affaires à dimension nationale ne représentent qu'une minorité des 2 757 affaires dont elle était saisie au début du mois de juin 2020.

La section J3 est avant tout compétente pour les atteintes aux STAD. Comme l'a expliqué aux rapporteurs Alice Chérif, cheffe de la section, son intégration dans la Junalco lui permettra d'intervenir plus facilement dans les dossiers où le numérique a été utilisé comme un moyen pour commettre l'infraction, sans qu'il y ait nécessairement eu une atteinte aux STAD.

---

[1] *La section J1 traite de la criminalité organisée et la section J2 de la criminalité financière.*

Une augmentation du nombre de saisines se heurterait cependant rapidement à une contrainte d'effectifs : la section J3 ne compte en effet que trois magistrats (ils n'étaient que deux jusqu'en septembre 2019), bénéficiant de l'appui d'un assistant spécialisé[1] dont l'apport technique est précieux pour faciliter la compréhension des faits. Au sein du pôle de l'instruction, quatre magistrats sont spécialisés dans la lutte contre la cybercriminalité ; deux de leurs collègues prennent en charge certains dossiers sans se consacrer entièrement à cette thématique.

En conséquence, comme l'a admis Alice Chérif, **la section J3 adapte le nombre de ses saisines à sa capacité à les traiter. Elle renonce régulièrement à se saisir de dossiers dont la complexité pourrait pourtant justifier une centralisation parisienne**.

Depuis 2019, chaque parquet local dispose d'un référent cyber, la liste de ces référents étant tenue par la direction des affaires criminelles et des grâces (DACG) à la Chancellerie. Il s'agissait auparavant d'une pratique qu'il a été décidé de systématiser l'an dernier. Le parquet de Paris a rassemblé une première fois l'ensemble de ces référents et prévoit de les réunir régulièrement afin de contribuer à l'animation de ce réseau.

3. Des services qui mériteraient d'être étoffés

Les professionnels entendus par les rapporteurs ont souligné la **qualité du travail fourni par les services chargés de lutter contre la cybercriminalité**. Alice Chérif a fait observer que si le parquet pouvait, en principe, requérir les services de l'ANSSI ou commettre des experts en informatique, les services d'enquête avaient en réalité les moyens techniques de mener eux-mêmes la plupart des investigations.

De nombreux exemples ont été donnés au fil de ce rapport d'affaires résolues par l'action de la justice et des services d'enquête. **Il n'y a donc pas d'impunité en matière de cybercriminalité**, même si la justice française se heurte encore trop souvent à la difficulté d'appréhender les auteurs d'infractions lorsque ceux-ci se trouvent à l'étranger, sur le territoire d'États peu coopératifs.

À l'échelle nationale, on constate une montée en puissance des moyens consacrés à la lutte contre la cybercriminalité, qui est cohérente avec la place croissante du numérique dans la vie quotidienne de nos concitoyens et dans l'activité économique. La gendarmerie notamment s'est fixé des objectifs volontaristes pour accroître encore ses capacités dans les deux ans qui viennent. **Le renforcement des moyens d'investigation apparaît indispensable pour faire face au développement de la criminalité dans l'univers numérique.**

---

[1] *Lors de l'audition organisée par les rapporteurs le 5 juin 2020, ce poste était vacant, le capitaine de police qui l'occupait ayant quitté ses fonctions sans être immédiatement remplacé.*

Par priorité, **ce sont les moyens du parquet spécialisé qui mériteraient d'être considérablement augmentés**. Un effectif de trois magistrats pour traiter les affaires de dimension nationale et internationale et animer un réseau de référents est **notoirement insuffisant**. Les effectifs du parquet spécialisé mériteraient **d'être décuplés** pour être portés au niveau de ceux des grands États européens les plus engagés dans ce domaine.

Si la spécialisation est nécessaire, elle ne doit pas être poussée à l'excès, compte tenu du caractère transversal de la cybercriminalité. Il est souhaitable que les équipes en charge de la cybercriminalité demeurent intégrées à des services de plus grande dimension afin que **des compétences variées puissent être mobilisées pour traiter une affaire**. Comme l'indique la direction générale de la gendarmerie nationale dans les réponses écrites qu'elle a adressées aux rapporteurs, il ne faut « pas aboutir à une trop grande spécialisation pour éviter de cloisonner une matière que l'on pense bien trop souvent hermétique aux techniques d'investigation classiques. C'est le cas pour le phénomène du *jackpotting*[1], où les techniques traditionnelles de terrain donnent plus de résultats que les investigations techniques ».

Indispensable pour traiter les dossiers les plus complexes, la centralisation doit s'accompagner d'**une diffusion de la culture cyber sur l'ensemble du territoire**, tant il est vrai que cette dimension est aujourd'hui présente dans un très grand nombre d'affaires qui ne peuvent pas toutes remonter à l'échelon central. Il convient donc d'encourager les efforts qui visent à former un plus grand nombre d'agents à ces problématiques et à constituer des réseaux de référents qui sont autant de relais pour une action efficace sur le terrain.

À cet égard, il est permis de se demander si une spécialisation de certains parquets régionaux, par exemple au niveau des JIRS, ne serait pas utile pour épauler le parquet de Paris qui pourrait ainsi se concentrer sur les affaires d'une très grande complexité ou particulièrement sensibles.

Il convient également **d'approfondir les liens entre les services en charge de la lutte contre la cybercriminalité et le secteur privé**. Les rapporteurs ont constaté que ces liens étaient déjà étroits. Le ministère de l'intérieur en particulier a mis en place des groupes de contact depuis 2015 afin de favoriser le dialogue avec les entreprises du numérique. L'objectif est notamment que les réquisitions judiciaires gagnent en efficacité : beaucoup de temps est économisé lorsque l'enquêteur sait de quelles informations dispose l'entreprise qu'il sollicite, dans quels délais elle peut les lui fournir et s'il parle le même langage que son interlocuteur.

---

[1] *Technique de piratage des distributeurs automatiques de billets.*

C. UN EFFORT DE PRÉVENTION À RENFORCER

Les rapporteurs ont été sensibilisés tout au long de leurs investigations à la question de la prévention, sur laquelle ils souhaitent procéder à quelques rappels indispensables.

1. Investir dans la cybersécurité

Les entreprises comme les administrations doivent veiller à ce que leurs systèmes d'information soient régulièrement mis à jour sur le plan de la sécurité. Elles peuvent bénéficier à cet effet des services de l'ANSSI qui joue un rôle important pour définir des normes techniques, ou de ceux de prestataires privés.

a) L'ANSSI, un acteur majeur de la cybersécurité

Créée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est rattachée au Secrétariat général de la défense et de la sécurité nationale. Elle est l'autorité nationale compétente en matière de sécurité des systèmes d'information.

Forte d'environ 600 agents et disposant d'un budget de près de 100 millions d'euros, elle contribue en premier lieu à la conception et à la coordination de la politique nationale en matière de sécurité informatique.

Elle joue ensuite un rôle important dans la prévention des attaques informatiques en aidant les ministères, les industriels et les opérateurs d'importance vitale à construire des **réseaux informatiques solides**. Elle procède à des **audits**, définit des **référentiels techniques** et promeut une offre nationale en matière de produits et de services de sécurité informatique en **certifiant des prestataires privés**. Elle assure des missions de formation des personnels qualifiés dans la sécurité des systèmes informatiques, en priorité en direction des administrations de l'État et des opérateurs d'importance vitale.

Elle joue aussi un **rôle de détection et d'alerte** quand une cyberattaque se produit. En son sein, le centre opérationnel de la sécurité des systèmes d'information (COSSI) travaille à l'analyse de la menace, à l'identification des vulnérabilités des systèmes et outils actuels, à la recherche des attaques en cours et à la définition des réponses à y apporter.

Elle remplit enfin une mission de **remédiation** en intervenant dans les grandes entités publiques ou privées victimes d'une attaque afin de les aider à appliquer des mesures correctrices urgentes et à rétablir leur système informatique.

L'ANSSI n'est pas un service d'enquête, mais elle peut échanger avec le parquet lorsque la justice est saisie d'une cyberattaque sur laquelle l'agence a travaillé. Elle n'est pas non plus un service de renseignement et ne procède ni à des attaques informatiques ni à des contre-attaques. Ce positionnement lui a permis de créer un climat de confiance avec l'ensemble des acteurs, propice à l'exercice de sa mission de sécurité informatique.

L'agence paraît disposer de moyens adaptés pour exercer convenablement sa mission, le principal frein à son développement résidant dans la difficulté de recruter les compétences pointues dont elle a besoin.

b) Les prestataires privés de cybersécurité

L'ANSSI intervient auprès d'acteurs de premier plan, mais ne peut répondre aux demandes de toutes les entités publiques et privées qui expriment des besoins en matière de cybersécurité.

Entendu par les rapporteurs, le *chief technology officer* de la société FireEye, David Grout, a évalué les dépenses de cybersécurité dans le monde à un montant compris entre 100 et 150 milliards de dollars.

Pour aider les clients à identifier plus facilement les prestataires les plus fiables en ce domaine, l'ANSSI délivre des **visas de sécurité** à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse. Avoir recours à l'une de ces solutions agréées participe à l'élévation du niveau de sécurité global des administrations, des entreprises et des citoyens face au risque numérique. En s'engageant dans une démarche d'obtention du visa de sécurité, le fournisseur de produit ou le prestataire de services concerné se donne les moyens de disposer d'une réelle valeur ajoutée concurrentielle, gage de compétitivité pour son entreprise et de sécurité pour ses clients.

Les acteurs du marché de la cybersécurité doivent s'adapter en permanence à l'évolution des techniques utilisées par les cybercriminels. Ils semblent qu'ils gagnent en efficacité puisque, comme l'a expliqué David Grout, le temps pendant lequel les attaquants sont présents dans un système avant que la victime ne s'en aperçoive (*dwell time*) tend à diminuer depuis cinq ans, ce qui témoigne d'une performance croissante.

Outre l'aspect technique de la sécurisation des réseaux et des équipements, il convient de souligner l'importance de la **sensibilisation des chefs d'entreprise et des salariés** à l'enjeu de la cybersécurité. La plupart du temps, c'est une imprudence humaine – ouvrir un spam ou cliquer sur un lien frauduleux – qui conduit à l'infiltration du réseau informatique.

La sous-direction en charge de la lutte contre la cybercriminalité de la DCPJ mène un travail de sensibilisation auprès des chefs d'entreprise : 1 200 ont été touchés au cours de la seule année 2019. Des initiatives notables ont également été prises au plan local au sein de la gendarmerie : la section opérationnelle de lutte contre les cybermenaces des Alpes-de-Haute-

Provence a par exemple mis en place un partenariat avec les entreprises du département afin de les aider à renforcer leur sécurité numérique, diffuser des recommandations et rappeler les bonnes pratiques. Le GIP Acyma conduit lui aussi des actions de sensibilisation en participant à des salons professionnels et en éditant des kits d'information aux risques liés au numérique ; en 2019, 37 760 kits complets de sensibilisation ont été téléchargés.

Dans le secteur public, les rapporteurs souhaitent appeler l'attention sur les investissements à réaliser dans les **établissements hospitaliers**, rendus plus vulnérables par la multiplication des objets connectés, ainsi que dans les **universités** qui constituent une cible de choix pour le cyber-espionnage, notamment de la part de la Chine.

2. La sensibilisation du grand public

Au-delà des entreprises et des administrations, le grand public mérite également d'être davantage sensibilisé à la cybercriminalité puisqu'elle cible aussi les particuliers.

Le GIP Acyma diffuse de l'information *via* son site www.cybermalveillance.gouv.fr, d'abord en direction du grand public. S'il a gagné en notoriété ces dernières années, son action pourrait être relayée par des **campagnes d'information** régulières dans les grands médias généralistes, sur la modèle de la campagne que le GIP a conçue en 2019 avec l'Institut national de la consommation (INC), diffusée sur France Télévision et sur des chaînes de la TNT.

Compte tenu de la vulnérabilité des mineurs, l'éducation nationale devrait également **sensibiliser les élèves à la sécurité numérique**. L'ANSSI a commencé à travailler avec le ministère en vue de développer des modules destinés aux élèves de seconde. Cette formation ne devrait pas se limiter aux aspects techniques, mais englober la prévention des infractions sexuelles et la question du respect de la vie privée.

Cette sensibilisation à l'école serait peut-être un moyen d'**attirer un plus grand nombre de jeunes vers les formations de l'informatique et du numérique**, qui demeurent trop peu souvent choisies alors qu'elles offrent d'excellents débouchés. Dans ce domaine, l'État d'Israël pourrait servir de modèle : les formations informatiques y sont valorisées, les capacités en informatique de tous les élèves sont évaluées à l'âge de quatorze ans et un enseignement en informatique y est dispensé de l'école primaire au lycée, avec la possibilité de suivre un cursus spécialisé en cyber-intelligence.

Cette attention à la formation n'est pas sans lien avec les succès économiques israéliens dans le domaine des hautes technologies. La France et l'Europe ne peuvent négliger cette dimension éducative si elles souhaitent rebâtir à terme leur souveraineté numérique.

III. LA COOPÉRATION EUROPÉENNE ET INTERNATIONALE, CLEF DE VOÛTE DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ, PHÉNOMÈNE TRANSNATIONAL PAR NATURE

La lutte contre la cybercriminalité, forme de délinquance ignorant les frontières, exige nécessairement une coopération internationale.

Le continent européen est en pointe dans cette lutte et bénéficie de l'action du Conseil de l'Europe et de l'Union européenne dont la coopération policière et judiciaire est de plus en plus intégrée.

A. LA GÉOGRAPHIE SANS FRONTIÈRES DE LA CYBERCRIMINALITÉ

Le **principe de territorialité de la loi pénale** donne compétence au juge répressif dès lors qu'une infraction est commise sur le territoire national, quelle que soit la nationalité des auteurs ou des victimes[1], même si la jurisprudence admet la compétence des juridictions françaises lorsque l'infraction commise à l'étranger a développé ses effets en France. Aussi, quand une enquête est ouverte en France, c'est généralement parce que les victimes s'y trouvent. Les auteurs eux-mêmes peuvent aussi s'y trouver, comme l'a montré cette affaire dans laquelle deux jeunes Français de 21 ans ayant envoyé des millions de messages électroniques de chantage à la vidéo intime (*sextorsion*) ont été arrêtés en France, fin décembre 2019, après que 28 000 personnes eurent signalé cette arnaque, et plus de 2 000 d'entre elles déposé plainte.

De même, les effets d'une décision de condamnation sont limités au territoire de l'État où elle a été rendue. De ce fait, un jugement de condamnation étranger n'est normalement pas exécutoire en France.

Or, la cybercriminalité est, par essence, un phénomène international : Internet permet de réaliser très rapidement quantité de délits dans plusieurs États. **Le cyberespace s'affranchit par nature de toutes les frontières étatiques**, d'autant plus que les cyberdélinquants ont tendance à commettre leurs délits dans des pays où la législation est embryonnaire, voire inexistante.

Ainsi, **beaucoup de cybercriminels se trouvent à l'étranger**, en particulier en Europe de l'Est – « Hackerville » est le surnom donné par la presse américaine à la ville roumaine de Ramnicu Vâlcea qui, selon elle, serait la capitale mondiale du vol sur Internet et où le FBI a envoyé une équipe épauler la police locale – dans l'ancien espace soviétique, ainsi qu'en Afrique. La directrice générale de Tracfin a par exemple expliqué que des centres d'appel se situant à l'étranger pouvaient organiser des escroqueries prenant la forme de faux investissements prétendument très rentables, dans des produits tels que des forêts, des terres rares ou des diamants, en incitant

[1] *Tel est le sens, par exemple, de l'article 113-2 du code pénal français.*

les victimes à s'enregistrer sur des sites Internet situés au Moyen-Orient, en Israël, en Europe de l'Est, voire au Royaume-Uni.

Il en est de même pour les atteintes sexuelles contre les mineurs sur Internet, qui impliquent très souvent des individus, les victimes en particulier, se trouvant non seulement hors du territoire national, mais aussi hors du territoire européen, en Asie en général. Cette situation constitue un **obstacle au traitement de ces affaires**.

Ainsi, tant les services enquêteurs que judiciaires peuvent se heurter aux frontières nationales et au principe de souveraineté dès lors que les États concernés ne veulent, ou ne peuvent, coopérer loyalement.

Il existe également des **zones de non droit**, propices à la prolifération d'activités illégales de toutes sortes, **y compris dans le cyberespace**. Par exemple, des cybercriminels se sont installés en Crimée depuis l'annexion illégale de ce territoire ukrainien par la Russie en 2014. Ils se trouvent ainsi à l'abri de toute procédure de coopération judiciaire : l'Ukraine n'a plus autorité sur ce territoire, et il est diplomatiquement inenvisageable d'émettre une demande à la Russie…

L'une des difficultés dans la lutte contre la cybercriminalité est que cette forme de délinquance mondiale défie les règles classiques de compétence législative fondées en grande partie sur la souveraineté étatique : les États sont libres dans l'organisation de leur système répressif de telle sorte qu'**une multitude de règles pénales nationales cohabitent**, ce qui pose problème en cas d'infraction concernant plusieurs États à la fois. **Le caractère international des infractions cybercriminelles est souvent source de difficultés pour déterminer la juridiction territorialement compétente pour juger de l'affaire.**

Le traitement judiciaire de la cybercriminalité appelle régulièrement des investigations transfrontalières.

Celles-ci sont rendues d'autant plus complexes que des informations doivent parfois être sollicitées auprès d'opérateurs étrangers ou dont les activités sont situées en territoire étranger, tels que les GAFAM[1], dont le siège se trouve aux États-Unis, ainsi qu'auprès des hébergeurs importants basés en Suisse.

Au total, **les cybercriminels paraissent souvent insaisissables**. Ils ne le sont cependant pas toujours, y compris les plus importants d'entre eux. Ainsi, le 23 janvier dernier, deux juges d'instruction du pôle financier du tribunal judiciaire de Paris ont obtenu de la Grèce l'extradition du Russe Alexander Vinnik, un grand délinquant du *darkweb*, également recherché par les États-Unis et la Russie. Dès son arrivée en France, il a été mis en examen pour blanchiment aggravé, association de malfaiteurs et piratage

[1] *Acronyme désignant les cinq principales entreprises américaines dominant le marché numérique, à savoir Google, Amazon, Facebook, Apple et Microsoft.*

informatique en bande organisée. Il est soupçonné de blanchiment d'argent sur la plateforme d'échange de bitcoins BTC-e, dont il est le fondateur, qui aurait été la plus grande « lessiveuse » de capitaux de la planète, avec un préjudice se chiffrant en milliards de dollars. La Russie a demandé son extradition à la France.

B. UNE NÉCESSAIRE COOPÉRATION INTERNATIONALE

Face aux limites de la coopération internationale classique, le Conseil de l'Europe a mis en place une convention innovante dont la portée universelle inspire les législations et les pratiques au-delà du Vieux Continent. Dans ce schéma d'ensemble, il est essentiel que l'Union européenne continue de coopérer étroitement avec le Royaume-Uni pour lutter contre la cybercriminalité.

1. L'entraide judiciaire internationale et ses limites

Toutes les conventions d'entraide judiciaire pénale, qui sont nombreuses, peuvent contribuer à lutter contre la cybercriminalité dès lors que l'infraction concernée relève de l'espace « cyber ». C'est le cas, par exemple, du traité de Paris de décembre 1998 entre la France et les États-Unis. Néanmoins, ce cadre bilatéral a, par définition, une portée restreinte.

La commission rogatoire est l'outil procédural privilégié d'entraide judiciaire permettant de poursuivre les infractions transnationales telles que les cybercrimes. Consistant, pour un juge, à confier à toute autorité judiciaire relevant d'un autre État la mission de procéder en son nom à des mesures d'instruction ou à d'autres actes judiciaires, elle porte sur tout acte d'instruction, l'audition des témoins, les perquisitions et saisies ou encore l'arrestation des suspects. Elle permet ainsi en théorie de surmonter les difficultés liées aux frontières.

Pourtant, la commission rogatoire est une procédure lourde à manier et présentant de longs délais de réponse ; elle est donc un outil lent par rapport à la vitesse d'exécution des infractions informatiques et la volatilité des preuves numériques.

Elle connaît **deux principales limites**.

La première tient à la subordination de la commission rogatoire à l'existence d'accords bilatéraux ou multilatéraux entre les États. Bien que l'envoi d'une demande ne soit pas, en principe, subordonné à l'existence d'une convention bilatérale entre l'État demandeur et l'État requis, l'existence de celle-ci conditionne souvent l'acceptation et la coopération des États. En l'absence d'une telle convention, le demandeur n'est jamais sûr d'une réponse positive. La recevabilité de la demande de commission rogatoire relève de l'appréciation de l'autorité compétente de l'État requis,

qui aura la possibilité d'invoquer l'exception de défaut de réciprocité et toute autre fin de non-recevoir. **Le principe de souveraineté permet en effet aux États de se dérober à leur obligation de coopération**, surtout lorsqu'il peut exister certaines tensions entre eux.

La seconde limite est relative aux difficultés liées à la portée de la commission rogatoire. L'exécution de la commission rogatoire dépend de la législation nationale de l'État qui reçoit la demande, la commission rogatoire étant exécutée conformément aux règles usuelles de procédures et de fond de l'État requis et non de l'État demandeur. Les traités bilatéraux, lorsqu'ils existent, peuvent limiter l'objet et la portée des commissions rogatoires. Certains traités limitent la commission rogatoire à l'audition de témoins ou la production de pièces à conviction ou des documents judiciaires. D'autres mesures d'instruction peuvent être subordonnées à des conditions particulières. Ainsi est-il généralement difficile d'obtenir des réponses positives de certains États tels que la Russie, la Chine ou Israël qui se montrent parfois réticents à communiquer des données stockées chez leurs fournisseurs d'accès à Internet. Il a également été indiqué aux rapporteurs que les services de police suisses souhaitaient rarement coopérer et qu'ils orientaient leurs collègues français vers cette procédure judicaire. Les autorités judiciaires américaines ne seraient pas non plus très allantes en matière d'entraide judiciaire internationale, alors que les GAFAM sont des entreprises américaines.

D'ailleurs, lors de la signature de la convention sur la cybercriminalité du Conseil de l'Europe, en 2001 (*cf. infra*), de nombreux États ont émis des réserves portant sur les demandes d'exécution de commission rogatoire, si la condition de double incrimination n'était pas remplie. En effet, la commission rogatoire suppose également une double incrimination, à savoir l'incrimination de l'infraction dans les deux États concernés. Or, de nombreuses cyberinfractions restent actuellement exclues de toute incrimination dans de nombreux États, **rendant ainsi la commission rogatoire inopérante dans de nombreux cas**. **Cette différence des règles nationales applicables peut compromettre l'instruction des infractions transnationales, ce qui permet aux cybercriminels de continuer à échapper à la justice.**

Cette difficulté peut se retrouver dans la lutte contre le blanchiment d'argent en ligne. Les standards du Groupe d'action financière (GAFI) définissent les modalités de coopération internationale et prévoient la réciprocité des échanges d'informations. Mais, selon Tracfin, la qualité des relations de travail diffère beaucoup selon la volonté de coopération de ses interlocuteurs étrangers : les échanges sont très bons en Europe, bons avec les pays d'Amérique centrale et du Sud et ceux du Golfe, qui ont adopté une démarche de coopération, mais ils le sont moins avec la Chine et même les États-Unis, d'autant plus que les services de renseignement financier de ces

derniers seraient dotés de pouvoirs d'investigation bien plus limités, ce qui réduit l'intérêt des informations transmises.

2. La convention de Budapest, « l'un des plus beaux succès du Conseil de l'Europe »

La sécurité de l'espace numérique se négocie dans un contexte mondial marqué par des intérêts et des objectifs divergents. Si l'Europe se positionne en faveur d'un Internet ouvert, ce n'est pas nécessairement le cas de certains de ses partenaires. Les négociations de conventions internationales en matière numérique sont rendues plus complexes par ce facteur géopolitique. C'est pourquoi elles aboutissent généralement à des textes de portée générale, dont le champ géographique est seulement régional ; tel est le cas, par exemple, de la convention de Malabo sur la lutte contre la cybercriminalité, qui concerne l'Afrique.

L'Union européenne, quant à elle, dispose d'une réglementation de plus en plus large en matière de cybercriminalité et de cybersécurité (*cf. infra*), mais pas d'un traité global. C'est pourquoi elle **soutient la convention sur la cybercriminalité du 23 novembre 2001, dite convention de Budapest, établie dans le cadre du Conseil de l'Europe, seul traité à portée universelle sur ce sujet**. Son objectif principal est de **poursuivre une politique pénale commune** destinée à protéger la société de la criminalité **dans le cyberespace**, notamment par l'adoption d'une législation appropriée et l'amélioration de la coopération internationale.

Certains États contestent toutefois le caractère universel de la convention de Budapest. Ainsi, à l'initiative de la Russie, l'Assemblée générale de l'ONU a, le 27 décembre 2019, adopté une résolution visant à établir une convention des Nations unies en matière de lutte contre la cybercriminalité. L'Union européenne et ses États membres s'étaient alors opposés à ce texte, estimant que le cadre juridique international actuel était suffisant et qu'il convenait de porter les efforts de la communauté internationale sur le développement de législations nationales et le renforcement des capacités. Depuis l'adoption de cette résolution, l'Union et ses États membres se coordonnent pour éviter que le nouveau processus de négociation pour une convention des Nations unies ne remette en cause l'équilibre nécessaire entre renforcement des moyens dédiés à la lutte contre la cybercriminalité et respect des droits fondamentaux et de l'État de droit, qui prévaut actuellement dans le cadre de la convention de Budapest.

La convention de Budapest est ouverte à l'ensemble des pays, au-delà des 47 États membres du Conseil de l'Europe – la Russie ne l'a ni signée ni ratifiée, contrairement à la Turquie. Elle compte d'ailleurs actuellement **65 États parties**, dont les États-Unis, et une centaine de pays s'inspireraient de ses dispositions dans leur législation nationale. Deux États membres de

l'Union européenne l'ont seulement signée sans la ratifier : la Suède et l'Irlande.

Cette convention, sans donner de définition de la cybercriminalité, aborde ce phénomène **sous deux angles : celui du droit pénal**, en visant des infractions qui doivent être intégrées dans la législation nationale des États parties, **et celui de la coopération internationale** – « dans la mesure la plus large possible » stipule l'article 23 –, en facilitant l'extradition entre États parties et l'entraide pénale judiciaire, par exemple par des échanges de preuves numériques localisées dans ces États. **Son champ d'application porte sur les atteintes aux systèmes d'information et de données, la fraude aux moyens de paiement et les atteintes aux mineurs en ligne.**

La convention de Budapest a été qualifiée par l'une des personnes auditionnées par les rapporteurs d' **« un des plus beaux succès du Conseil de l'Europe »**. Cet instrument a en effet démontré son efficacité : il permet une harmonisation des outils d'entraide tels que la conservation des données informatiques, très utile aux enquêteurs pour obtenir des preuves, l'injonction de produire, la perquisition et la saisie de données informatiques stockées ou encore l'accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public. Ce texte permet de « figer les scènes de crimes numériques » et donne ainsi la possibilité de remonter jusqu'aux auteurs des infractions informatiques. Par exemple, il constitue le fondement de la base de données relative aux commissions rogatoires internationales initiées par les autorités françaises. Les États-Unis, le Canada, l'Australie, le Royaume-Uni, l'Allemagne ou encore les Pays-Bas, ainsi que la France, comptent parmi les États parties les plus impliqués dans la mise en œuvre de la convention de Budapest.

La convention a également institué un **« réseau 24/7 »**, c'est-à-dire un point de contact joignable 24 heures sur 24, 7 jours sur 7, désigné par chaque État partie afin d'assurer une assistance immédiate pour mener des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Le point de contact français est l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), division de la sous-direction de la lutte contre la cybercriminalité au sein de la direction centrale de la police judiciaire du ministère de l'intérieur.

Le **comité de la convention sur la cybercriminalité**, qui représente les États parties, a pour objectif de faciliter l'usage et la mise en œuvre effective de la convention, l'échange d'informations et l'examen de tout futur amendement à la législation. Il publie des rapports et des notes d'information sur tout sujet se rapportant à la convention, en particulier sur l'interprétation des dispositions de la convention au regard des évolutions techniques intervenues, ce qui permet une adaptation souple de l'application

de la convention. Il publie également des formulaires d'utilisation concrète de la convention, sur la conservation des données par exemple.

Par ailleurs, la convention de Budapest donne lieu à des **programmes de coopération** en faveur des États parties les moins avancés, en Afrique, au Maghreb ou en Asie-Pacifique. Les actions de formation, en particulier le programme GLACY +, mis en œuvre conjointement avec l'Union européenne, sont conduites et coordonnées par le Bureau de programme sur la cybercriminalité (C-PROC), institué par le Comité des ministres du Conseil de l'Europe en 2013, situé à Bucarest.

La convention de Budapest fait, depuis septembre 2017, l'objet d'importantes négociations visant à la doter d'un deuxième protocole additionnel[1].

Celui-ci a pour objectif de **moderniser et compléter la convention sur plusieurs aspects** : une entraide juridique plus efficace (régime simplifié pour les demandes d'entraide, injonctions de produire internationales, coopération directe entre autorités judiciaires pour les demandes d'entraide, enquêtes et équipes d'enquête communes, audition audio/vidéo des témoins, des victimes et des experts, procédures d'urgence pour les demandes d'entraide) ; la coopération directe avec des fournisseurs de services dans d'autres juridictions pour ce qui est des demandes relatives à des informations sur les abonnés, des demandes de conservation et des demandes en urgence ; un cadre plus clair et des garanties plus fortes concernant les pratiques existantes en matière d'accès transfrontière aux données, et des garanties, notamment quant aux conditions relatives à la protection des données.

La Commission européenne a mandat, depuis juin 2019, pour participer à ces négociations au nom de l'Union européenne et de ses États membres. Les négociations donnent souvent lieu à des débats et soulèvent des interrogations sur la souveraineté territoriale dans le cyberespace. Elles sont prévues pour se terminer fin 2020, mais seront sans doute prolongées, du fait à la fois de la crise sanitaire et de la longueur des discussions. Le deuxième protocole additionnel, après son adoption, devra être approuvé par l'Assemblée parlementaire du Conseil de l'Europe puis ratifié par l'ensemble des États parties.

3. Les conférences Octopus

La lutte contre la cybercriminalité donne lieu, depuis 2007 et tous les 12 à 18 mois, à l'organisation d'un événement international, connu sous le nom de **conférence Octopus**. La dernière édition de la conférence a été organisée à Strasbourg, du 20 au 22 novembre 2019, dans le cadre de la

[1] *Le premier protocole additionnel à la convention de Budapest, du 28 janvier 2003, porte sur l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.*

Présidence française du Comité des ministres du Conseil de l'Europe, avec un ordre du jour portant notamment sur les preuves dans le cyberespace, l'exploitation et les abus sexuels d'enfants en ligne, les enjeux de la protection des données et de la justice pénale, la coopération en matière de cybercriminalité et de cybersécurité ou encore les *fake news* et l'ingérence électorale.

Les conférences Octopus réunissent des ministres, des représentants d'organisations internationales et non gouvernementales, des universitaires, des associations, des entreprises privées, en particulier les GAFAM, ou encore des représentants des autorités nationales de protection des données, telles que la CNIL française, soit environ 250 personnes.

Elles permettent de débattre des dernières évolutions, les cyberviolences par exemple, et de « tester » les réactions des acteurs du cyberespace.

4. Veiller à la qualité de la relation future de l'Union européenne avec le Royaume-Uni

Compte tenu de la forte implication des services britanniques dans la lutte contre la cybercriminalité, il est important, après le Brexit, que le nouveau partenariat entre l'Union européenne et le Royaume-Uni accorde une place éminente à ce sujet essentiel pour la sécurité de l'ensemble du continent européen.

Tel est l'objectif poursuivi par le mandat de négociation adopté, le 25 février 2020, par le Conseil Affaires générales de l'Union européenne. Ce texte indique que le partenariat envisagé devrait permettre, notamment : un dialogue sur la cybersécurité, incluant une coopération en vue de promouvoir au sein des instances internationales compétentes des pratiques mondiales efficaces en matière de cybersécurité ; un échange rapide et réciproque d'informations, notamment sur les incidents et les tendances en la matière ; une coopération, avec garantie de réciprocité, entre le Royaume-Uni et l'équipe d'intervention d'urgence informatique de l'Union européenne (*CERT-EU*).

Cependant, à ce stade, le Royaume-Uni n'a pas fait part de positions particulières sur la cybersécurité. Lors des dernières négociations, il a tenu des propos contradictoires sur le sujet, disant parfois ne pas exclure une coopération, tout en indiquant ensuite ne pas y tenir.

Lors de son audition devant les commissions des affaires européennes et des affaires étrangères, le 25 juin dernier, Michel Barnier, commissaire européen, directeur de la *task force* pour les relations avec le Royaume-Uni, a indiqué qu'il percevait un « mouvement britannique » dans les négociations sur les questions de sécurité intérieure, les Britanniques lui paraissant plus disposés à une coopération en matière de cybersécurité.

Il est nécessaire que l'Union européenne et le Royaume-Uni continuent de coopérer étroitement dans la lutte contre la cybercriminalité. Cela suppose également la **participation**, selon des modalités qui seraient définies par les négociateurs, **de ce pays aux agences européennes Europol, Eurojust et ENISA**.

Le Sénat avait d'ailleurs pris position en ce sens dans sa résolution européenne sur le nouveau partenariat euro-britannique.

Résolution européenne (n° 75) du Sénat du 6 mars 2020
sur le mandat de négociation du nouveau partenariat
Union européenne – Royaume-Uni (extraits)

– Concernant la sécurité intérieure et la coopération judiciaire

Rappelle que l'Union européenne et le Royaume-Uni partagent des valeurs communes et un attachement aux droits fondamentaux, illustrés notamment par l'adhésion des États membres et du Royaume-Uni à la convention européenne des droits de l'Homme ; souligne que l'Union européenne et le Royaume-Uni sont confrontés à des menaces communes de nature transfrontalière, en particulier le terrorisme et la criminalité organisée ; fait observer que le Royaume-Uni, en tant qu'État tiers, ne fait pas partie de l'espace Schengen, ne bénéficie d'aucun accès privilégié aux systèmes d'information de l'Union européenne et n'appartient pas aux agences européennes intervenant dans l'espace de liberté, de sécurité et de justice ;

Considère dès lors qu'il est indispensable d'instituer une coopération entre l'Union européenne et le Royaume-Uni permettant de répondre à ces menaces de façon à assurer la sécurité de leurs citoyens, dans le respect de l'autonomie de l'Union européenne et de la souveraineté du Royaume-Uni ; approuve les dispositions du mandat de négociation dans ce domaine de coopération, qui portent sur l'échange de données, la coopération opérationnelle entre services répressifs et judiciaires en matière pénale et la lutte contre le blanchiment de capitaux et le financement du terrorisme ;

Estime que le nouveau partenariat devra garantir un haut niveau de protection et de coopération dans ce domaine ; demande que les négociateurs prennent plus particulièrement en compte les normes et contrôles en matière de protection des données, y compris les données des dossiers passagers (PNR), les relations du Royaume-Uni avec Europol et Eurojust et les modalités d'extradition et d'entraide judiciaire, qui remplaceront le mandat d'arrêt européen ;

Appelle à instituer la coopération la plus étroite possible, dans le respect de l'autonomie de l'Union européenne et de la souveraineté du Royaume-Uni, dans les domaines de la cybersécurité et de la lutte contre la cybercriminalité et la migration irrégulière ; souhaite que la protection civile pour ce qui est des catastrophes naturelles ou d'origine humaine fasse également l'objet d'une coopération étroite ;

C. DONNER SA PLEINE MESURE À LA COOPÉRATION EUROPÉENNE

La mise en place progressive d'un espace judiciaire européen a pour objectif de pallier les difficultés inhérentes à la coopération interétatique, qui constitue encore un obstacle à une politique commune de lutte contre la cybercriminalité.

La coopération européenne en la matière a été jugée par tous les interlocuteurs des rapporteurs comme de bonne qualité. Elle ne pourra que s'approfondir si l'ensemble des États membres y participent effectivement.

1. Des marges de progression persistantes dans certains États membres

Les États membres sont engagés dans la lutte contre la cybercriminalité. Tous sont liés par la réglementation européenne, bénéficient du soutien des agences européennes compétentes et, à l'exception de la Suède et de l'Irlande, sont parties à la convention de Budapest.

Néanmoins, ils allouent à cette lutte des moyens inégaux. Par ailleurs, si la cybercriminalité les affecte tous, force est de constater que **tous ne sont pas impliqués de la même façon dans la coopération européenne**. Ainsi, les responsables compétents du parquet de Paris entendus par les rapporteurs ont indiqué que l'Allemagne, les Pays-Bas ou le Royaume-Uni comptaient parmi les pays européens les plus actifs en matière de coopération judiciaire, mais qu'ils n'avaient personnellement jamais été en contact avec des magistrats espagnols, italiens ou roumains. Ils se sont même demandé si l'Espagne, par exemple, avait des magistrats spécialisés dans le cybercrime. En revanche, les magistrats français reçoivent beaucoup de demandes de coopération de leurs homologues européens car la France héberge de grandes entreprises informatiques dotées de nombreux et puissants serveurs – OVH par exemple –, ce qui n'est pas forcément le cas de tous les États européens.

Des **marges de progrès** ont d'ailleurs été identifiées au cours du 7e cycle d'évaluation mutuelle sur la mise en œuvre pratique et opérationnelle des politiques européennes en matière de prévention et de lutte contre la cybercriminalité. La principale difficulté tient au **coût élevé des investissements à réaliser dans ce domaine pour acquérir l'expertise technique et humaine et pour rester à niveau**. De même, les **actions de formation** sont parfois conduites de manière cloisonnée et les services judiciaires n'y sont pas suffisamment impliqués. On l'a dit, certains États membres ne vont pas non plus assez loin dans la coopération de leurs services ou institutions en charge de la lutte contre la cybercriminalité avec leurs homologues des autres États membres. La mesure de la cybercriminalité est d'ailleurs rendue délicate non seulement par l'absence de définition harmonisée du phénomène, tant entre les États qu'au niveau

international, mais aussi par la qualité variable des statistiques, qui constitue un obstacle à leur agrégation et leur collecte. Enfin, des efforts restent nécessaires, dans plusieurs États membres, pour développer les **actions de prévention et de sensibilisation du public**, en particulier pour ce qui concerne les abus sexuels sur mineurs en ligne.

2. Un axe de la stratégie de sécurité intérieure de l'Union européenne

Prévenir et combattre la cybercriminalité, de même que renforcer la cybersécurité, constituent des priorités d'action de la stratégie de sécurité intérieure renouvelée pour l'Union européenne 2015-2020, adoptée en juin 2015**.**

Cet axe est abordé dans cette stratégie **sous deux angles** : **d'une part, l'attention particulière portée à la promotion de technologies de l'information et de communication sûres et sécurisées afin de renforcer la cybersécurité**[1] au sein de l'Union, et, **d'autre part, sur un plan opérationnel**, le rappel du **rôle de premier plan que doit jouer le cycle politique** de l'Union européenne[2] pour lutter contre la criminalité organisée.

L'actuel cycle politique de lutte contre la criminalité organisée, qui couvre les années 2018 à 2021, comporte ainsi une **priorité « cybercriminalité », subdivisée en trois thèmes** correspondant à autant de plans d'action opérationnels : **les attaques contre les systèmes informatiques**, ou *CAIS* (*Combating Against Information Systems*), **la lutte contre la fraude et la contrefaçon concernant les moyens de paiement autres que les espèces**, ou *NCPay* (*Non Cash Means of Payment Fraud*), **et la sécurité des enfants sur Internet**, notamment *via* la lutte contre la production et la diffusion de contenus à caractère pédopornographique, ou *CSA/CSE* (*Combating Child Sexual Abuse & Exploitation*).

La France est très engagée dans la mise en œuvre de la priorité « cybercriminalité ». Ainsi, en 2019, elle a participé à 194 actions du cycle politique, soit près de 80 % du total, dont 37 actions cyber. Elle est leader d'une action *CAIS*, co-leader de cinq actions (une autre action *CAIS*, deux actions *NCPay* et deux actions *CSA/CSE*) et participe à d'autres actions (treize actions *CAIS*, neuf actions *NCPay* et neuf actions *CSA/CSE*).

La stratégie de sécurité intérieure s'achevant à la fin de cette année, la Commission européenne a inscrit dans son programme de travail l'élaboration d'une nouvelle stratégie de l'Union européenne en matière de

---

[1] *L'Union européenne s'est par ailleurs dotée en 2013 d'une stratégie de cybersécurité (texte JOIN (2013) 1 final du 7 février 2013), actualisée en 2017 (texte JOIN (2017) 450 final du 13 septembre 2017).*

[2] *Le cycle politique est une méthodologie adoptée en 2010 par l'Union européenne : chaque cycle, qui dure quatre ans, prévoit les modalités d'organisation de la coopération opérationnelle dans plusieurs domaines de criminalité.*

sécurité, qui devrait logiquement porter aussi sur le terrorisme et la criminalité organisée, y compris dans le cyberespace, et sur la cybersécurité.

3. Une réglementation européenne qui s'enrichit progressivement

a) Le dispositif réglementaire en vigueur

De manière à pouvoir réprimer la cybercriminalité, l'Union européenne s'est dotée progressivement d'une réglementation que les États membres doivent transposer ou appliquer directement – on notera que **cette réglementation ne donne pas de définition de la cybercriminalité**. La Commission européenne élabore régulièrement des rapports de suivi et d'évaluation de manière à apprécier la mise en œuvre de cette réglementation au sein des États membres.

Cette réglementation européenne comporte actuellement plusieurs textes, dont les principaux sont les suivants :

- la directive 2011/93/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI : ce texte permet de mieux réprimer ces infractions en prenant en compte leur commission en ligne, par exemple le *grooming* (*cf. supra*) ;

- la directive 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision cadre 2005/222/JAI : ce texte vise à lutter contre les cyberattaques à grande échelle en invitant les États membres à renforcer leur arsenal législatif en matière de cybersécurité et à introduire des sanctions pénales plus sévères ;

- la directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite « directive NIS » : ce texte, qui s'inscrit dans la stratégie numérique lancée par l'Union européenne en 2010, vise à renforcer le niveau de sécurité des réseaux et de l'information dans un contexte où l'interpénétration des réseaux et des systèmes informatiques fait peser un risque collectif sur les États membres. Sa révision, annoncée pour 2020, a été maintenue dans le programme de travail révisé que la Commission a présenté dans le contexte de la pandémie de Covid-19 ;

- la directive (UE) 2019/713 du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI : ce texte actualise le cadre juridique, supprime les obstacles à la coopération opérationnelle et renforce la prévention et l'assistance aux victimes, pour rendre plus efficaces les mesures répressives contre la fraude et la contrefaçon des moyens de paiement virtuels ;

- le règlement (UE) 2019/881 du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), **dit *Cybersecurity Act*** : ce règlement définit la cybersécurité (« les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces ») et la cybermenace (« toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes »), réforme le mandat de l'ENISA, crée un cadre européen de certification de sécurité pour les produits et services et instaure un cadre européen de réponse aux crises cyber de grande ampleur (*Blueprint*) ;

- la décision (PESC) 2019/797 du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres : les cyberattaques relevant de ce régime de sanctions ont leur origine ou sont menées à l'extérieur de l'Union européenne, ou utilisent des infrastructures situées à l'extérieur de l'Union, ou sont menées par des personnes ou entités établies ou agissant à l'extérieur de l'Union, ou sont menées avec l'appui de personnes ou entités agissant à l'extérieur de l'Union ; les tentatives de cyberattaques ayant des effets potentiels importants sont également couverts par ce régime de sanctions.

b) Les négociations en cours sur le retrait des contenus terroristes

Au niveau européen, la lutte contre la cybercriminalité donne actuellement lieu à des **négociations sur la façon d'éviter la dissémination des contenus illicites en ligne, terroristes en l'espèce**.

Le 12 septembre 2018, la Commission avait présenté une proposition de règlement[1] relative à la prévention de la diffusion en ligne des contenus à caractère terroriste, dont l'objectif est de dépasser le cadre coopératif actuel, aux résultats jugés insuffisants[2]. Ce texte impose le retrait, dans l'heure, par tout fournisseur de service d'hébergement d'un contenu terroriste, à la demande d'un État membre. En cas contraire, celui-ci pourrait prononcer une sanction représentant jusqu'à 4 % du chiffre d'affaires annuel de la société. Le retrait sur une base volontaire demeure toutefois une option possible.

Ces éléments demeurent dans l'orientation générale adoptée par le Conseil JAI du 6 décembre 2018. Le Parlement européen a arrêté sa position en première lecture le 17 avril 2019, c'est-à-dire sous la précédente législature. La position du Parlement européen s'écarte significativement de

[1] *Texte COM (2018) 640 final.*

[2] *Cette proposition de règlement avait fait l'objet d'une communication de Jacques Bigot et André Reichardt devant la commission des affaires européennes, le 21 février 2019.*

celle du Conseil : les signalements (hors autorité nationale compétente) sont supprimés, les mesures proactives ne sont plus obligatoires, l'autorité compétente doit être soit judiciaire, soit administrative indépendante, ce qui remettrait en cause la plateforme française Pharos qui donne de bons résultats. Le principe du retrait dans l'heure, central dans la proposition de la Commission, est maintenu, mais seul l'État membre hébergeant le fournisseur de service d'hébergement aurait la faculté d'émettre une injonction dans ce sens, les autres États membres pouvant procéder à un géoblocage au niveau de leur seul territoire.

Les négociations interinstitutionnelles ont débuté à la mi-octobre 2019.

c) Les négociations en cours sur la preuve électronique

Un autre dossier important fait l'objet de négociations en cours : la preuve électronique (*e-evidence*).

Le Conseil JAI du 9 juin 2016[1] avait adopté des conclusions sur l'amélioration de la justice pénale dans le cyberespace, aux termes desquelles la Commission était appelée à présenter une initiative législative visant à accélérer et simplifier l'accès des magistrats aux éléments de preuve électronique, ce qu'elle fit, le 17 avril 2018, avec des projets de règlement[2] et de directive[3] sur l'accès transfrontière aux preuves électroniques. **Cette approche transfrontalière présente un intérêt opérationnel majeur compte tenu de l'importance prise par l'accès aux éléments de preuve électronique dans le cadre des enquêtes transnationales auxquelles donnent lieu de très nombreuses affaires de cybercriminalité.** Comme l'a indiqué la direction des affaires criminelles et des grâces du ministère de la justice, **dans trois quarts de ce type d'affaires, les preuves ne se trouvent pas en France**.

La conservation unifiée des données,
enjeu majeur dans la lutte contre la cybercriminalité

En juillet 2019, les agences Eurojust et Europol ont publié un rapport conjoint qui recense les principaux défis dans la lutte contre la cybercriminalité transfrontière, dont il ressort que, dans le domaine des cyberattaques, de l'exploitation sexuelle des enfants en ligne ou encore de la fraude aux paiements transfrontières, **l'absence de conservation unifiée des données reste un défi majeur pour les autorités répressives**.

[1] *C'est également lors de cette réunion du Conseil que mandat a été donné à la Commission pour négocier avec le Conseil de l'Europe le deuxième protocole additionnel à la convention de Budapest* (cf. supra).
[2] *Texte COM (2018) 225 final*.
[3] *Texte COM (2018) 226 final*.

Selon ce rapport, les **arrêts de la Cour de justice de l'Union européenne (CJUE) invalidant à plusieurs reprises les dispositifs nationaux et européens** ont laissé les services répressifs et les procureurs des États membres dans l'**incertitude quant aux possibilités d'obtenir des données des acteurs privés**.

Dans son arrêt *Digital Rights Ireland*, rendu le 8 avril 2014, la CJUE a invalidé les dispositions d'une directive de 2006 permettant aux opérateurs de télécommunications de stocker pour 6 à 24 mois maximum les données de téléphonie de leurs clients, afin que les forces de police puissent s'en servir à des fins de prévention ou d'enquête sur des faits de terrorisme et de criminalité grave, au motif qu'elles violaient gravement les droits fondamentaux. Dans leur rapport, Eurojust et Europol estiment que l'arrêt *Télé2Sverige*, rendu le 21 décembre 2016, aggrave encore ce problème. Dans certains États membres, la législation nationale est toujours en place pour garantir que les fournisseurs de services Internet conservent des données à des fins répressives, tandis que, dans d'autres, la législation nationale a été abrogée pour prendre en compte l'arrêt de la CJUE. Le rapport note ainsi que « de telles divergences entravent le travail des autorités compétentes et peuvent entraîner la perte de pistes d'enquête et, en fin de compte, nuire à la capacité de poursuivre efficacement les activités criminelles en ligne ». Selon les deux agences, **la majorité des autorités répressives et judiciaires des États membres serait favorable à un cadre législatif au niveau européen**.

Un mois avant la publication de ce rapport, le Conseil avait adopté des conclusions demandant à la Commission de préparer une étude approfondie sur de possibles solutions en matière de rétention des données de télécommunications à des fins répressives, y compris l'examen d'une future initiative législative. La Commission avait répondu favorablement à cette demande et assuré que l'étude serait disponible avant la fin de l'année 2019. Néanmoins, cette étude, confiée à un consultant privé, n'a pas encore été publiée et pourrait l'être à la fin juillet 2020.

Le projet de règlement introduit une injonction de production ou de conservation de données, adressée par l'autorité judiciaire d'un État membre pour les fins de la procédure pénale, directement aux fournisseurs de service Internet (FSI) actifs sur le territoire de l'Union, quel que soit leur localisation ou le lieu de stockage des données. Il cherche ainsi à dépasser le critère du lieu de stockage des données ou du siège social du FSI et retient le critère de la fourniture de services sur le territoire de l'Union. Cet accès s'effectuerait par des décisions européennes de production ou de préservation directement adressées aux opérateurs qui auront des délais courts pour répondre, à savoir 10 jours, et 6 heures en cas d'urgence. Quant au projet de directive, il instaure l'obligation pour les FSI de désigner un représentant légal dans l'Union chargé de recevoir et exécuter les décisions aux fins de la collecte de preuves par les autorités nationales dans les procédures pénales.

Ces textes ambitieux, dont la France soutient les principes, donnent lieu à des négociations serrées, en particulier avec l'Allemagne, sur la question de l'opportunité d'introduire un mécanisme de notification *ex ante* à

l'autorité compétente d'un État membre, ainsi que sur une possibilité d'injonction sur cette base. Les négociations ont permis de s'orienter vers un mécanisme de notification à l'État d'exécution avec un effet contraignant pour les données de contenu et un mécanisme de consultation de ce même État pour les données de transaction. Cette solution ne donnerait pas de droit d'opposition à l'État membre d'exécution, mais obligerait l'État membre d'émission à tenir compte des informations reçues pour s'abstenir d'émettre l'injonction, la retirer ou l'adapter. Ainsi, le dispositif ne s'appliquerait que dans les cas où la procédure comporte un aspect transnational – c'est-à-dire une personne visée résidant hors de l'État membre d'émission – limité aux données les plus sensibles (données de contenu et de transaction), au sein d'un système comportant plusieurs niveaux de vigilance et garanties.

Il conviendrait d'achever rapidement les négociations sur ces textes, qui se trouvent actuellement en phase de trilogues, même s'ils ne produiront pleinement leurs effets qu'en complémentarité avec le deuxième protocole additionnel à la convention de Budapest du Conseil de l'Europe, également en cours de négociation (*cf. supra*).

d) Les projets de la Commission von der Leyen

La Commission entrée en fonction à l'automne 2019 a inscrit plusieurs projets relatifs à la lutte contre la cybercriminalité dans son programme de travail 2020, intitulé « Une Union plus ambitieuse », qui relèvent de l'axe « numérique » et de l'axe « mode de vie européen ».

La Commission envisage d'explorer plusieurs pistes : les **opportunités offertes par l'intelligence artificielle**, y compris pour mettre cette technologie au service de la sécurité de l'Union et pour lutter contre les cybermenaces ; des initiatives visant à **rendre la finance numérique plus résistante aux cyberattaques**, par exemple une proposition sur les actifs cryptographiques[1] ; l'élaboration d'une **stratégie de lutte contre les abus sexuels sur mineurs**, qui devrait nécessairement comporter une dimension numérique ; une consultation visant à **apprécier l'opportunité d'une initiative législative en matière de lutte contre les vols d'identité**, phénomène cybercriminel ayant pris une ampleur préoccupante ces dernières années ; l'élaboration d'une **nouvelle stratégie de l'Union européenne en matière de sécurité** (*cf. supra*) ; une **révision du mandat d'Europol** devant permettre à cette agence de se doter des outils nécessaires pour mieux lutter contre la cybercriminalité.

Par ailleurs, en janvier 2020, la Commission a présenté une **« boîte à outils 5G » visant à garantir la sécurité des réseaux 5G** en renforçant les exigences de sécurité, évaluant les profils de risque des fournisseurs, appliquant des restrictions utiles aux fournisseurs considérés à haut risque et

[1] *Qui permettent des transactions avec des tiers virtuels de confiance.*

mettant en place des stratégies de diversification des fournisseurs. Un rapport sur le suivi de la mise en œuvre de cette « boîte à outils » est prévu à l'été 2020.

Sur la cybersécurité proprement-dite, la Commission a fait de la **défense de la souveraineté technologique de l'Union européenne** l'un des axes forts de son programme de travail. La stratégie numérique qu'elle a présentée le 19 février 2020 tend à déployer une stratégie européenne en matière de cybersécurité, avec la mise en place d'une unité conjointe de cybersécurité, une révision de la directive NIS et une impulsion donnée au marché unique de la cybersécurité.

Enfin, il conviendra de progresser dans la négociation de la proposition de règlement établissant le **Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité** et le **Réseau de centres nationaux de coordination**, qui avait été présentée par la Commission Juncker[1].

Ce texte, dont l'objectif est de contribuer à structurer la filière européenne de cybersécurité, vise à instituer un tel Centre européen pour une durée de sept ans et à lui confier l'attribution de subventions et la passation de marchés en matière de recherche et développement, de déploiement de technologies européennes, de soutien à l'industrie et de création de synergies avec le secteur de la cyberdéfense, dans le cadre des programmes pour une Europe numérique et Horizon Europe. Le Centre européen prendrait la forme d'un partenariat associant l'Union européenne, les États membres et l'industrie. Il s'appuierait sur un Réseau de centres nationaux de coordination chargés de recenser et de soutenir les projets les plus pertinents dans les États membres et de favoriser la participation de l'industrie à des projets transfrontaliers. Enfin, une communauté de compétences réunissant laboratoires de recherche et industriels serait instaurée pour favoriser la diffusion de l'expertise et des capacités et l'amélioration de la coopération et des synergies.

Après une interruption des négociations en mars 2019, à la suite du rejet du mandat de trilogue, les discussions ont repris, mais de nombreuses interrogations demeurent sur la nature juridique du Centre, sa gouvernance et sa capacité à mettre en œuvre les programmes-cadres.

4. Des agences européennes à vocation opérationnelle

L'Union européenne, dès 1996, a créé un comité d'experts chargés de la cybercriminalité. Puis elle s'est progressivement dotée de plusieurs agences qui, dans leur domaine de compétences, contribuent à lutter contre ce phénomène.

---

[1] *Texte COM (2018) 630 final du 12 septembre 2018.*

Par ailleurs, elle a cherché à assurer la sécurité informatique de ses propres institutions. Une décision de la Commission du 11 septembre 2012 a ainsi créé une équipe d'intervention d'urgence informatique, le *CERT[1]-EU*, dont la mission est de protéger les institutions européennes contre les cyberattaques. Dotée d'une trentaine d'agents issus de différentes institutions de l'Union, cette structure doit répondre à des incidents de sécurité et à des cybermenaces, 24 heures sur 24 et 7 jours sur 7. Ses missions relèvent à la fois de la prévention, de la détection, de la réponse et de la réparation des incidents informatiques ; il met également les structures nationales similaires en réseau et promeut ainsi une culture commune.

a) Europol et son Centre européen de lutte contre la cybercriminalité (EC3)

La lutte contre la cybercriminalité constitue l'une des missions de l'Agence de l'Union européenne pour la coopération des services répressifs, plus connue sous le nom d'Europol, et dont le mandat a été profondément révisé par le règlement (UE) 2016/794 du 11 mai 2016.

Dénuée de compétence propre d'investigation, Europol n'est pas un « FBI européen », mais a pour mission de soutenir les services de police des États membres dans la lutte contre la criminalité organisée sous toutes ses formes et contre le terrorisme, dès lors que plus d'un État membre est concerné. Le traitement de certaines affaires de cybercriminalité peut aussi conduire Europol à travailler avec des entreprises privées qui mettent à profit leur expertise, comme l'a expliqué l'un des dirigeants de FireEye, entreprise américaine spécialisée en cybersécurité, que les rapporteurs ont auditionné. L'agence conduit également des actions opérationnelles en matière de cybercrimes dans le cadre, plus large, de son cycle politique de lutte contre la criminalité organisée.

Europol a adopté, fin 2019, sa stratégie dite « 2020+ », centrée sur la lutte contre la criminalité organisée et 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 (*cf. supra*). La mise en place de ce laboratoire est confiée à l'équipe interne dédiée à la définition de la stratégie d'innovation, dirigée par un Français, Grégory Mounier.

Pour renforcer la réponse des autorités répressives à la cybercriminalité, Europol a créé en sein, en 2013, **le Centre européen de lutte contre la cybercriminalité (EC3)**, qui constitue le **point focal permettant de mettre en commun l'expertise européenne en la matière et de soutenir les enquêtes sur la cybercriminalité dans les États membres**. Depuis sa création, EC3 a été impliqué dans des dizaines d'opérations policières et des

[1] Computer Emergency Response Team.

centaines de mesures de soutien opérationnel à des services nationaux, à l'origine de plusieurs centaines d'arrestations. Son activité est en croissance régulière : EC3 a fourni un support opérationnel dans 57 affaires de cybercriminalité en 2013, 257 en 2018 et 397 en 2019.

EC3 dispose d'un effectif de 92 personnes, sur les 636 agents d'Europol affectés aux opérations (14,5 %) et d'un budget annuel de près de 13 millions d'euros (8 % du budget d'Europol consacré aux opérations). Le Centre est organisé en trois secteurs : la criminalistique, qui comprend deux équipes, numérique et documentaire ; la stratégie, avec deux équipes, la première chargée de nouer des partenariats et de coordonner les mesures de prévention et de sensibilisation, et la seconde responsable de l'analyse stratégique, de la définition de politiques et de mesures normatives et du développement d'une formation standardisée ; les opérations, avec une priorité donnée à la criminalité cyber-dépendante, l'exploitation sexuelle des enfants en ligne et la fraude au paiement.

Chaque année, EC3 publie un rapport stratégique, dit *Internet Organized Crime Threat Assessment* (*IOCTA*), qui expose les principales conclusions, menaces et tendances en matière de cybercriminalité. Cette évaluation annuelle met en évidence la **persistance de plusieurs menaces majeures**. Elle démontre également la complexité de la lutte contre la cybercriminalité et le fait que les cybercriminels n'innovent que lorsque leurs modes opératoires ont échoué. Les nouvelles menaces ne résultent pas seulement de technologies nouvelles ; elles proviennent de vulnérabilités connues des technologies existantes, qui affectent en particulier les données. Ainsi, selon l'*IOCTA* 2019, **le rançongiciel reste la principale menace** : même si une diminution du volume global d'attaques est observée, celles-ci sont plus ciblées, plus rentables et causent des dommages plus substantiels. Ce rapport relève également l'importance de la **fraude par carte**, du **faux message électronique d'affaires** ou encore de l'**attaque par déni de service distribué (*DDoS*)**. Le volume de **données pédopornographiques** détectées en ligne continue d'augmenter. Cette évolution exerce une pression considérable sur les ressources des services répressifs. Ces derniers ont, eux aussi, besoin d'avoir accès aux données pertinentes dans la conduite de leurs enquêtes, en raison de l'**utilisation accrue par les cybercriminels du cryptage permettant de masquer leurs traces et des crypto-monnaies pour dissimuler leurs revenus illicites**. En outre, les difficultés d'accès aux données pertinentes tiennent aussi au principe de territorialité, qui restreint la compétence et les pouvoirs d'enquête des forces de l'ordre et des tribunaux définis par le droit national.

Au-delà de la capacité répressive d'Europol, **EC3 a étendu son champ d'action, notamment en offrant un soutien opérationnel et analytique aux enquêtes des États membres**.

Ce soutien est illustré par la création, en septembre 2014, au sein d'EC3, de la ***Joint Cybercrime Action Taskforce* (*J-CAT*), compétente pour les cybercrimes de dimension internationale les plus importants**, car d'aucuns considéraient que l'action d'Europol était trop limitée à la « petite » cybercriminalité. Son objectif est de **conduire une action coordonnée, basée sur le renseignement**, contre les principales menaces et cibles de la cybercriminalité en facilitant l'identification, la hiérarchisation, la préparation, l'ouverture et la conduite conjointes d'enquêtes et d'opérations transfrontalières.

Son champ de compétences porte sur les crimes cyber-dépendants, la fraude au paiement transnationale, l'exploitation sexuelle des enfants en ligne et les cyber-facilitateurs (services anti-antivirus, utilisation criminelle du *darkweb*, etc.). Pour chacune de ces catégories, EC3 centralise l'information et le renseignement criminels, fournit diverses analyses relatives à la prévention et à la lutte contre la cybercriminalité, soutient les opérations et les enquêtes nationales en apportant une analyse opérationnelle, une coordination et une expertise, définit une politique de sensibilisation destinée à des acteurs publics et privés, soutient la formation et le renforcement des capacités des autorités nationales compétentes, fournit du soutien technique et numérique pour la conduite des enquêtes, représente la communauté des services répressifs de l'Union européenne dans des domaines d'intérêt commun (recherche-développement, gouvernance d'Internet et élaboration de politiques).

La *J-CAT* est dirigée par un conseil d'administration qui, conjointement avec EC3, définit l'orientation stratégique. Elle se compose d'une équipe opérationnelle comprenant des officiers de liaison provenant de neuf États membres (Autriche, France, Allemagne, Italie, Pays-Bas, Roumanie, Pologne, Suède et Espagne) et de pays partenaires hors Union européenne (Australie, Canada, Colombie, Norvège, Suisse, Royaume-Uni et États-Unis), complétés par du personnel d'EC3. L'ensemble de ces agents travaillent au siège d'Europol, dans le même bureau pour s'assurer d'une communication fluide entre eux. En outre, un expert national détaché d'Eurojust auprès d'EC3 coopère régulièrement avec la *J-CAT* pour discuter des cas et des projets d'intérêt mutuel. La *J-CAT* sélectionne et classe par ordre de priorité les affaires à poursuivre, sur la base des propositions des officiers de liaison.

Par ailleurs, Europol s'est doté, le 1er juillet 2015, d'une **unité de référencement Internet (*EU IRU*)**, disposant d'une équipe d'une quarantaine de personnes rassemblant des experts informatiques, des policiers et des gestionnaires. Son objet est de détecter des contenus, comptes ou sites Internet présentant un caractère terroriste afin de les signaler aux opérateurs en vue d'un retrait et d'un déréférencement. **Cette unité** n'a pas de pouvoir de contrainte : elle n'**émet** pas d'injonctions, mais **des signalements**, transmis préalablement aux États membres concernés ; les opérateurs sont

libres de donner suite ou non à ces signalements. Dans la pratique cependant, cette unité a noué des relations avec environ 400 opérateurs, pour un résultat qu'elle estime globalement efficace.

***EU IRU* enregistre et sauvegarde les signalements émis dans le système *IRMa*[1].** Des réflexions sont en cours pour faire évoluer I*RMa* : en plus des signalements d'*EU IRU*, cette plateforme recevrait l'ensemble des injonctions de retrait émises par les États membres. *EU IRU* deviendrait ainsi un organe de coordination au niveau européen, permettant d'éviter des doublons entre les différentes autorités nationales. Cette évolution présenterait plusieurs avantages : avantages d'ordre pratique et opérationnel, pour les États membres et pour les plateformes, plus grande traçabilité européenne des suites effectivement données aux injonctions de retrait (taux de retrait et de déréférencement, rapidité de l'exécution, difficultés rencontrées), élaboration commune de solutions, soutien aux petites plateformes et respect des équilibres s'attachant aux enjeux de souveraineté, les États membres restant seuls compétents pour émettre des injonctions de retrait.

Europol a également commencé à réfléchir à mettre en place en son sein une plateforme d'assistance aux victimes, sur le modèle du GIP Acyma en France, qui permettrait de les orienter rapidement vers les services de police compétents pour le signalement et le traitement de l'infraction, de manière à ne pas les laisser sans réponse.

Les relations qu'entretient la France avec EC3 passent par l'intermédiaire de la direction centrale de la police judiciaire (DCPJ) du ministère de l'intérieur, et plus précisément **de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)**, bureau de la sous-direction de la lutte contre la cybercriminalité au sein de la DCPJ. L'OCLCTIC assure les fonctions de coordonnateur de la lutte contre la cybercriminalité au niveau national et de point de contact unique pour la coopération internationale. Il est donc l'interlocuteur d'EC3, où il représente la France. L'OCLCTIC participe à deux programmes du cycle politique de l'Union européenne : *Cyberattacks Against Information System* et *Non Cash Payment Card Fraud*. Le programme *Child Sexual Exploitation*, en revanche, relève de l'Office central pour la répression des violences aux personnes de la DCPJ.

[1] Internet Referral Management application.

Les interactions entre EC3 et les services français de police et de gendarmerie

EC3 est devenu un relais important des actions policières françaises, et cela de différentes manières : les programmes quadriennaux (2018-2021) EMPACT de coopération policière, dont la première priorité porte sur le cybercrime, l'assistance de la *J-CAT* aux enquêtes françaises, le recours aux bureaux mobiles d'Europol dans le cadre d'opérations d'envergure, la participation aux semaines d'action commune (*Joint Action Weeks*) ou encore la mise en place d'outils opérationnels innovants. EC3 a ainsi permis la résolution d'enquêtes françaises majeures en mutualisant les moyens ou en facilitant le déplacement d'enquêteurs au-delà des frontières européennes pour procéder à l'arrestation de *hackers*.

L'utilisation par les services enquêteurs français des bases de données d'Europol, notamment la messagerie sécurisée SIENA, est quotidienne et améliore l'échange d'informations.

En outre, EC3 facilite les contacts des services français avec les autres États membres, permet l'organisation de réunions de coordination et sert de point de contact avec Eurojust, de plus en plus souvent associée aux enquêtes.

Par ailleurs, EC3 met à la disposition des États membres des capacités techniques complémentaires à celles développées à un niveau national, tels que des outils de déchiffrement et d'analyse des flux de crypto-monnaies ou des protocoles de réponse à incidents en cas de crises majeures.

Enfin, EC3 collecte des données pertinentes et les exploite rapidement afin d'améliorer la réponse policière. À ce titre, il joue un rôle stratégique en tant que « diffuseur de connaissances ».

Pour ce qui concerne la gendarmerie française, EC3 entretient également des relations étroites avec le centre de lutte contre la criminalité numérique (C3N). En moins d'un an, trois projets ont été menés dans le cadre des programmes EMPACT en matière de lutte contre le blanchiment au moyen de cryptocartes et contre des trafics de stupéfiants. Fin 2019, le C3N a impliqué Europol dans une affaire majeure permettant d'obtenir des renseignements très importants concernant les activités de plusieurs organisations criminelles. Des échanges réguliers ont lieu entre EC3 et le C3N pour lutter contre les *ransomwares*, par exemple pour mettre en place des outils permettant de casser des mots de passe. Le C3N participe également à des actions opérationnelles, ou *action days*, sur le *darkweb* et les atteintes sur mineurs. Les enquêteurs du Centre national d'analyse des images de pédopornographie (CNAIP), qui gère et exploite au plan national l'ensemble des images et des vidéos pornographiques impliquant des mineurs recueillies au cours des enquêtes judiciaires, interviennent dans la formation de policiers européens à la technique des enquêtes sous pseudonyme. Enfin, le C3N intervient également très régulièrement lors des conférences sur la cybercriminalité organisées par Europol, notamment au profit des groupes d'experts animés par EC3.

b) Eurojust

Créée en 2002, dans le contexte des attentats du 11 septembre 2001 aux États-Unis, par une décision du Conseil[1], modifiée en 2008[2], l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale, dite **Eurojust**, est une **entité de concertation des parquets nationaux de l'Union européenne**. Les compétences d'Eurojust ont été renforcées par le traité de Lisbonne : ainsi, Eurojust, qui pouvait déjà demander aux États membres d'initier une enquête – ceux-ci peuvent refuser, mais doivent motiver leur refus –, peut désormais **ouvrir elle-même cette enquête**. **S'agissant du déclenchement de poursuites, elle ne conserve qu'un pouvoir de proposition.**

Eurojust a connu une **réforme** en 2018[3] qui l'a **transformée en une véritable agence européenne** de manière à **améliorer son efficacité dans la lutte contre le crime transfrontalier et à prendre en compte la création du Parquet européen** qui, selon le traité, doit être institué « à partir d'Eurojust ».

Eurojust est compétente pour le même type de criminalité qu'Europol[4], ainsi que pour **la criminalité informatique**, la fraude, la corruption, les infractions pénales au détriment des intérêts financiers de l'Union, le blanchiment des produits du crime et la participation à une organisation criminelle.

Les missions d'Eurojust s'articulent autour de **trois objectifs majeurs** :

- promouvoir et améliorer la coordination des enquêtes et des poursuites entre les autorités compétentes des États membres ;

- améliorer la coopération entre ces autorités, en facilitant notamment la mise en œuvre de l'entraide judiciaire internationale et l'exécution des demandes d'extradition ;

- soutenir les autorités nationales afin de renforcer l'efficacité de leurs enquêtes et de leurs poursuites, par exemple au moyen d'équipes communes d'enquête, voire de centres de coordination, qui sont des dispositifs d'urgence mis en place en cas d'interpellations réalisées en commun.

---

[1] *Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité.*

[2] *Décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité.*

[3] *Règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil.*

[4] *Trafic illicite de stupéfiants, filières d'immigration clandestine, trafic de véhicules volés, traite des êtres humains, faux-monnayage et falsification, trafic de matières radioactives et nucléaires, cybercriminalité, terrorisme et criminalité organisée transnationale.*

Eurojust joue également un rôle déterminant pour **encourager la coopération judiciaire entre les États membres et les États tiers**, en particulier les pays des Balkans occidentaux et de la région Moyen-Orient et Afrique du Nord, mais aussi les États-Unis – pays particulièrement important en matière de lutte contre la cybercriminalité compte tenu de l'importance de l'industrie numérique américaine et de la présence de très nombreux serveurs sur son territoire. Elle a ainsi établi des points de contact en Algérie, en Égypte, en Irak, en Israël, en Jordanie, au Liban, en Arabie saoudite, en Tunisie et auprès de l'Autorité palestinienne, mais aussi en Colombie et en Libye. Eurojust dispose actuellement de points de contact dans 41 États tiers. Qu'un pays n'ait pas d'officier de liaison à Eurojust complique la tâche de cette dernière : ainsi, Eurojust n'a ouvert aucun dossier de cybercriminalité avec un pays d'Afrique subtropicale, ce qui ne veut pas dire pour autant que ce phénomène ne touche pas ces pays…

Chacun des 27 États membres a détaché un **représentant permanent** au siège d'Eurojust, situé à La Haye. **Ces représentants sont des procureurs, des juges ou des officiers de police.** Eurojust peut accomplir ses tâches par l'intermédiaire d'un ou plusieurs membres nationaux ou bien en tant que collège. Les membres nationaux sont secondés par des adjoints, des assistants et des experts nationaux détachés par les États membres – le bureau français comprend quatre magistrats. Ensemble, ils remplissent le mandat d'Eurojust afin de coordonner les autorités nationales à chacune des étapes d'une enquête criminelle ou de poursuites judiciaires, et résolvent également les difficultés et problèmes pratiques engendrés par les divergences entre les systèmes juridiques des différents États membres.

Par exemple, le membre national d'Eurojust pour la France peut être saisi d'une demande liée à une affaire de cybercriminalité par la section J3 du parquet de Paris ; le membre national pour un autre pays peut aussi saisir son homologue français pour être associé à une enquête concernant également son pays. Selon des informations obtenues par les rapporteurs auprès du membre national pour la France, et qui recoupent celles de la section J3 du parquet de Paris, les États membres les plus actifs en matière de cybercriminalité sont l'Allemagne, la France – notre pays compte parmi les pays concernés par les dossiers les plus anciennement ouverts et les plus importants –, les Pays-Bas, la Belgique et la Roumanie, ainsi que les États-Unis et le Canada pour ce qui concerne les pays partenaires. En revanche, certains États membres n'ouvrent jamais ou presque de tels dossiers, par exemple l'Espagne et l'Italie, à tel point qu'ils « sortent des radars » de la coopération européenne dans ce domaine.

Par ailleurs, Eurojust s'appuie sur le **Réseau judiciaire européen** afin de recueillir des informations sur les mesures d'application nationales de la réglementation communautaire en vigueur, les modalités de saisine des tribunaux, l'assistance juridique ou encore l'organisation et le fonctionnement des professions juridiques dans chaque État membre. Les

points de contact de ce réseau sont à la disposition des autorités judiciaires locales de leur État membre.

Lors du Conseil JAI du 9 juin 2016, les ministres européens de la justice ont adopté des conclusions sur la **mise en place, « avec l'appui d'Eurojust », du Réseau judiciaire européen en matière de cybercriminalité**, qui doit constituer « un centre d'expertise spécialisée » et faciliter et renforcer la coopération entre les autorités judiciaires compétentes intervenant dans le domaine de la cybercriminalité et de la criminalité facilitée par les technologies de l'information et de la communication et chargées d'enquêtes dans le cyberespace, dans le respect de la structure et des compétences au sein d'Eurojust et du Réseau judiciaire européen. Ce réseau permet de :

- faciliter les échanges de savoir-faire, de bonnes pratiques et d'autres connaissances et expériences pertinentes, y compris l'application pratique des cadres juridiques existants et de la jurisprudence pertinente et une coopération judiciaire transfrontière efficace ;

- encourager le dialogue entre les différents acteurs et parties prenantes qui contribuent à garantir le respect de l'État de droit dans le cyberespace, notamment Europol/EC3, Eurojust, l'ENISA, CEPOL, Interpol, le Conseil de l'Europe, le secteur privé, en particulier les prestataires de services, et d'autres organismes et réseaux concernés dans le domaine de la cybersécurité.

La direction des affaires criminelles et des grâces (DACG) du ministère de la justice représente la France au cours des réunions semestrielles de ce Réseau, qui se tiennent dans les locaux d'Eurojust ; ce Réseau n'est toutefois pas doté d'un secrétariat propre.

En **2019**, Eurojust a été saisie de **125 nouveaux dossiers de cybercriminalité**, soit environ 3 % de la totalité des dossiers dont l'agence est saisie, et de **72 depuis le début de l'année 2020**, ce qui laisse présager une augmentation totale du nombre de saisines par rapport à l'année précédente.

Eurojust se mobilise de plus en plus auprès des autres acteurs de la lutte contre la cybercriminalité, Europol en particulier – Eurojust dispose d'ailleurs d'un officier de liaison auprès d'Europol. Elle a conclu un accord de partenariat international incluant Europol et le FBI, qui a abouti au démantèlement d'un vaste réseau de cybercriminalité, prenant la forme d'un *botnet*. En prenant le contrôle de centaines, voire de milliers d'ordinateurs, les *botnets* permettent d'envoyer des pourriels ou des virus, voler des données personnelles ou réaliser des attaques *DDoS*. Ainsi, le *botnet* surnommé Avalanche, actif depuis 2009, a été démantelé le 30 novembre dernier après quatre ans d'une enquête ayant impliqué des enquêteurs de trente pays différents et permis d'arrêter cinq personnes, de bloquer 800 000 domaines et de saisir 39 serveurs. Le réseau Avalanche a piraté 500 000 ordinateurs et fait des victimes dans 180 pays ; leurs identifiants de

comptes bancaires étaient volés puis utilisés pour effectuer des virements ensuite blanchis par des complices.

c) L'ENISA

L'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a été instituée en 2004, pour une période de cinq ans, par le règlement (CE) n° 460/2004 du 10 mars 2004, remplacé par le règlement (UE) n° 526/2013 du 21 mai 2013. La durée du mandat de l'ENISA a été prorogée à plusieurs reprises puis **son mandat lui-même a été profondément révisé par le règlement (UE) 2019/881 du 17 avril 2019, dit *Cybersecurity Act*** qui prévoit deux domaines d'action supplémentaires : favoriser le recours à la certification européenne de cybersécurité et promouvoir un niveau élevé de sensibilisation des citoyens et des entreprises aux questions de cybersécurité.

Comme Europol et Eurojust, l'ENISA est une agence facilitatrice, et non un organe supranational de cybersécurité de l'Union européenne.

Dans l'accomplissement de ses tâches, elle agit de façon indépendante tout en évitant la duplication des activités des États membres et en tenant compte des compétences existantes de ces derniers. Sise à Héraklion, en Crète, mais disposant d'une antenne opérationnelle à Athènes, plus accessible, l'agence a vu ses moyens croître sensiblement. Son budget est ainsi passé de 11 millions d'euros en 2016 à **21,2 millions en 2020**, et ses effectifs de 84 agents à **111**, dont la moitié environ est constituée de contractuels. La mise en œuvre du *Cybersecurity Act* va conduire à augmenter encore ces moyens d'ici à 2024, avec un budget de 24 millions d'euros et des effectifs de 121 agents. Si ces moyens paraissent suffisamment calibrés à ce stade, l'agence éprouve parfois des **difficultés de recrutement** en raison à la fois d'une attractivité salariale insuffisante par rapport au secteur privé et d'un vivier réduit qui compte des ingénieurs très diplômés mais relativement peu nombreux et encore peu expérimentés.

L'ENISA a pour but de **parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union européenne** : elle encourage les États membres et les institutions, organes et organismes de l'Union à améliorer la cybersécurité et leur sert de **point de référence** en matière de conseils et compétences. Ainsi, à la mi-juin dernier, l'ENISA a mis en place, pour un an, un groupe de travail sur l'**intelligence artificielle**, composé de quinze membres représentant le secteur public, des entreprises privées, le monde associatif et celui de la recherche, ainsi que de sept observateurs issus des institutions européennes, dont la DG CONNECT de la Commission et Europol. Ce groupe de travail a pour objectif d'aider l'agence à identifier les menaces liées à l'intelligence artificielle et à élaborer des lignes directrices.

L'ENISA contribue à rapprocher les dispositions législatives, réglementaires et administratives des États membres relatives à la cybersécurité.

Elle a pour mission d'aider l'Union européenne et ses États membres à être mieux équipés et préparés pour prévenir, détecter et répondre aux problèmes de cybersécurité. Elle favorise le recours à la **certification européenne de cybersécurité** en vue d'éviter la fragmentation du marché intérieur, la plupart des États membres ayant aujourd'hui leurs propres normes de certification, et contribue à l'établissement et au maintien d'un cadre européen de certification de cybersécurité. La certification devrait sensiblement se développer dans les prochaines années, par exemple pour les objets connectés, le *cloud* et les systèmes industriels. L'engagement européen en la matière pourrait faire de l'Union européenne un leader et une source d'inspiration pour d'autres régions du monde, d'autant plus que les États-Unis sont plutôt hostiles à la certification, qu'ils considèrent comme contraire à la liberté du commerce.

L'ENISA **contribue également à l'élaboration des stratégies nationales de cybersécurité**, encourage la coordination entre équipes d'intervention en cas d'urgence et publie des rapports et études sur le sujet. Si elle s'adresse principalement aux gouvernements des États membres et institutions européennes, elle aide également le grand public, les universités et le secteur privé (PME, télécoms, fournisseurs d'accès Internet, etc.).

Par ailleurs, le *Cybersecurity Act* met en place un **réseau d'officiers de liaison nationaux** visant à renforcer les échanges entre autorités nationales et l'ENISA et à mieux informer les États membres sur les activités de cette dernière. **L'un des défis de l'ENISA sera de mobiliser l'expertise des autorités nationales compétentes en s'appuyant sur ce réseau.** L'ENISA pourra également accompagner les États membres dans le développement de capacités nationales de prévention et de réaction aux cyberattaques ciblant leur territoire. Elle pourra ainsi fournir une assistance sur demande pour évaluer l'impact d'un incident et faciliter sa gestion technique, notamment pour les incidents transfrontaliers de grande ampleur. L'ENISA devrait également apporter son expertise au futur centre cyber.

L'ENISA travaille en étroite collaboration avec Europol et son EC3. La coopération entre les équipes de sécurité informatique[1] et les forces de l'ordre est relativement nouvelle et résulte en partie d'un protocole d'accord conclu entre l'ENISA, C3N, l'Agence européenne de défense et le *CERT-EU* de la Commission.

[1] *Plus connues sous l'acronyme anglais de* CSIRT *(*Computer Security Incident Response Team*).*

De même, l'ENISA entretient de très bonnes relations avec l'ANSSI – le président de son conseil d'administration est d'ailleurs un agent de **l'ANSSI** – qui est l'**opérateur national constituant sa première source d'informations et d'expertise**.

d) Les autres structures de coordination et de travail

- **La coopération entre les agences**

Au niveau stratégique, les agences européennes relevant de l'espace de liberté, de sécurité et de justice se réunissent au sein d'un réseau informel, dit des agences JAI (Justice et affaires intérieures), qui est un lieu de partage d'informations, de bonnes pratiques et d'échanges. Ce réseau rassemble de nombreuses agences, dont Europol, Eurojust, l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL), l'Agence européenne des droits fondamentaux, Frontex ou encore le Bureau européen d'appui en matière d'asile (EASO), mais pas l'ENISA. Néanmoins, la directive 2013/40/UE relative aux attaques contre les systèmes d'information, dont l'objectif est de renforcer la coopération entre les autorités compétentes, mentionne les agences et organes spécialisés compétents de l'Union, tels qu'Eurojust, Europol et l'EC3, ainsi que l'ENISA.

En 2019, parmi les priorités du réseau informel des agences JAI, figurait la lutte contre la cybercriminalité. Celle-ci a notamment pris la forme de formations spécifiques organisées par le CEPOL ou de la rédaction de rapports d'analyse conjoints traitant, par exemple, des abus sexuels sur mineurs en ligne.

Au niveau opérationnel, la mise en œuvre du cycle politique permet aux agences JAI de coopérer entre elles dans le cadre d'actions spécifiques, y compris en matière de lutte contre la cybercriminalité. Ainsi, des prochaines actions conjointes, auxquelles les agences prendront part, sont prévues sur la surveillance des commerces illicites et des trafics sur Internet et le *darkweb*.

Enfin, **au niveau technique**, un **laboratoire d'innovation**, institué par le Conseil à l'automne 2019, devrait être **mis en place au sein d'Europol** dans l'objectif d'observer les grandes tendances apparues au titre du mandat de cette agence et de stimuler la recherche et l'innovation, en particulier en matière d'intelligence artificielle. Ce laboratoire réunira l'ensemble des agences JAI souhaitant se coordonner en vue de la mise en œuvre de projets qui bénéficieront aux États membres et d'abord à ceux dont les moyens sont plus réduits. La lutte contre la cybercriminalité et la mise au point de solutions technologiques communes aux États membres en matière de sécurité intérieure constituent les grandes priorités de ce laboratoire d'innovation, dont le champ d'action et l'organisation sont en cours de négociation.

- **Les groupes de travail**

La lutte contre la cybercriminalité est également traitée au sein de groupes de travail du Conseil et de la Commission, et de réseaux *ad hoc*.

Il est ainsi possible de citer :

- le groupe horizontal sur les questions cyber, au sein du Conseil, qui informe les États membres sur les sujets d'actualité et examine les initiatives législatives transversales ;

- le groupe de coopération NIS, institué par la directive éponyme pour accompagner les États membres dans sa transposition en élaborant des méthodologies communes, qui réunit les représentants des États membres – l'ANSSI pour la France –, de la Commission et de l'ENISA, dans le but de soutenir et faciliter la coopération stratégique entre les États membres, de favoriser l'échange d'informations, de renforcer la confiance mutuelle et de rehausser les capacités nationales de cybersécurité, par exemple en matière de formation et d'équipements techniques ;

- le forum Internet de l'UE, créé en 2015, à l'époque pour lutter contre la diffusion de contenus terroristes en ligne, qui réunit, sur une base volontaire, les États membres, des plateformes, des chercheurs et universitaires et des ONG, et dont le champ d'activités devrait être étendu aux contenus pédopornographiques et aux discours politiques extrémistes et violents.

5. La participation de l'Union européenne aux instances internationales compétentes

L'implication de l'Union européenne dans la lutte contre la cybercriminalité comprend également une **dimension internationale**.

Ainsi a-t-elle le **statut d'observateur à l'Office des Nations Unies contre la drogue et le crime**, principale enceinte internationale compétente en matière de lutte contre la cybercriminalité, au sein duquel elle coordonne une position commune, en lien avec les États membres, dans le cadre d'un groupe d'experts.

Par ailleurs, l'Union européenne **participe au Forum mondial de l'Internet contre le terrorisme**, initiative lancée en juillet 2017 par Facebook, Microsoft, Twitter et YouTube, visant à travailler de manière coordonnée au retrait des contenus terroristes en ligne. Ce Forum a créé une base d'empreintes numériques de contenus illicites partagée, de manière à éviter la réapparition de contenus retirés. L'Appel de Christchurch de mai 2019 cherche à faire évoluer ce Forum vers davantage de transparence et d'appui aux plus petites plateformes ; une gouvernance plus formelle a été mise en place et réunit l'Union européenne, des États et des plateformes.

L'Union européenne participe aussi aux travaux menés sur la cybersécurité au sein de diverses autres enceintes internationales telles que l'OSCE, l'OCDE, le G7 et le G20.

Surtout, l'Union européenne joue un **rôle actif dans le cadre de la convention du Conseil de l'Europe sur la cybercriminalité, dite convention de Budapest**, ouverte au-delà des États membres du Conseil de l'Europe et comptant actuellement 65 États parties (*cf. supra*). Depuis juin 2019, la Commission participe, au nom des États membres, aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest, dont l'objectif est de renforcer la coopération entre les États parties, notamment en matière d'accès à la preuve électronique et de mise en œuvre d'équipes communes d'enquête.

6. Vers un Parquet européen compétent dans la poursuite des cybercrimes ?

Les travaux des rapporteurs les ont convaincus que l'Union européenne devait encore améliorer son organisation pour **poursuivre les cybercriminels de façon plus systématique et plus efficace**, d'autant plus que la criminalité informatique ne va cesser de progresser dans les années à venir. La **menace** est donc **grandissante**. Or, **ces criminels mettent précisément à profit les différences des systèmes judiciaires dans l'Union européenne.**

Dans cet objectif, **le Parquet européen**, qui devrait être opérationnel à la fin de cette année, **pourrait contribuer à renforcer la lutte contre la cybercriminalité en diligentant des poursuites à l'échelle européenne**, en particulier sur les affaires transfrontières les plus importantes telles que *NotPetya* (*cf. supra*).

Cela demanderait une extension du champ de compétences du Parquet européen, actuellement limité aux infractions pénales portant atteinte aux intérêts financiers de l'Union européenne. L'article 86 du TFUE prévoit que le Parquet européen puisse voir sa compétence étendue à la **criminalité organisée transfrontalière. La cybercriminalité en est une forme.** Il s'agit même d'une délinquance complexe et de plus en plus organisée qui nécessite une connaissance de l'écosystème global et des tendances en matière de fraudes.

Des propositions d'élargissement de cette compétence ont d'ailleurs déjà été faites. Le Président de la République, lors de son discours de la Sorbonne de septembre 2017, et Jean-Claude Juncker, lorsqu'il présidait la Commission européenne, ont évoqué une telle extension aux infractions terroristes transfrontières, cette proposition ayant même fait l'objet d'une communication de la Commission en septembre 2018[1], tandis que les

[1] *Texte COM (2018) 641 final*.

conclusions du Conseil européen du 18 octobre suivant invitaient à « examiner l'initiative de la Commission ».

La compétence du Parquet européen en matière d'infractions cybercriminelles permettrait de **consolider la coopération judiciaire des États membres en matière pénale** et de **gagner en efficacité dans le traitement d'affaires touchant plusieurs États**, les enquêtes et les poursuites pénales dans l'ensemble des États membres participants étant mieux cordonnées et même impulsées au niveau européen. Par ailleurs, l'Union européenne parlerait d'une seule voix dans ce dossier qui, on l'a vu, fait l'objet d'une coopération internationale croissante. Enfin, cette orientation traduirait une **plus grande intégration du fonctionnement de l'Europe de la justice**.

Naturellement, les rapporteurs n'ignorent pas qu'une telle extension du champ de compétences du Parquet européen se heurterait à des obstacles. Ils en voient plus particulièrement deux, qui sont liés : d'une part, les réticences de certains États membres à porter atteinte à leur souveraineté nationale sur un sujet régalien comme celui-là – la création du Parquet européen dans sa forme actuelle avait déjà suscité des réserves et n'avait pu se faire que sous la forme d'une coopération renforcée –, et, d'autre part, des difficultés juridiques tenant à ce que l'extension du champ de compétences du Parquet européen requiert l'unanimité du Conseil européen, et donc aussi l'accord des États membres non participants.

C'est pourquoi les rapporteurs proposent une **approche prudente et progressive**, passant par la **conduite d'une réflexion sur les voies et moyens d'une telle extension du champ de compétences du Parquet européen**. Ils sont bien conscients qu'il s'agit d'une **perspective de long terme**, d'autant plus que le Parquet européen tel qu'il est prévu n'a pas encore commencé à fonctionner – il ne le fera pas avant le 20 novembre 2020.

Cette perspective ne peut elle-même s'affranchir d'une réflexion plus large sur la façon de **renforcer la souveraineté numérique de l'Union européenne** qui est aujourd'hui excessivement dépendante des serveurs des GAFAM et des technologies étrangères – les débats sur la place d'une entreprise comme Huawei dans le déploiement de la 5G en Europe, avec les risques à la fois techniques et politiques qu'il comporte, le montrent bien. L'Union européenne et ses États membres doivent se donner l'ambition de se doter de leurs propres outils en la matière.

EXAMEN EN COMMISSION

La commission des lois et la commission des affaires européennes se sont réunies le jeudi 9 juillet 2020 pour l'examen du rapport de Mme Sophie Joissains et de M. Jacques Bigot relatif à la lutte contre la cybercriminalité. À l'issue de la présentation, le débat suivant s'est engagé :

M. Jean Bizet, président de la commission des affaires européennes. – La pandémie virale que nous vivons se déclinera peut-être demain en pandémie numérique. Nous pourrions interroger l'ANSSI à ce sujet, notamment pour identifier les entreprises, en particulier françaises, compétentes pour lutter contre ces dangers.

Je relève un point de votre texte : à cause du Brexit, nous allons perdre un partenaire, mais j'aimerais que celui-ci reste notre allié dans la lutte contre la cybercriminalité car il dispose d'une réelle expertise. Le Royaume-Uni s'affranchit en matière de politique de défense, cela me désole, mais il faut que nous parvenions à maintenir un partenariat et une complémentarité.

Enfin, nous sommes encore sous le régime de la territorialité de la loi pénale – l'Europe, en la matière, c'est toujours le temps long et le vote unanime –, mais il faut envisager le parquet sous l'angle européen, car chaque internaute peut être impliqué dans la cybercriminalité.

M. André Gattolin. – Je suis membre de l'Assemblée parlementaire du Conseil de l'Europe et j'ai le sentiment que nous nous inspirons trop rarement de ce qui s'y fait ; le rappel de la convention de Budapest est à cet égard bienvenu.

S'agissant de la place d'Europol et d'Eurojust, j'ai eu la chance de mener une mission à La Haye, il y a six ans, et, en effet, à mon sens, il faut élargir leurs compétences et mieux les doter. La coopération est encore faible, mais on ne peut pas la décréter : il faut que les acteurs apprennent et aient envie de travailler ensemble. Le fait que nous ayons intégré ces agences dans le droit communautaire au lieu de renforcer la coopération entre les services nationaux a conduit à une baisse de la volonté d'intégration des organes nationaux. Le processus a conduit à trop bureaucratiser les institutions plutôt qu'à construire de la coopération.

À mon sens, la cybercriminalité est une chose trop sérieuse pour être laissée à des administrations, certes brillantes, comme l'ANSSI, mais dont les ressources humaines sont gérées sur un mode quasi militaire, sans beaucoup de souplesse et d'intelligence dans la conservation des compétences. Mon expérience m'a convaincu que le rôle des politiques était essentiel ; il faut associer les commissions parlementaires des deux chambres pour faire remonter l'information et mettre en place des législations adéquates.

Je m'étais inquiété, il y a trois ans, que tout le système d'échanges de Bpifrance se trouve sur le *cloud* de Microsoft, et je viens d'apprendre que les données relatives aux prêts à taux zéro du Gouvernement sont maintenant hébergées sur le *cloud* d'Amazon… Imaginez un piratage ou un détournement d'informations sur des données aussi stratégiques que l'état de nos entreprises ! Cela m'inquiète ; j'ai alerté les administrations et les ministères. L'ANSSI joue un rôle important en matière de sécurité, mais je ne comprends pas que ces données ne soient pas hébergées sur des *clouds* souverains.

Aujourd'hui encore, beaucoup de choses reposent sur des coopérations bilatérales. Au niveau européen, l'ENISA est une très belle institution, mais elle sert surtout à recevoir les « patates chaudes » que l'on n'a pas envie de traiter au niveau national.

Mme Marie Mercier. – En travaillant sur la pédopornographie, j'ai mesuré combien Internet était un royaume sans roi, sans lois et sans frontières, dans lequel l'imagination n'a pas de limite et la perversion est grandissante et glaçante. En visitant Pharos et l'Office central pour la répression des violences aux personnes (OCRVP), nous avons constaté le déficit considérable de moyens humains dont souffraient ces institutions par rapport à leurs homologues d'autres pays – on compte leurs agents sur les doigts de la main quand ils sont 150 ou 200 au Royaume-Uni, par exemple.

Les grands risques sont climatiques, épidémiologiques, mais aussi numériques : imaginons que l'on pirate le système informatique d'un hôpital, qui rassemble les données des patients. Aujourd'hui, on souligne qu'il y a beaucoup de personnels administratifs dans les hôpitaux, mais il faut prêter attention à ceux qui surveillent ces systèmes, les ingénieurs informatiques.

Je partage votre constat : nous devons prévoir beaucoup de mesures de contrôle et de répression. Sur l'accès à la pornographie des mineurs, les Britanniques sont allés très loin, mais le processus a échoué au dernier moment car la société qui a obtenu le marché du système de contrôle appartenait en réalité à des sites pornographiques payants. Faisons confiance à notre imagination vertueuse !

Mme Sophie Joissains, rapporteure. – Nous sommes en phase avec ce que vous dites, j'espère que nos travaux serviront à l'élaboration d'un prochain rapport et au renforcement des effectifs dans les organismes français compétents.

M. Jacques Bigot, rapporteur. – Dans le soutien à cette démarche, ce rapport marque une étape utile sur les plans national et européen ; j'espère que notre proposition de résolution européenne sera votée et qu'une suite lui sera donnée dans cette lutte à long terme !

M. Jean Bizet, président de la commission des affaires européennes. – Je reste attentif à ce que nos amis anglais ne divergent pas trop de ces objectifs…

La commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale et la commission des affaires européennes autorisent, à l'unanimité, la publication du rapport d'information.

La commission des affaires européennes adopte la proposition de résolution européenne disponible en ligne sur le site du Sénat, ainsi que l'avis politique qui en reprend les termes et qui sera adressé à la Commission européenne.

PROPOSITION DE RÉSOLUTION EUROPÉENNE

Le Sénat,

Vu l'article 88-4 de la Constitution,

Vu les articles 67 et 82 à 89 du traité sur le fonctionnement de l'Union européenne,

Vu la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001, dite convention de Budapest,

Vu la stratégie de sécurité intérieure renouvelée pour l'Union européenne 2015-2020,

Vu la communication conjointe de la Commission et de la Haute Représentante de l'Union pour les affaires étrangères et la politique de sécurité au Parlement européen et au Conseil du 13 septembre 2017 intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide », JOIN (2017) 450 final,

Vu la déclaration de la Haute Représentante, au nom de l'Union européenne, sur le respect de la primauté du droit dans le cyberespace du 12 avril 2019,

Vu sa résolution européenne n° 117 (2018-2019) du 21 juin 2019 sur la coopération judiciaire en matière pénale et la mise en œuvre du Parquet européen,

Vu le rapport stratégique, dit *Internet Organized Crime Threat Assessment*, 2019 du Centre européen de lutte contre la cybercriminalité d'Europol,

Vu les conclusions pertinentes du Conseil JAI du 9 juin 2016, du Conseil Affaires générales des 15 et 16 novembre 2016, du Conseil JAI du 18 mai 2017, du Conseil Affaires générales du 20 novembre 2017, du Conseil Affaires étrangères du 16 avril 2018, du Conseil Affaires générales du 26 juin 2018, du Conseil européen du 18 octobre 2018, du Conseil Affaires générales du 19 février 2019, du Conseil Affaires générales du 19 mars 2019, du Conseil Transports, télécommunications et énergie du 3 décembre 2019 et du Conseil Affaires générales du 10 décembre 2019,

Note que la forte croissance de la cybercriminalité constitue une menace affectant l'Union européenne et ses États membres, qui recouvre des formes variées aux conséquences potentiellement très lourdes ;

Observe que le cyberespace est dépourvu de frontières, ce qui constitue un défi pour les autorités répressives et judiciaires en matière d'enquêtes et de poursuites pénales, comportant un risque élevé d'impunité ; considère par conséquent que les cybercrimes doivent être traités dans le cadre de la coopération judiciaire en matière pénale, avec l'appui du réseau judiciaire européen en matière de cybercriminalité ;

Note que l'efficacité des enquêtes et poursuites pénales relatives aux cybercrimes est particulièrement tributaire de l'obtention et de la conservation de données aux fins de preuves numériques ; regrette l'absence de régime de conservation des données au niveau de l'Union européenne ; appelle par conséquent à l'adoption d'un régime européen de conservation des données permettant de répondre aux besoins opérationnels des services répressifs et judiciaires, prenant en compte les exigences de la jurisprudence de la Cour de justice de l'Union européenne et des tribunaux nationaux et respectueux des droits fondamentaux tels que le respect de la vie privée, la protection des données à caractère personnel, la non-discrimination et la présomption d'innocence ;

Juge nécessaire, pour mieux lutter contre la cybercriminalité et assurer la cybersécurité, d'allouer aux autorités répressives et judiciaires des États membres, à Europol et à Eurojust des ressources financières et humaines suffisantes pour faire face aux nouveaux défis que constituent les avancées technologiques et l'évolution des menaces, y compris par le renforcement des partenariats avec le secteur privé ; souligne l'importance de la formation à la sécurité numérique et considère que les agences européennes compétentes ont un rôle à jouer en la matière ;

Souligne le rôle central d'Europol et de son Centre européen de lutte contre la cybercriminalité ; invite l'ensemble des États membres à coopérer au mieux avec cette agence et à alimenter ses bases de données avec des informations complètes et de qualité ; appelle au renforcement d'Europol dans la lutte contre la cybercriminalité grâce à l'extension du champ de compétences de l'unité de référencement Internet *EU IRU* au signalement de l'ensemble des contenus illicites en ligne et à l'adaptation en conséquence de la base de données européenne de contenus illicites *IRMa*, au développement d'une plateforme de signalement des transactions bancaires frauduleuses, ainsi qu'au soutien à la création de dispositifs nationaux d'assistance aux victimes et à leur mise en réseau ; demande la mise en place rapide au sein d'Europol du laboratoire d'innovation qui permettra d'associer en amont les autorités répressives aux évolutions et au développement technologiques ;

Soutient l'action de l'ENISA en vue d'un cadre européen de certification en matière de cybersécurité ; souhaite que cette agence rejoigne le réseau des agences relevant de l'espace de liberté, de sécurité et de justice ; invite l'ENISA à renforcer sa coopération opérationnelle avec les autorités répressives et judiciaires ;

Estime que la lutte contre la cybercriminalité exige une coopération internationale efficace permettant de promouvoir la sécurité et la stabilité du cyberespace ; considère que l'amélioration de cette coopération requiert la ratification de la convention de Budapest par l'ensemble des États membres de l'Union européenne et la conclusion dans les meilleurs délais des négociations sur le deuxième protocole additionnel à cette convention ; souhaite le renforcement de la coopération entre l'Union européenne et le Conseil de l'Europe dans la lutte contre la cybercriminalité, dans le respect de leur mandat respectif ;

Estime que le Royaume-Uni doit demeurer un partenaire indispensable dans la lutte contre la cybercriminalité ; demande par conséquent que le nouveau partenariat entre le Royaume-Uni et l'Union européenne permette d'instaurer la coopération la plus étroite possible, dans le respect de l'autonomie de l'Union européenne et de la souveraineté du Royaume-Uni, dans les domaines de la cybersécurité et de la lutte contre la cybercriminalité, y compris pour ce qui relève de la coopération judiciaire ; considère que ce nouveau partenariat devra garantir les relations du Royaume-Uni avec Europol, Eurojust et l'ENISA, ainsi que les modalités d'extradition et d'entraide judiciaire, qui remplaceront le mandat d'arrêt européen ;

Estime que l'Union européenne doit s'organiser pour poursuivre plus efficacement les cybercriminels ; constate que la territorialité de la loi pénale constitue encore trop souvent un obstacle aux poursuites, en particulier lorsque les cybercrimes impliquent plusieurs États membres ; demande par conséquent la conduite d'une réflexion approfondie sur les voies et moyens d'une extension du champ de compétences du Parquet européen à la lutte contre la cybercriminalité ; est conscient qu'une telle évolution ne pourra intervenir, le cas échéant, que si plusieurs conditions sont réunies, en particulier l'unanimité au Conseil européen, le respect du principe de subsidiarité et le fonctionnement probant du Parquet européen dans son champ initial de compétences ; estime en effet que la centralisation au Parquet européen du traitement des affaires transfrontalières de cybercriminalité permettrait une plus grande intégration du fonctionnement de l'Union européenne face à des menaces grandissantes ;

Invite le Gouvernement à soutenir ces orientations et à les faire valoir dans les négociations en cours et à venir au Conseil.

PERSONNES AUDITIONNÉES

Mercredi 15 avril 2020

Pierre Penalba, commandant de police, auteur du livre *Cyber Crimes* (Albin Michel, janvier 2020)

Mercredi 22 avril 2020

Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Jeudi 23 avril 2020

Jérôme Notin, directeur général du GIP ACYMA (Actions contre les cybermalveillances), dispositif national d'assistance aux victimes d'actes de cybermalveillance

Jeudi 7 mai 2020

Cyrille Baumgartner, secrétaire général adjoint des affaires européennes, **Olivier Alary**, chef du secteur sécurité de l'espace européen, coopération policière et douanière, échange d'information, groupe horizontal drogue, protection civile, **François Gibelli**, chef du secteur industrie, télécommunications, numérique, énergie, environnement, climat, compétitivité, et **Constance Deler**, cheffe du secteur parlements

Maryvonne Le Brignonen, directrice générale de Tracfin

Vendredi 15 mai 2020

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

Lundi 18 mai 2020

David Grout, *chief technology officer* pour la région Europe, Moyen-Orient et Afrique de l'entreprise FireEye

Mercredi 20 mai 2020

Vanessa El Khoury-Moal, adjointe au chef du bureau de la négociation pénale européenne et internationale à la direction des affaires criminelles et des grâces du ministère de la justice, et **Emmanuel Kessler**, officier expert cybercriminalité à la sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire du ministère de l'intérieur

Jeudi 28 mai 2020

Jacques Martinon, chef de la mission de lutte contre la cybercriminalité à la direction des affaires criminelles et des grâces du ministère de la justice

Mercredi 3 juin 2020

Thierry Martin, responsable du bureau de liaison français d'Europol

Le général de division Jean-Philippe Lecouffe, sous-directeur de la police judiciaire à la direction des opérations et de l'emploi de la direction générale de la gendarmerie nationale du ministère de l'intérieur, **et le colonel Éric Freyssinet**, chef du pôle national de lutte contre les cybermenaces

Vendredi 5 juin 2020

Christophe Perruaux, procureur de la République adjoint, chef de la juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO), **et Alice Chérif**, vice-procureure, cheffe de la section J3 du parquet de Paris

Vendredi 12 juin 2020

Catherine Chambon, sous-directrice de la lutte contre la cybercriminalité à la direction centrale de la police judiciaire du ministère de l'intérieur, **et Olivier de Mazières**, délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces

Jeudi 18 juin 2020

Steve Purser, *Head of Core Operations Department*, à l'Agence de l'Union européenne pour la cybersécurité (ENISA)

Vendredi 26 juin 2020

Baudoin Thouvenot, membre national d'Eurojust pour la France