REVUE
de la gendarmerie nationale

REVUE TRIMESTRIELLE / JUIN 2022 / N° 272 / PRIX 6 EUROS
Sous la direction scientifique de Marc WATIN-AUGOUARD

FIC 2022

NUMÉRO SPÉCIAL

FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ 2022

Lutter contre la criminalité du XXIe siècle

Le FIC 2022 sera, à nouveau, un événement marquant dans le calendrier de la cybersécurité. Créé, il y a 15 ans, à l'initiative de la gendarmerie nationale, il devrait rassembler cette année près de 15 000 participants venus du monde entier.

L'Europe sera, bien sûr, au cœur des échanges, notamment en raison de la présidence française du Conseil de l'Union européenne (PFUE) qui a inscrit cette manifestation dans son programme.

Le FIC 2022 mettra en avant l'action du Commandement de la gendarmerie dans le cyberespace (COMCYBERGEND), dont la création, en 2021, témoigne des ambitions de la gendarmerie au service d'une cybersécurité au profit de tous : l'État, les entreprises, les administrations territoriales, les particuliers. Cette revue de la gendarmerie nationale, publiée traditionnellement à l'occasion du FIC, s'ouvre par un regard sur les victimes. De plus en plus nombreuses, hélas ! elles doivent recevoir un soutien approprié par les forces de sécurité. La légitimité de l'État repose en grande partie sur sa capacité à répondre aux sollicitations. D'où l'importance de la formation des personnels, d'une organisation qui assure une protection de proximité. Mais il nous faut aussi être capables de mieux maîtriser la lutte contre la cybercriminalité « criminalité du XXIe siècle », comme le soulignait le titre du 1er FIC, en 2007. 15 années se sont écoulées. Des progrès ont été accomplis, mais il faut accélérer les réformes, augmenter les moyens, adapter les modes d'action à ce nouveau fléau. Le renseignement criminel, la recherche de la preuve numérique, l'accès aux données sont des composantes essentielles des investigations numériques. Enfin, la Revue porte un regard sur l'Europe qui doit être une puissance numérique, faute de quoi tous les efforts resteront vains ou insuffisants. Cette Europe, construite sur le Marché commun, devenu Marché unique, doit développer des capacités de cybersécurité qui résultent à la fois de l'addition des forces de États membres, mais qui doivent aussi être le fruit de sa propre action, notamment par la mutualisation des moyens rares.

Bienvenue au FIC à tous les visiteurs qui pourront bénéficier de ces instants forts qui mêlent connaissances techniques et approches géopolitique de l'espace numérique. Bonne lecture de ce numéro traditionnel de la Revue de la gendarmerie à tous les lecteurs qui ne pourront pas venir et qui trouveront, dans cet ouvrage un aperçu des enjeux de la transformation numérique.

Général d'armée (2S) Watin-Augouard
Ancien directeur du CREOGN
Fondateur du FIC

FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ 2022

FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ 2022

LA VICTIME FACE AUX CYBERPRÉDATEURS : COMMENT MIEUX LA PRENDRE EN COMPTE DANS LE PROCÈS PÉNAL ?

Internet et les technologies numériques occupent une place centrale dans nos vies. En particulier, les jeunes générations se sont appropriés ces outils pour s'amuser, créer et partager des contenus ou tout simplement communiquer. Un véritable environnement virtuel est venu se superposer à l'environnement réel, au point parfois de totalement s'y substituer.

Mais, comme toute médaille a son revers, cette centralité des technologies numériques présente une part d'ombre. Si Internet a permis d'ouvrir des perspectives nouvelles en matière de communication et de commerce, ces nouveaux espaces sont autant de lieux où règne parfois la loi du plus fort.

Cyberescroqueries, cyberharcèlements, piratage, le nouveau monde a emprunté les pires défauts de l'ancien. Face à ces vagues de cyberdélinquance, les victimes se sentent parfois seules face au web. Pourtant, depuis plusieurs décennies la victime est au cœur de l'attention des politiques publiques. La place de la victime dans le procès pénal n'a cessé de s'affirmer et ce tout particulièrement s'agissant des parties civiles et du développement de leurs droits. L'article préliminaire II du code de procédure pénale, issu de la loi du 15 juin 2000, affirme par exemple que « *l'autorité judiciaire veille à l'information et à la garantie des droits des victimes au cours de toute procédure pénale* ». Dès lors, si les droits des victimes font partie intégrante du procès pénal, le maintien de cette garantie est un enjeu majeur à l'ère numérique.

XAVIER LEONETTI

Magistrat, Chef de la mission de prévention et de lutte contre la cybercriminalité

La lente reconnaissance de la place de la victime dans le procès pénal

L'Histoire judiciaire a connu une lente migration d'un système fondé sur l'accusation privée vers un système reposant sur l'action publique. Dans un premier temps, au cours de l'Antiquité, le système d'accusation privée a favorisé l'émergence d'un système judiciaire au détriment de la vengeance privée. Par la suite, le XII^{e} siècle a vu l'introduction de la procédure inquisitoire devant les juridictions ecclésiastiques, puis devant les juridictions seigneuriales et royales. À l'époque, la dénonciation fait son apparition, permettant de saisir le juge et de lui abandonner les poursuites. La poursuite d'office par le juge va ensuite progressivement s'imposer. Sous le règne de Louis XIV, la grande ordonnance de 1670 institue trois modes de déclenchement de l'action publique : la dénonciation, la plainte et la poursuite d'office par le juge.

Puis, dans la lignée du droit révolutionnaire, le code d'instruction criminelle et le code de procédure pénale vont étendre les prérogatives reconnues aux victimes. En particulier, la faculté de déclencher l'action publique, autrefois réservée à la citation directe, a été étendue à la plainte avec constitution de partie civile par le célèbre arrêt Laurent-Atthalin du 8 décembre 1906[1].

Vers une meilleure prise en compte des « victimes du web »

Aujourd'hui, la victime est devenue une préoccupation majeure des politiques pénales. De par sa qualité, elle occupe une place essentielle dans le procès pénal en qualité de partie, bénéficiant de ce fait des prérogatives qui sont attachées à ce statut.

Pour autant, face aux cybercriminels, les victimes se trouvent souvent isolées et parfois démunies. Dans un monde numérique où la cyberdélinquance a opéré une véritable « révolution industrielle », la victime est désormais noyée sous le flot des tentatives de cyberattaques et de fishing. La situation est inédite puisque aujourd'hui 100 % des internautes ont été victime, a minima, d'une tentative de cyberinfraction.

Confrontée à une « pandémie cyber » la victime doit à la fois adopter les gestes barrières de la cyberprotection mais également signaler toute infection malveillante. Pour ce faire, le signalement sur la plateforme Pharos constitue le point d'entrée de la connaissance des contenus illicites, pouvant le cas échéant conduire à l'ouverture d'une enquête. Au mois de janvier 2022 des individus s'étant filmés en train de traîner deux piétons depuis leur voiture ont pu être interpellés au moyen de dispositifs de signalement.

En matière d'escroqueries ou de fraudes bancaires les plateformes PERCEVAL et THESEE viennent compléter ce dispositif de signalement et constituent un lien nouveau entre les services de police et la population. Un signalement sur une plateforme offre l'avantage de l'immédiateté et de la facilité, par rapport à l'option d'un dépôt de plainte. De même le site cybermalveillance.gouv.fr offre des solutions de protection et remédiation gratuites et librement accessibles aux particuliers et aux entreprises.

Pour autant, le numérique ne peut se concevoir en substitution du lien humain offert par l'accueil dans un commissariat ou dans une brigade. De manière générale, la proximité et l'accessibilité du système judiciaire se conçoit au moyen de deux étapes complémentaires et parfois successives : l'une numérique et l'autre physique. À l'image du monde médical, la téléconsultation ne remplacera jamais totalement une consultation chez son praticien.

Le dépôt de plainte doit demeurer l'acte réflexe de toute victime

En matière correctionnelle, selon les dispositions de l'article 85 du Code de procédure pénale il n'est pas possible de déposer une plainte avec constitution de partie civile directement. Une plainte simple est désormais une condition préalable

1 Crim. 8 déc. 1906, DP 1907. 1. 207, note F. T. et rapp. Laurent-Atthalin.

indispensable[2]. Cette procédure permet d'éviter notamment les dépôts de plaintes fantaisistes ou infondés.

Au cœur de cette régulation, le procureur de la République dispose de l'opportunité des poursuites. Mais qu'en est-il lorsque des infractions sont dénoncées en ligne au seul sein de la communauté des internautes ? La tribune offerte par les réseaux sociaux est à la fois une chance de libération de la parole des victimes mais interroge également sur la garantie du principe de présomption d'innocence en dehors de toute procédure judiciaire. En effet, en l'absence de possibilité de procès pénal, en raison bien souvent des délais de prescription, Internet demeure le lieu de catharsis de la parole de la victime.

Or, le dépôt de plainte est une étape indispensable dans la prise en considération de la victime permettant l'introduction de nombreuses mesures destinées sinon à effacer, du moins à apaiser les troubles issus de l'infraction. Cette préoccupation se traduit, en amont du procès, par un effort conséquent d'information des victimes sur leurs droits et devoirs. C'est dans cette perspective que la Chancellerie met à disposition un guide des droits des victimes ; que les tribunaux judiciaires disposent de bureaux d'accueil et de renseignement ; que les commissariats et les brigades disposent de chartes d'accueil des victimes et de personnes formées ; qu'un tissu associatif d'aide aux victimes a été créé. En outre, la qualité de victime ouvre un accès au droit, par exemple au moyen de l'aide juridictionnelle.

2 La plainte avec constitution de partie civile n'est recevable qu'à la condition que la personne justifie qu'une première plainte à soit été classée par le procureur de la République soit qu'un délai de trois mois s'est écoulé depuis le dépôt de cette plainte.

Si bien qu'un post sur Internet ne remplacera jamais le fait de pousser la porte d'un commissariat ou d'une brigade pour déposer plainte. En effet, selon les articles 10-2 et suivants du Code de procédure pénale les victimes doivent être informées par les OPJ/APJ de leur droit. En particulier, de la possibilité d'obtenir « *réparation de leur préjudice, par l'indemnisation de celui-ci ou par tout autre moyen adapté, y compris, s'il y a lieu, une mesure de justice restaurative ; de se constituer partie civile soit dans le cadre d'une mise en mouvement de l'action publique par le parquet, soit par la voie d'une citation directe de l'auteur des faits devant la juridiction compétente ou d'une plainte portée devant le juge d'instruction ; d'être, si elles souhaitent se constituer partie civile, assistées d'un avocat qu'elles peuvent choisir ou qui, à leur demande, est désigné par le bâtonnier de l'ordre des avocats près la juridiction compétente, les frais étant à la charge des victimes sauf si elles remplissent les conditions d'accès à l'aide juridictionnelle ou si elles bénéficient d'une assurance de protection juridique ; d'être aidées par un service relevant d'une ou de plusieurs collectivités publiques ou par une association conventionnée d'aide aux victimes ; de saisir, le cas échéant, la commission d'indemnisation des victimes d'infraction, lorsqu'il s'agit d'une infraction mentionnée aux articles 706-3 ou 706-14 du présent code ; d'être informées sur les mesures de protection dont elles peuvent bénéficier ; pour les victimes qui ne comprennent pas la langue française, de bénéficier d'un interprète et d'une traduction des informations indispensables à l'exercice de leurs droits ; d'être accompa-*

gnées chacune, à leur demande, à tous les stades de la procédure, par leur représentant légal et par la personne majeure de leur choix, sauf décision contraire motivée prise par l'autorité judiciaire compétente ».

Le souci de protection des victimes se traduit également, depuis près de quatre décennies, par le développement d'un fonds de garantie des victimes d'infractions pénales, destiné à permettre ou faciliter l'indemnisation des victimes de certaines infractions. La loi n° 2008-644 du 1er juillet 2008 créant de nouveaux droits pour les victimes et améliorant l'exécution des peines a mis en place un service d'aide au recouvrement des dommages-intérêts pour les victimes (SARVI) qui permet aux victimes d'obtenir le versement total (inférieur à 1 000 €) ou partiel (dans la limite de 3 000 €) des sommes accordées par le tribunal au titre des dommages-intérêts ou des frais de procédure.

La spécialisation judiciaire face aux victimes du web et le réseau des cyber-référents

Les réseaux de communication électroniques ne connaissant pas de frontière terrestre ou politique, il est fréquent que des infractions visant des personnes françaises soient commises depuis un autre État. Afin d'améliorer la répression des phénomènes cyberdélinquants transnationaux, le législateur a introduit dans le Code pénal l'article 113-2-1 qui dispose que « *tout crime et délit réalisé au moyen d'un réseau de communications électroniques, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République* ».

Par ailleurs, dans le cadre d'une cyber-attaque, il est possible qu'une partie de l'infrastructure technique (par exemple un serveur informatique) soit localisée sur le territoire, ce qui est un élément constitutif de l'infraction, entraînant la compétence des juridictions françaises.

Dès lors, si toutes les juridictions peuvent connaître de faits de cybercriminalité, des compétences spéciales ont été instituées pour leur traitement. 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 a ainsi attribué à la juridiction parisienne une compétence nationale concurrente en matière d'atteintes aux STAD.

Aussi, l'augmentation exponentielle et l'évolution des diverses formes de cybercriminalité, de même que l'intégration de la section « cyber » du parquet de Paris (J3) à la Juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO), ont conduit à préciser le rôle des différents acteurs judiciaires en la matière. Il résulte ainsi de la dépêche du Garde des Sceaux en date du 9 juin 2021 que les compétences des juridictions locales, des juridictions inter-régionales spécialisées (JIRS) et du tribunal judiciaire de Paris ont vocation à s'articuler en fonction de la nature et du degré de complexité de l'affaire, au regard de plusieurs critères objectifs.

Dans le même temps, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment en lien avec le phénomène de « cybérisation » de la criminalité organisée. Ainsi, la désignation et la formation de « cyber-référents » au sein des JIRS mais également au sein de parquets locaux a permis d'une part de créer un réseau judiciaire d'échanges entre les acteurs de la lutte contre la cybercriminalité et, d'autre part, de mieux spécialiser la prise en compte judiciaire de ce contentieux.

À l'heure du big data, de l'open data, du cloud, des objets connectés, des smartphones, les failles de sécurité constituent un moyen de pénétration dans les systèmes de traitement automatisé. Dans le même temps, les réseaux sociaux constituent des lieux propices à la diffusion de la haine en ligne et plus que jamais la victime se trouve à portée de clic des cyberdélinquants.

Aussi, face à la multiplication des menaces et des victimes potentielles, un renforcement de la lutte contre ces délits de type nouveau et évolutif est nécessaire, en particulier s'agissant du volet d'aide aux victimes. Dans cette optique, le chef de l'État a annoncé la création de 1 500 cyberpatrouilleurs dans le cadre d'un plan d'investissement d'un milliard d'euros pour renforcer la lutte contre la cybercriminalité. La mise en place d'une plateforme numérique équivalente aux « appel I17 » est également prévue afin que chaque citoyen puisse signaler en direct une cyberattaque.

Xavier LEONETTI en bref :

Titulaire d'un doctorat en droit, Xavier Leonetti a d'abord exercé les fonctions d'officier de gendarmerie avant de rejoindre la magistrature. Successivement en poste au parquet général d'Aix en Provence puis à la JIRS de Marseille, il est également l'auteur de plusieurs ouvrages « Smartsécurité et cyberJustice » (2021, PUF), « Le petit RGPD » (2021, Dunod) et à paraître « Cyberguide, mode d'emploi » (PUF, mai 2022).

CYBERCRIMINALITÉ : LA PROTECTION DES VICTIMES, UNE PRIORITÉ D'EUROPOL

Pour l'Union européenne, la protection des organisations, des entreprises et des citoyens, contre les cyber-menaces, est une priorité. Europol est l'agence de l'Union européenne pour la coopération des services répressifs. Dans le cadre de sa mission de soutien aux investigations des services répressifs (Law enforcement) contre la criminalité organisée, le terrorisme et la cybercriminalité, Europol contribue pleinement à cette priorité de l'UE. L'action d'Europol repose sur un cadre d'intervention et des capacités. Ces atouts vont permettre la réussite des investigations qui constituent une part importante de la réponse aux attentes des victimes.

Au sein de l'UE, Europol est en charge de fournir un soutien aux services d'application de la loi (police, gendarmerie, douanes) des pays membres, qui sont confrontés à des cybercriminels exploitant à leur avantage la dimension transfrontière de l'espace numérique. Le mandat de l'agence couvre les affaires de crime organisé ou de terrorisme, concernant plusieurs pays membres. Elle peut soutenir les cas les plus complexes nécessitant des mois d'investigation et des moyens conséquents. Elle répond à des menaces souvent massives, ciblant un grand volume de victimes.

JEAN-PHILIPPE LECOUFFE

Général de corps d'armée, Directeur exécutif adjoint d'Europol

Son centre dédié à la lutte contre la cyber criminalité, EC3 – European Cyber-Crime Centre, dispose d'experts en lutte contre les cyberattaques (rançongiciels, malwares, Botnets,..), contre certaines fraudes en ligne (skimming, phishing, usage frauduleux de données bancaires, fraude à la téléphonie..), contre les abus de mineurs en ligne, contre la fourniture de moyens criminels sur le darknet. D'autres services au sein de l'agence, œuvrent aussi contre les menaces numériques qui ont un caractère horizontal. C'est le cas des autres centres : le Centre de lutte contre la criminalité organisée (European Serious and Organised Crime Centre – ESOCC), le Centre de lutte contre la criminalité économique et financière (European Financial and Economic Crime Centre – EFECC) ou du Centre européen de lutte contre le terrorisme (European Centre for Counter Terrorism – ECTC), dont le dispositif SIRIUS propose aux enquêteurs un soutien méthodologique et des outils pour l'obtention d'informations numériques auprès du secteur privé, en appui à leur enquête sur l'espace numérique.

Sur la base de ces capacités, Europol mène des opérations au bénéfice des victimes. Quatre principaux modes d'engagement sont identifiables : l'identification des victimes, la mise hors état de nuire

des cybercriminels, l'aide à la réparation des dommages, la prévention de nouvelles victimes.

Un premier engagement repose sur l'identification des faits et des victimes se trouvant parfois en situation de grande vulnérabilité, comme les mineurs victimes d'abus sexuels, dont les images sont diffusées en ligne. Des opérations spéciales visant à les identifier (victim identification taskforce) sont régulièrement organisées. En novembre 2021, la 10e édition de l'opération a réuni dans les locaux de l'agence, 40 enquêteurs de 24 pays, qui ont identifié 18 victimes et permis l'arrestation de 4 suspects. Plus de 150 éléments d'information ont été diffusés à des services locaux pour des enquêtes à poursuivre. Depuis 2014, ces opérations ont vu plus de 533 mineurs sécurisés et 182 individus arrêtés.

Un système d'analyse d'image et de vidéo a été développé pour soutenir ce travail d'identification. Il contient près de 64 millions de contenus, ce qui en fait l'un des principaux outils mondiaux, permettant d'opérer un recoupement optimisé des informations.

Le programme « stop Child abuse-Trace an Object » est un autre outil innovant. Toute personne peut se connecter au site en ligne qui propose des photographies d'objets particuliers (vêtements, lieux) en lien avec la commission des actes. Toute information recueillie peut utilement orienter les recherches sur les pays concernés et les autorités compétentes. De 2017 à 2021, 250 objets présentés en ligne, ont généré plus de 27 000 réactions du public, sauvant 23 mineurs victimes. 18 enquêtes sont en cours sur la base d'informations issues de la dernière édition de cette opération (www.europol.europa.eu/stopchildabuse), qui a été adopté par la police australienne.

Les opérations « E-commerce et Carding action weeks », menées dans le cadre du plan opérationnel d'action EMPACT (European Multidisciplinary Platform Against Criminal Threats) et soutenues par l'agence, mobilisent les enquêteurs dans une vingtaine de pays de l'UE, notamment contre l'utilisation de données bancaires dérobées par des groupes criminels. L'identification sur le darknet, des données compromises permet de prévenir leur utilisation avant préjudice, l'identification des transactions permet aussi d'identifier les propriétaires légitimes des cartes bancaires pour les inviter à déposer plainte.

Un second engagement repose sur l'interpellation des cybercriminels, synonyme de leur mise hors d'état de nuire, afin d'empêcher l'apparition de nouvelles victimes. C'est tout le sens du travail d'enquête mené par le policier ou le gendarme, appuyé par l'agence. La coordination efficace de ces enquêtes complexes est facilitée au sein d'un groupe permanent, le J-CAT (Joint Cybercrime Action taskforce), rattaché à EC3, regroupant les représentants de 19 services européens et extra UE. En 2021, il a soutenu plus de 80 opérations d'envergure et des équipes communes d'enquête, et l'arrestation de nombreux cybercriminels. C'est aussi une structure, bâtie sur la confiance entre ses membres, qui permet un très actif d'échange d'informations opérationnelles.

L'analyse des contenus numériques (disques durs, smartphones, serveurs) saisis lors des perquisitions, est essentielle. L'unité forensique d'EC3 détient une expertise de haut niveau dans ce domaine et est régulièrement sollicitée par les services permettant l'identification des cybercriminels et de leurs victimes.

Le centre fournit également des services de recoupement des informations (cyber-intelligence) ou d'analyse des flux de crypto-monnaies.

L'entrave des capacités criminelles est une autre approche efficace, avec des opérations visant à perturber la diffusion de contenus illégaux et l'acquisition des capacités techniques nécessaires aux cybercriminels pour commettre leurs attaques (malwares, rançongiciels, proposés sur le darknet). En 2021, Europol a soutenu 9 services d'enquête pour le démantèlement de « Darkmarket », une plateforme majeure de vente de produits illicites sur le darknet. Europol a aussi participé au démantèlement de « Boystown », la plateforme du darkweb, servant à l'échange de contenus pédopornographiques.

Le troisième engagement en faveur des victimes, porte dans certaines situations sur une aide à la réparation du préjudice causé, dans la mesure du possible. Dans ce domaine, Europol appuie des initiatives innovantes, reconnues tant au niveau européen qu'international.

La plateforme « No *more Ransom* » (www.nomoreransom.org), développée par l'agence, en partenariat avec le secteur privé et plusieurs services d'enquêtes permet aux victimes de neutraliser un nombre important de rançongiciels et de récupérer leurs données sans avoir à payer de rançon. Elle propose à une victime d'attaque par rançongiciel, un accès libre aux solutions de déchiffrement existantes, ainsi que des conseils ou des liens de contacts vers les services compétents au plan national. La victime peut dès lors récupérer son contenu sans verser la rançon aux cybercriminels. Depuis 2016, ce dispositif propose plus de 121 outils de déchiffrements couvrant 151 familles de rançongiciels. Ses outils ont été téléchargés par les victimes, plus de 6 millions de fois, évitant un préjudice estimé à 900 millions de dollars. L'accès est disponible en 37 langues. 170 partenaires privés ont contribué à cette initiative emblématique qui réunit la lutte contre un modèle criminel et la protection des victimes.

Dans tous les autres cas, la restitution aux victimes, de fonds dérobés demeure un objectif prioritaire. Dans certaines affaires, elle est rendue possible par le travail des enquêteurs sur les flux de crypto-monnaies utilisés pour exfiltrer ou détourner les fonds. Europol/EC3 dispose d'experts reconnus au niveau international qui soutiennent les enquêtes et qui partagent leur savoir afin de créer partout en Europe des capacités supplémentaires dans ce domaine nouveau et absolument indispensables des enquêtes modernes. Ils contribuent en cela à la résolution de nombreuses enquêtes au profit des victimes.

La neutralisation à distance de dispositifs criminels (malwares) sur les ordinateurs des victimes est une opération complexe,

mais qui reste possible. Dans ce domaine, Europol a soutenu une opération majeure et exemplaire en janvier 2021, contre le botnet EMOTET. Elle a impliqué les services de 15 pays et a réuni à Europol plus de 30 enquêteurs, afin de neutraliser le malware ayant infecté un vaste réseau d'ordinateurs et servant à la propagation d'autres malwares et rançongiciels. Dans cette affaire, la législation de certains pays de l'UE, a permis de diffuser une mise à jour réparatrice qui a mis fin au contrôle opéré par les cybercriminels dont certains ont été arrêtés. Cette affaire, au même titre que celle conduite en 2019 par la gendarmerie française pour neutraliser le botnet RETADUP, met en lumière que les avancées technologiques ou juridiques d'un des partenaires d'une investigation appuyée par Europol peuvent parfois être mutualisées au bénéfice de tous, et contribuent à protéger les victimes.

Ces affaires peuvent d'ailleurs nourrir une réflexion juridique et opérationnelle sur une approche plus « offensive » de la lutte contre les cybecriminels, visant à mieux protéger les victimes en neutralisant les moyens d'attaque des criminels…même si le sujet reste très délicat au plan juridique et des principes.

Diminuer ou mieux ramener à zéro la vulnérabilité des victimes est un objectif premier dans la protection des mineurs victimes d'exploitation sexuelle sur internet. Cela consiste à procéder à leur mise en sécurité, mais aussi à effectuer le retrait des contenus en ligne. Europol a développé depuis des années des relations opérationnelles très fortes avec tous les services spécialisés dans le monde, et en particulier avec le NCMEC des États-Unis d'Amérique (National center for Missing Exploited Children). Depuis 2014, l'unité d'Europol contre la pédopornographie en ligne a relayé plus de 850 000 contenus vers ses partenaires, aux fins de traitement et de retrait. L'agence actuellement entend rendre cet effort encore plus efficace par la création d'un système automatisé (GRACE) qui optimisera l'analyse des contenus et l'information des partenaires afin d'identifier les auteurs et victimes.

Le quatrième engagement en faveur des victimes consiste tout simplement à limiter le risque d'en créer de nouvelles. C'est tout le sens du travail de prévention qui est relayé au niveau européen notamment par Europol. En effet, Europol mène ou contribue à des actions de communication, notamment au moyen du compte twitter @ EC3Europol, suivi par 30 000 contacts.

Concernant la protection des mineurs, cet effort concourt aussi à l'obtention des signalements. En 2021, EC3 a participé à 6 campagnes de prévention en partenariat avec des associations (#stopChildAbuse, Safer Internet Day, Trace an object, #InternationalChildrensDay,…).

Europol participe également à des actions visant à sensibiliser les consommateurs sur le risque d'escroquerie en ligne, dans des campagnes dédiées (#CyberScams, E-commerce, #BlackFriday, #CyberMonday..). L'autre effort de sensibilisation est porté sur les règles essentielles d'hygiène informatique et de cyber sécurité. Europol est notamment partenaire des campagnes annuelles de prévention déployées lors

du mois de la cybersécurité européenne (ECSM).

La protection des victimes est, en définitive, étroitement liée aux succès opérationnels qu'Europol soutient et appuie au service des États membres et des partenaires de l'union européenne. Ces succès sont le fruit d'une coopération active entre les services européen d'application de la loi soutenus par Europol, notamment sous l'égide de l'EU Cyber Task Force (EUCTF) qui regroupe les représentants de ces unités cyber menant ce travail d'enquête au quotidien. Ces succès reposent sur la synergie avec les autres partenaires européens (ENISA, CERT UE, Commission et Conseil, Eurojust, SEAE, AED,..) avec lesquels Europol construit le cadre nécessaire aux opérations.

Les menaces cyber-criminelles ayant une empreinte mondiale, globale, tout succès est aussi le fruit d'une coopération internationale avec des partenaires majeurs extra-européens au premier rang desquels les États-Unis.

Enfin ces succès sont aussi le résultat de partenariats quotidiens avec le secteur privé. Depuis 2014, EC3 développe cette coopération essentielle au sein de trois groupes dédiés, les « advisory groups » (secteur financier, opérateurs de télécommunication, entreprises de cybersécurité) dont 70 principaux partenaires fournissent un appui précieux aux opérations, à l'évaluation des menaces, au développement de l'expertise, dans un esprit de confiance mutuelle.

La recherche permanente de l'innovation contre l'utilisation des nouvelles technologies par les criminels est enfin une dimension clé de tout succès. Chaque enquête est un défi opérationnel, juridique, de coopération, mais aussi technologique.

Face à une technologie en constante évolution, dont les cybercriminels saisissent rapidement les opportunités nouvelles de développer leur prédation, le droit doit également évoluer. Les succès sont, ne seront possibles que grâce à des capacités juridiques puissantes, contrôlées dans la cadre de l'état de droit, que le législateur, notamment européen, a le devoir de faire évoluer. L'adaptation des capacités d'enquête numérique (preuve numérique, conservation des données, intelligence artificielle, chiffrement…) dans le contexte des nouvelles technologies conditionnera aussi les succès de demain.

La protection des victimes par la prévention, par la diminution des surfaces d'attaques, par la neutralisation des cybercriminels ou par la neutralisation proactive de leurs infrastructures techniques sont des préoccupations majeures d'Europol à travers son centre européen de lutte contre la cybercriminalité – EC3. Ils demeurent des enjeux majeurs qu'Europol aborde avec confiance grâce à sa force de coopération, à son sens de l'innovation et surtout à son expérience opérationnelle quotidienne acquise aux contacts des services d'enquête des États membres de l'Union européenne.

Le général Jean-Philippe LECOUFFE en bref :

Le général de corps d'armée Jean-Philippe Lecouffe est Directeur exécutif adjoint d'Europol. Il a servi pendant plus de 30 ans dans la gendarmerie, ou il a occupé diverses fonctions opérationnelles de commandement, notamment à la tête de la sous-direction de la police judiciaire.

LA PRÉVENTION, UN IMPÉRATIF POUR LUTTER EFFICACEMENT CONTRE LES CYBERMENACES

La prochaine crise sera cyber ! Cette sentence peut apparaître péremptoire mais l'actualité le confirme. Il suffit pour cela de se rendre sur un des multiples sites proposant une cartographie en temps réel des cyberattaques pour se rendre compte du phénomène à l'échelle mondiale. La crise sanitaire ou la crise ukrainienne ont, par ailleurs, révélé que toute crise d'ampleur peut avoir une composante cyber, soit comme opportunité soit comme partie intégrante d'une manœuvre globale.

> **Définition de la cybersécurité par l'ANSSI**
>
> État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

BARNABÉ WATIN-AUGOUARD

Colonel, dirige la division proximité numérique du commandement de la gendarmerie dans le cyberespace

On peut également avancer que la crise cyber est déjà en cours. En effet, pour telle collectivité territoriale, la crise cyber débute peut-être en ce moment-même par la découverte d'une cyberattaque. Pour telle entreprise, elle a commencé il y a plusieurs mois et le retour à la normale est difficile et coûteux, et la liquidation envisagée. Prévenir une crise cyber apparaît dès lors comme un enjeu majeur pour toute organisation.

Pleinement intégrée dans les missions structurantes du commandement de la gendarmerie dans le cyberespace, la prévention cyber est exercée au quotidien, dans les territoires, par le réseau des cybergendarmes. Si la prévention passe inévitablement par une sensibilisation adaptée des usagers, il est indispensable, en amont, de convaincre les décideurs que le risque cyber est un véritable enjeu et de les accompagner dans la montée en puissance de leurs organisations.

Convaincre les décideurs

Bon nombre de dirigeants considèrent encore qu'ils ne sont pas une cible potentielle des cybermenaces du fait de leur taille ou de leur secteur d'activité. Ces critères ne sont en rien des freins pour les cyberattaquants. Si de grandes métropoles ou de grands groupes sont visés, un nombre conséquent de petites communes ou de

© MININT

Le dialogue avec les entreprises est primordial en matière de cybersécurité

TPE/PME sont également victimes de cyberattaques. En outre, aucun secteur n'est épargné : transports, santé, logistique, nouvelles technologies, bâtiment, textile, agroalimentaire, mais également administrations ou associations. Avec la forte croissance des cyberattaques, il est malheureusement facile de s'attaquer à ces idées reçues en s'appuyant sur des exemples concrets et évocateurs par leur taille, leur activité, voire leur proximité géographique. Si ce dernier critère peut sembler n'avoir aucun sens dans un cyberespace sans frontière, c'est pourtant un ressort psychologique efficace.

Il faut s'appuyer également sur la définition de la cybersécurité. Souvent associée, à tort, à la seule technique, cette notion ne doit pas être considérée comme une fonction annexe, mais bien comme un état recherché, comme le propose l'ANSSI dans sa définition. Une cyberattaque résulte de la rencontre d'un attaquant avec des données ou services au travers de vulnérabilités. « Je suis en cybersécurité quand je prends les mesures nécessaires pour éviter au maximum une cyberattaque et le cas échéant, y remédier ». Ces mesures relèvent de la sécurité des systèmes d'information mais également de la lutte contre la cybercriminalité ou de la cyberdé-

fense qui sont intimement liées. L'objectif de la prévention cyber est alors d'amener un décideur à prendre en compte sa cybersécurité comme il le fait naturellement pour sa sécurité incendie par exemple.

Au-delà de cette prise de conscience, il demeure souvent difficile d'appréhender le risque cyber. La probabilité d'occurrence peut être perçu comme relativement faible

Or on estime qu'une attaque par rançongiciel est déclenchée toutes les 11 secondes dans le monde. En outre, les impacts d'une cyberattaque sont nombreux et souvent démultipliés : incapacité de produire ou d'assurer ses missions, désorganisation de la structure, confiance interne ou externe entamée, responsabilités civiles ou pénales engagées... L'impact financier est souvent le plus déterminant. Si investir en amont peut sembler inutilement coûteux face à une menace que l'on a du mal à appréhender, il n'est pas rare de voir des entreprises pour lesquelles la crise est fatale. À titre d'exemple, le préjudice global pour la ville d'Atlanta, victime d'une rançongiciel en 2018, est estimé à environ 7 fois le coût de la sécurisation de ses systèmes d'information. Plus proche de nous, un établissement de santé a évalué le coût direct de la cyberattaque dont il a été victime à près de 1 % de son chiffre d'affaire auquel pourraient s'ajouter 2 % de pertes financières. Une analyse des impacts potentiels d'une cyberattaque est souvent l'élément déclencheur d'une prise en compte du risque cyber encouru et de la nécessité d'entreprendre des actions correctrices.

Sensibiliser les utilisateurs

La lutte contre les cybermenaces est une affaire de responsabilité. Il ne s'agit pas ici d'une responsabilité à vocation punitive en cas de faute, qui mène à la honte et à la tentation de taire un incident. Il s'agit d'une responsabilité valorisant chacun comme contributeur de la défense globale. On présente souvent la cybersécurité comme étant l'affaire de tous.

Cela peut toutefois laisser penser qu'une faiblesse individuelle ne fait qu'affaiblir la sécurité d'un groupe. Or, chaque utilisateur est un maillon, plus ou moins fragile, d'une chaîne de sécurité. Si elle est brisée, elle perd toute son efficacité quelle que soit la résistance des autres éléments la composant. Il suffit parfois d'un clic sur un lien malveillant pour déstabiliser tout l'édifice. La cybersécurité est plus exactement l'affaire de chacun. En tant qu'individu, collaborateur ou citoyen, il peut par une action correctrice, un respect des règles d'hygiène numérique, un signalement d'un élément suspect ou un conseil avisé contribuer à la défense collective. C'est l'objet d'une politique de sensibilisation large et adaptée aux différents usagers

On observe une progressive transhumance dans le cyberespace de la cybercriminalité. Celle-ci représente d'ores et déjà 9 % de la délinquance constatée par la gendarmerie et connaît une augmentation annuelle de 20 à 25 %. Les cyberdélinquants utilisent les systèmes d'information et les réseaux comme cible ou comme vecteur pour leurs actions malveillantes. Si une intrusion dans un réseau ou une escroquerie en ligne semblent relever de deux registres

© DR

Les trois piliers de la cybersécurité

différents, elles s'appuient toutes deux, dans près de 8 cas sur 10, sur le facteur humain pour arriver à leur fin en exploitant les émotions des usagers : la honte, la pitié, l'envie, la peur... Sensibiliser les membres d'une organisation aux menaces et aux techniques utilisées par les cyberdélinquants pour arriver à leurs fins contribue ainsi efficacement à la protection globale.

Cette sensibilisation passe par la démystification des aspects techniques. Ces derniers peuvent rebuter les usagers, les conforter dans l'idée que ces sujets ne sont pas de leur ressort ou les induire en erreur comme, par exemple, la sacralisation du protocole HTTPS désormais largement utilisé par les cybercriminels. La vulgarisation des notions en s'appuyant sur le monde réel contribue également à la prise de conscience des dangers : on comprend mieux l'intérêt d'avoir plusieurs mots de passe quand on les compare aux clés qui nous permettent d'ouvrir un logement, un véhicule, un bureau ou un coffre-fort. On hésite à utiliser une clé USB trouvée sur un bureau si on la compare à une brosse à dents ! Il est par ailleurs prudent de séparer nettement ses usages professionnels et personnels, mais il est souhaitable

d'adopter une prudence similaire avec les outils numériques chez soi et au travail. La cybersecurité doit devenir une évidence pour tous, en tout temps et en tous lieux.

Accompagner les organisations

La prévention ne se limite pas à ces deux étapes. Elle doit s'inscrire dans une dynamique d'accompagnement visant à améliorer, dans le temps, la cybersécurité

des entités. Cette démarche a été initié par la gendarmerie pour les collectivités territoriales, en partenariat avec l'association des maires de France et cybermalveillance.gouv.fr, avec le dispositif I.M.M.U.N.I.T.E. Cyber. Celui-ci repose sur une première évaluation de la maturité cyber d'une collectivité. Il se poursuit avec un pré-diagnostique élémentaire permettant d'identifier les fragilités. Il ne s'agit pas de se substituer à des opérateurs privés mais d'aider une collectivité à connaître ses forces et faiblesses pour établir un plan d'action afin de renforcer sa protection et prévenir les risques. Ce dispositif en cours de déploiement sera, à court terme décliné pour les TPE/PME ou d'autres types d'organismes.

Outre les mesures permettant de réduire au maximum les vulnérabilités, il importe d'amener chacun à s'intéresser aux données. En flux ou en stock, elles sont souvent les principales cibles des cybercriminels. Sur leurs revenus, estimés à près 1 500 milliards de dollars à l'échelle mondiale, 45 % proviendraient de la revente de données (à caractère personnelles mais également relevant de la propriété intellectuelle ou du secret des affaires) tandis qu'ils ne dépasseraient pas les 0,1 % pour les rançongiciels. Ces derniers mettent à mal la disponibilité des données, mais cache, la plupart du temps, une atteinte à leur confidentialité avec une exfiltration avant la phase de chiffrement. S'ajoute une éventuelle modification de l'intégrité des données. Souvent oubliée dans les analyses de risques, elle demeure, dans bien des cas, l'élément premier du bon fonctionnement d'une organisation. La réduction de la surface d'attaque doit par conséquent intégrer une réflexion exigeante et parfois iconoclaste en la matière pouvant mener à la frugalité dans une ère où l'espace de stockage est quasi-illimité ou à la conservation hors réseau dans un monde désormais hyperconnecté.

Malgré toutes les mesures prises précédemment, le pire peut survenir. Il est par conséquent indispensable d'inviter les organisations à se préparer à la gestion d'une crise cyber. Cette anticipation est malheureusement souvent oubliée. Beaucoup disposent de nombreux plans de gestion de crise, de continuité ou de reprise d'activité pour la plupart des risques qu'elles encourent. Rares sont ceux qui ont élaboré des plans pour affronter une cyberattaque. Or, dans la crise qui s'installe, les outils courants comme la messagerie, l'annuaire, la téléphonie sont souvent indisponibles. En outre, la technicité nécessaire à la compréhension de ce qui se passe peut paralyser les décideurs et les amener à s'en remettre à leurs techniciens internes ou à des prestataires externes. Si l'appui de ces derniers est indispensable, il revient aux dirigeants de fixer les priorités pendant et après la crise. La sidération est inévitable mais l'impréparation peut mener au chaos. Prendre le temps d'y réfléchir en amont est salvateur : un plan imparfait vaut toujours mieux qu'une absence de plan !

Convaincre, sensibiliser et accompagner, telle pourrait être la devise de toute bonne prévention. L'objectif est de repousser au plus loin les cybermenaces en adoptant des mesures, certes techniques, mais également organisationnelles tout en se tenant prêt à affronter un choc qui peut, malgré

tout arriver. Alors, la prévention s'efface au profit de l'intervention pour laquelle la gendarmerie continue à accompagner la victime avec des enquêteurs spécialisés, des experts techniques, voire des négociateurs de crise… pour peu que la victime nous prévienne !

Le colonel Barnabé WATIN-AUGOUARD en bref :

Commandant de la division proximité numérique du commandement de la gendarmerie dans le cyberespace, le colonel Barnabé Watin-Augouard est issu de l'École navale, ingénieur spécialisé en détection électromagnétique. Il a rejoint la gendarmerie en 2004 après 7 années passés dans la marine.

Après plusieurs commandements, en mer ou à terre, notamment au sein de la gendarmerie maritime, et une affectation au secrétariat général de la mer, il a occupé les fonctions d'adjoint au chef de la session nationale de l'institut des hautes études de défense nationale.

Il était également responsable de la conduite de la session nationale souveraineté numérique et cybersécurité de l'IHEDN, avant de rejoindre le COMCYBERGEND à sa création à l'été 2021.

COMMENT ÉVITER AUX COLLECTIVITÉS TERRITORIALES D'ÊTRE DES PROIES NUMÉRIQUES ?

Les cyberattaques contre les collectivités territoriales françaises, ne sont pas des phénomènes nouveaux. Néanmoins au cours des années 2019/2020, ces dernières ont connu une nette accélération, relevée notamment par l'ANSSI[1].

Comment cette situation peut-elle s'expliquer ?

Plusieurs facteurs sont à prendre en considération. Tout d'abord, le sentiment pour les collectivités que ces dernières ne sont pas « intéressantes » par rapport à d'autres secteurs d'activité comme la recherche, le secteur bancaire... Pour beaucoup d'élus, ce sujet est éloigné des préoccupations quotidiennes ; il est technique et relève du service informatique. Malheureusement, trop souvent encore la prise de conscience se fait dans la douleur, lorsque la collectivité a perdu des informations cruciales ou qu'elle ne peut plus assurer ces missions de service public[2]. Pourquoi ces dernières investiraient-elles des sommes importantes contre une menace perçue comme marginale ? Pourtant l'ANSSI dans son rapport annuel sur l'évolution de la menace cyber en 2018[3], indiquait observer des changements. En effet, ces mêmes secteurs avait fait évoluer de façon significative les moyens alloués à la Cybersécurité rendant les attaques contre eux plus coûteuses. L'agence avertissait alors sur une évolution à venir dans la posture des cybercriminels pour le choix des cibles futures ; frapper des entités moins bien préparées.

CYRIL BRAS

Directeur Cybersécurité chez WHALLER et Vice-président de l'INCRT

Autre élément à prendre en compte, la diversité des collectivités territoriales françaises. Qu'il s'agisse de villes, de communautés de communes, de métropoles, de départements ou de régions ces entités ont en commun de disposer d'informations sensibles (état civil, données de santé, systèmes industriels...) qui peuvent être convoitées. Malheureusement, ces entités publiques ne sont pas toutes égales dans leur capacité à se protéger. En effet, une mairie de quelques centaines d'habitants ne dispose pas des mêmes ressources qu'une métropole. Commençons par la base, disposer d'un service informatique. Bien souvent pour les petites collectivités,

1 Cybersécurité : L'Anssi alerte sur une explosion des menaces », *usine-digitale.fr*. https://www.usine-digitale.fr/article/cybersecurite-l-anssi-alerte-sur-une-explosion-des-menaces.N1102619.

2 S. Barby et F. Gatel, « Les collectivités territoriales face au défi de la cybersécurité », Sénat, Paris, 283 (2021-2022), déc. 2021.

3 ANSSI, Éd., « Rapport annuel 2018 ». ANSSI, 2019.

le système d'information se limite à un simple ordinateur bureautique, celui de la secrétaire de mairie.

Ce même ordinateur est maintenu en service par un prestataire informatique pas toujours au fait des exigences en Cybersécurité. Pour celles, plus chanceuses, qui disposent d'un service informatique, aucune garantie que le sujet soit mieux adressé ; là encore par manque de compétence cyber au sein du service informatique. La fonction RSSI commence à apparaître dans les services informatiques de communauté d'agglomération (sans pour autant être la règle[4].) Cette fonction est bien souvent cumulée avec celle de RSI ou de DSI. Elle commence à être dédiée dans les grandes villes, les métropoles, les départements ou les régions mais reste malheureusement bien trop souvent dans le giron de la DSI. La parole du RSSI est loin d'être entendue ou audible par les instances dirigeantes ou les élus de par son positionnement dans l'organigramme. Son rôle reste bien trop souvent perçu comme seulement technique et non stratégique.

Enfin, le dernier point concerne les sous-traitants informatiques. Qu'il s'agisse de petites entreprises en charge de l'entretien du système d'information d'une petite collectivité ou du développement d'un logiciel spécifique, le niveau de protection mis en œuvre n'est pas toujours au rendez-vous[5]. Les collectivités au travers de leurs RSSI[6] ont du mal à imposer de la Cybersécurité à certains de leurs sous-traitants. Or, les attaques dîtes de « Supply Chain » sont de plus en plus répandues et augmentent là encore les possibilités d'intrusions sur les SI des collectivités.

Une cyberattaque, un problème purement technique, pas si sûr ?

Les impacts d'une cyberattaque pour une collectivité sont forts, dépassent le cadre du service informatique, et peuvent être de différentes natures. Avec la transformation numérique, la dépendance à l'informatique est une réalité pour assurer les missions de service public ; la survenue d'une attaque a donc en premier lieu un impact sur les missions[7]. Suivant le type de SI concerné, l'impact peut être humain ou environnemental[8] mais dans tous les cas aura un impact sur la gouvernance car l'attaque aura un coût technique et humain pour la remise en service[9]. Ces fonds n'auront pas forcément été planifiés et nécessiteront la temporisation de certains projets. Mais l'attaque en elle-même peut avoir des effets directs sur les finances de l'entité en entraînant des pertes financières[10].

4 *Études Menaces informatiques et pratiques de sécurité* - Collectivités territoriales - Édition 2020 (MIPS 2020).

5 S. Meurant et R. Cardon, *La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?* Sénat, 678 (2020-2021), juin 2021.

6 J. Cheminat, *Les RSSI des collectivités territoriales créent un réseau de partage* - Le Monde Informatique 16 février 2021.

7 A. Vitard, *L'agglomération du Grand Guéret victime d'un ransomware, des services publics à l'arrêt*, usine-digitale.fr, 2 décembre 2021

8 *Piratage informatique d'un service d'épuration des Pyrénées-Atlantiques* », 20minutes, 29 septembre 2021.

9 A. Léchenet, *Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône*, La Gazette des Communes, 29 juillet 2021.

10 Annecy. *Parkings : 80 000 euros de perte pour la Ville après la cyberattaque*. https://www.ledauphine.com/economie/2021/12/09.

© MININT

La gendarmerie est le partenaire cybersécurité des collectivités locales

Du point du vue juridique, même si jusqu'à présent cela n'a pas été le cas pour des collectivités[11], des amendes peuvent être appliquées mais aussi des poursuites engagées par les citoyens. Enfin, ne négligeons pas l'impact sur la confiance et l'image de la collectivité, comme l'a évoqué la ville de La Rochelle au cours d'une conférence[12].

11 L. Lainé, *Cyberattaque : Marriott écope d'une amende de 18,4 millions de livres*, L'Écho Touristique, 30 octobre 2020.

12 J. Dulac, Denis Vermot, Mathieu Souchard, E. Hazanne, P. Steuer, et C. Bras, « *TRIP printemps 2021 | Avicca | Cybersécurité : de la menace à l'action territoriale* », 11 mai 2021.

Comment les collectivités peuvent-elles lutter ?

Les collectivités (élus et directions générales) doivent cesser de percevoir la Cybersécurité comme un centre de coûts et un sujet uniquement technique mais doivent en faire un levier pour la transformation numérique. Elles doivent faire de la Cybersécurité un gage de la confiance pour les usages du numérique. Concrètement, elles doivent se mettre en ordre de bataille au travers de quatre axes principaux :

- **Changer leur perception de la cybersécurité**

Les collectivités doivent s'appuyer sur un référentiel d'exigences communes de Cybersécurité comme par exemple le cahier des clauses simplifiées de Cybersécurité publié au journal officiel en 2018[13]. Ces exigences doivent être éliminatoires, bien avant l'analyse fonctionnelle ou le tarif.

- **Acculturation aux enjeux liés à la Cybersécurité**

Les élus et directeurs généraux doivent s'approprier le sujet Cybersécurité. Pour cela il convient d'intégrer des modules de formation spécifiques pour ces profils particuliers. Il convient également d'intégrer la Cybersécurité dans les enseignements à destination des futurs cadres de la fonction publique territoriale.

- **La mutualisation de moyens humains**

Pour les entités qui, de par leur taille, ne peuvent disposer de la compétence SSI en interne, des chantiers de mutualisation doivent être mis en œuvre[14]. Cette mutualisation peut intégrer l'ensemble des acteurs d'un territoire au travers de partenariats public privé[15] tout en favorisant l'emploi local en formant des profils grâce à des formations spécifiques[16].

- **L'attractivité des carrières et des missions SSI**

Lorsque la fonction RSSI existe dans une collectivité, il convient de la rattacher au plus haut niveau stratégique pour la rendre efficace afin que ce dernier puisse apporter son expertise auprès des élus et de la direction générale. Ce rattachement permet aussi au RSSI de connaître les projets en cours et d'en déduire les éventuelles sources de menaces. Enfin, il est plus que nécessaire de revoir la rémunération associée si l'on souhaite attirer ou conserver les talents dans la fonction publique. Une étude du CESIN sur ce sujet montre un retard certain de la sphère publique[17].

Cyril BRAS en bref :

Cyril Bras a rejoint WHALLER en mars 2022 en qualité de directeur Cybersécurité, après 4 années passés à la métropole de Grenoble en tant que RSSI au cours desquelles il a initié la création du réseau des RSSI de collectivités. Il est auditeur IHDEN de la 2e session nationale Cybersécurité et Souveraineté Numérique et officier de réserve citoyenne de la Gendarmerie Nationale.

13 Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité.

14 E. Lambert, « *L'Institut National pour la Cybersécurité et la Résilience des Territoires (INCRT)* », 3 mai 2021. https://www.cyberblog.bzh/bretagne/linstitut-national-pour-la-cybersecurite-et-la-resilience-des-territoires-incrt/

15 C. Bras, « *Les partenariats public-privé en Cybersécurité* », Pour Une Cybersécurité Coop. Collect., no 268, p. 48 53, janv. 2021.

16 *Six Formations Informatiques Bac+2 à Bac+6 LIWI*, Groupe AEN. https://www.groupe-aen.info/liwi

17 *Le Cesin dévoile une enquête exclusive sur la rémunération des fonctions RSSI*. CESIN.

L'EXPLOITATION JUDICIAIRE DES TÉLÉPHONES REND DE PLUS EN PLUS SERVICE À LA VICTIME

Les téléphones mobiles, possédant des capacités de stockage de plus en plus importantes, constituent des éléments matériels qui peuvent, dans un premier temps, orienter les enquêtes judiciaires puis, dans un second temps, servir de preuves devant les juridictions pénales. « *La quasi-totalité des infractions commises dans l'espace physique trouve un écho dans l'espace numérique* », tels sont les mots écrits par le Directeur général de la gendarmerie nationale en 2021 sur son blog. Cela illustre parfaitement l'omniprésence et la nécessité de rechercher la preuve numérique dans un monde de plus en plus connecté.

Les éléments présents dans un téléphone mobile permettent de faire ressortir des informations capitales relatives à son propriétaire et donc aux auteurs de crimes ou de délits. La victime, elle, peut être concernée soit directement, soit indirectement, par l'extraction et l'analyse de ces éléments. Elle sera directement concernée lorsque l'analyse porte sur les données de son téléphone (recherche des causes de la mort, communications avec un mis en cause, etc.) et indirectement concernée lorsque l'analyse porte sur les données du téléphone de l'auteur (assassinat, vidéos pornographiques, etc.) dont les actions ont eu des répercussions sur la victime.

THIBAUT HECKMANN

Chef d'escadron, Gendarmerie Nationale, chargé de Projets au CREOGN, docteur en Mathématiques de l'ENS Paris-Ulm

MATHÉO GILBERT

Apprenti Chargé d'études au CREOGN, étudiant du master Intelligence Économique à l'Université Gustave Eiffel

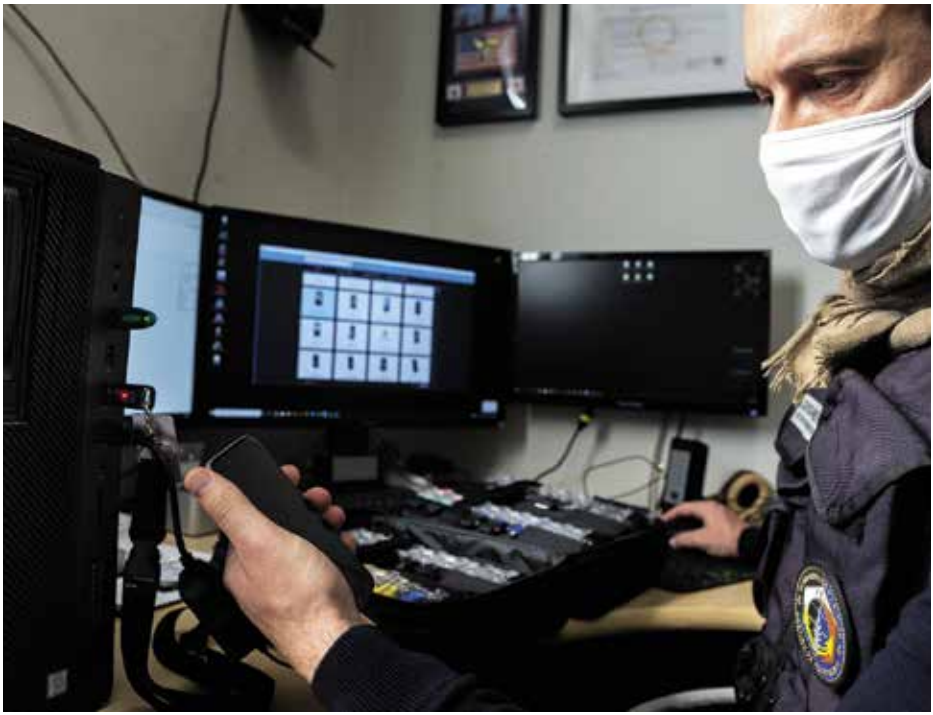
Concernant le téléphone portable, élément cible ici, nous constatons une évolution très rapide de sa sécurité avec, d'une part, la généralisation du chiffrement natif des terminaux et, d'autre part, le renforcement, par les constructeurs, de la sécurité logicielle (*software*) mais également matérielle (*hardware*). De ce fait, les forces de l'ordre ont dû s'adapter à ces évolutions technologiques tout en respectant les règles de droit applicables lors de leurs opérations techniques. Ces évolutions les menant vers une convergence indispensable des sciences « dures » et des sciences humaines et sociales, et passant indéniablement par l'acceptabilité sociale de la population envers les nouvelles techniques d'investigation intrusive.

Ainsi, l'investigation numérique (en anglais : *digital investigation ou digital forensic*), qui englobe la récupération (extraction et recherche des données effacées) et l'investigation (analyse avec ou sans interprétation)

des téléphones portables, est devenue une science de plus en plus déterminante servant directement la cause des victimes dans la manifestation de la vérité et incitant les criminels à les détruire. L'actualité récente de l'affaire Maëlys illustre parfaitement ce dernier point. Après sa première garde à vue, l'auteur du meurtre de la fillette a volontairement détruit son téléphone portable avant de le jeter dans un lac. Ainsi, l'enjeu du huitième jour du procès était de déterminer les informations contenues dans ce téléphone ; y avait-il des éléments permettant d'expliquer le déroulement des faits (indispensable au deuil de la famille de la victime), des éléments de géolocalisation datés ou des enregistrements vidéo (prouvant le penchant pédophile ou permettant d'identifier d'autres victimes potentielles) ? Nous sommes ici dans une analyse indirecte pour la victime, qui porte sur l'analyse du téléphone de l'auteur.

Aussi constatons-nous que cette évolution des capacités d'investigations numériques des forces de l'ordre entraîne une grande méfiance des auteurs de crimes dans les données contenues dans les téléphones et leurs périphériques (carte SIM, carte micro-SD). Ainsi, les destructions volontaires des téléphones (destruction des preuves) deviennent de plus en plus courantes et les enquêteurs doivent développer de nouvelles techniques de diagnostic et de réparation. Il en est de même suite à des explosions (attentats), des incendies, des accidents ou des crashs aériens. Par exemple, lors des investigations en 2015 après le crash de l'avion de la Germanwings, un gros travail technique avait été mené pour extraire les données des téléphones portables des victimes et des pilotes. Les objectifs étaient multiples : premièrement, il s'agissait de pouvoir retrouver dans les téléphones des victimes des vidéos tournées dans les derniers moments avant le crash (orientation de l'enquête) mais également des données pour une restitution aux proches des victimes (deuil des familles). Il s'agit, ici, d'un exemple d'une analyse directe du téléphone de la victime permettant d'apporter des éléments sur les causes de la mort. Les cas des destructions volontaires sont également très présents dans le cadre des affaires de violences intrafamiliales (VIF). Il est de plus en plus courant de voir l'auteur de tels actes venir détruire volontairement le téléphone de la victime, qui peut contenir des données accablantes (échanges de messages, menaces audios, vidéos, etc.). Aussi, lors des interpellations, il est fréquent de voir les auteurs tenter de détruire les preuves numériques, ce qui nécessite de mettre en place de nouveaux protocoles de préservation de la preuve numérique qui servira les victimes.

L'exploitation d'un téléphone peut parfois également servir à éviter le passage à l'acte (assassinats, attentats) et donc à préserver la vie humaine de victimes potentielles. Le droit français permet aux forces de l'ordre, dans le cadre des crimes et délits les plus graves (*article 703-73 CPP, crime en bande organisée, terrorisme, tortures et traite d'êtres humains*), de mettre en place des techniques spéciales d'enquête (investigations numériques intrusives) directement sur les téléphones. Ainsi, l'article 706-102-1 du Code de procédure pénale (CPP)



© MININT

Les données téléphoniques sont un élément important de l'enquête judiciaire

prévoit le recours « *à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur [...]* ». La conférence de presse d'Eurojust du 2 juillet 2020 sur le démantèlement du réseau EncroChat confirme la nécessité de telles techniques : « *L'enquête permettait de réunir des éléments sur le fonctionnement technique de la solution, et aboutissait à la mise en place d'un dispositif technique grâce auquel des communications non chiffrées des utilisateurs pouvaient être obtenues [et] a permis d'intercepter, de partager et d'analyser des millions de messages échangés entre les criminels dans le but de planifier des infractions graves [...] ces messages ont été lus par les forces de l'ordre en temps réel, à l'insu des expéditeurs* ». Nous sommes, ici, dans le cadre de la préservation de la vie humaine obtenue grâce à une analyse indirecte portant sur les téléphones des criminels. Cette préservation de la vie pour être également permis par une analyse

directe du téléphone de la victime, par exemple, en cas de localisation en temps réel du téléphone (disparition inquiétante, malaise, personne égarée).

Les premières versions de l'iPhone d'Apple (à partir de 2009/2010) intègrent très vite des options de chiffrement avancées (https://www.intego.com/mac-security-blog/the-evolution-of-ios-security-and-privacy-features/), tandis que les téléphones RIM Blackberry contenaient également, dès leurs premiers modèles au début des années 2000, des fonctionnalités de chiffrement avancées particulièrement prisées de certaines typologies de délinquants. Ces technologies sont utilisées, au détriment des victimes, par les criminels qui y voient un moyen d'agir en toute impunité. Les opérations menées, qu'elles soient logicielles (*software*) ou matérielles (*hardware*), visent à aller récupérer la clé de chiffrement puis à l'utiliser afin de rendre les données exploitables. Il existe aujourd'hui de nombreuses solutions « sur étagère » qui permettent l'exploitation d'un téléphone et l'extraction des données. La société Deveryware a été retenue par la Gendarmerie pour l'appel d'offre national quant à l'analyse des données de téléphonie. La solution logicielle (*DeveryAnalytics Telephony Data*) permet d'alléger les travaux des enquêteurs et d'augmenter les capacités d'investigation. D'autres sociétés spécialisées, comme XRY ou Cellebrite par exemple, proposent des solutions d'extraction de données spécialement réservées aux forces de l'ordre pour faire face aux nombreux nouveaux modèles. De plus, les forces de l'ordre peuvent également développer leurs propres techniques, en s'appuyant sur leurs experts internes. Ces dispositifs techniques sont très complexes à mettre en œuvre et nécessitent des opérations de rétro-conception longues et coûteuses. Elles sont prévues dans le cadre de l'article 230-1 du CPP : « *Lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, ou que ces données sont protégées par un mécanisme d'authentification, [l'autorité judiciaire] saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir l'accès à ces informations, [...], si cela apparaît nécessaire* ». Plus globalement, ces technologies visent à pouvoir traiter une masse plus importante de modèles dans un spectre toujours plus grand de données, toujours au service des victimes. Ainsi, l'accès aux informations détenues sur le téléphone mobile d'un suspect permet, en outre, d'accéder aux informations de paiement (historique des transactions, destinataires de virement, lieux de paiement, cryptomonnaies), aux éléments de traçabilité dans le temps via l'exploitation des informations dans les applications de messagerie instantanée, les capteurs biométriques, les accéléromètres ou les SMS. Ces données sont bien souvent liées aux victimes et permettent de confronter les déclarations des victimes et celles des auteurs de crime ou de délit. L'accès aux galeries d'images et aux fichiers peut aussi s'avérer très utile puisqu'il permet d'étudier la vie de l'individu et de retracer ses faits

et gestes passés ainsi que ses centres d'intérêts. Les métadonnées constituent ainsi des éléments déterminants qui permettent souvent de faire progresser une enquête. Enfin, ces techniques peuvent être réalisées directement sur le téléphone de la victime, par exemple lorsqu'une personne décédée utilisait un téléphone chiffré dont le mot de passe n'est pas connu de ses proches. L'accès aux données du téléphone concernant les réseaux sociaux peut, enfin, être révélateur notamment lors des échanges effectués sur le téléphone de la victime.

Ainsi, les méthodes et les compétences développées autour de l'avènement des nouvelles technologies, en particulier celles relatives au téléphone portable, permettent de faciliter le travail des enquêteurs et de venir appuyer le dossier d'accusation en fournissant des preuves tangibles et matérielles aux magistrats, au profit des victimes.

Le chef d'escadron Thibaut HECKMANN en bref :

Le chef d'escadron Thibaut HECKMANN est docteur en mathématiques de l'École normale supérieure de Paris et chercheur associé à l'ENS depuis 2018. Ancien chercheur associé à l'université de Londres et à l'université de Cambridge, en 2017 et 2018, il a rejoint le CREOGN en août 2020. Il a été de 2015 à 2020 expert à l'IRCGN et a notamment dirigé l'Unité d'expertise extraction des données (UEED). Il a obtenu en 2018 le prix Européen Emerging Forencic Scientist Award 2018-2021 de l'Académie européenne de police technique et scientifique (ENFSI) et le Trophée de cybersécurité du Cercle K2 en 2020. Il est membre du comité d'organisation de nombreuses conférences internationales et projets européens. Il est inscrit sur la liste des Experts Européens Externes près l'Agence Européenne de Cybersécurité et est membre fondateur du Cercle K2.

Mathéo GILBERT en bref :

Apprenti au CREOGN depuis septembre 2021, Mathéo Gilbert étudie les sujets du renseignement, de la cybersécurité, de la blockchain et de l'ingérence économique. Il est étudiant en première année du master Intelligence Économique à l'Université Gustave Eiffel, après un parcours juridique et commercial. Il est aussi rédacteur pour le site *intelligence-economique.co*.

RECHERCHE DE LA VÉRITÉ : L'ENJEU DU TRAITEMENT DES DONNÉES DE MASSE

De 1,2 zettaoctet (1 zettaoctet étant égal à 1 000 milliards de gigaoctet) de données générées dans le monde entier en 2010, nous sommes passés à 47 zettaoctets en 2020 et les prévisions avancent un chiffre de 2 140 zettaoctets pour 2035. Cette explosion quantitative des données numériques nous oblige à adopter une nouvelle approche pour analyser le monde et ses mécanismes. Le volume colossal de données numériques disponibles, implique de mettre en œuvre de nouveaux ordres de grandeur concernant la capture, le stockage, la recherche, le partage, l'analyse et la visualisation des données. L'augmentation exponentielle des données produites permet, à l'aide d'outils technologiques spécifiques, des recoupements et des analyses prédictives dans de nombreux domaines : scientifique, santé, économique, judiciaire, commercial…

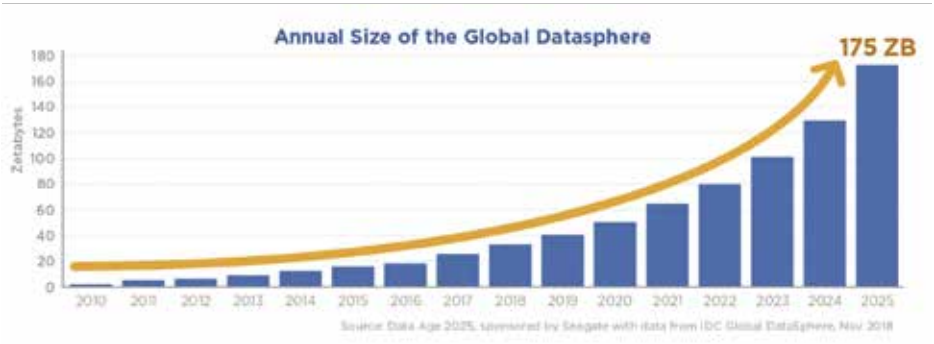
À l'instar des acteurs les plus importants de ces secteurs qui ont su appréhender la multiplicité des applications permises par cette révolution de la donnée et investir humainement, financièrement et technologiquement dans ce domaine afin de gagner en compétitivité, la gendarmerie a rapidement pris la mesure de l'importance de cet enjeu et a su mener la politique nécessaire, via notamment la création d'unités dédiées et l'allocation de moyens humains et techniques pour utiliser les avantages du traitement de données à des fins judiciaires dans le but de poursuivre l'amélioration du service rendu à la population tout en respectant les différents cadres juridiques en vigueur et les libertés fondamentales.

GUILLAUME CAZOTTES

Capitaine, chef adjoint du CSDSCRC de la Gendarmerie nationale

La gendarmerie nationale a très tôt perçu l'importance de l'enjeu du traitement de données de masse. Dans la continuité de la conceptualisation développée au début des années 2000 de l'approche sérielle de la criminalité, la gendarmerie nationale a soutenu la mise en place des cadres juridiques qui régissent actuellement le traitement de l'information d'intérêt judiciaire[1]. Le décret n° 2013-1 054 concernant les bases d'analyse sérielle se révèle aujourd'hui essentiel dans la mesure où il autorise la mise en œuvre de bases de données, accessibles aux forces de l'ordre, ayant pour finalité de « rassembler les preuves et d'identifier les auteurs des crimes ou délits présentant un caractère sériel, grâce à l'établissement de liens entre les individus, les événements ou les infractions » ou de rechercher les causes de la mort ou de la disparition d'une personne.

1 Logiciels de rapprochements judiciaires (art. 230-20 à 230-27 du CPP) et fichiers d'analyse sérielle (art. 230-12 à 230-18 et R40-35 à R40-37 du CPP, et décret n°2013-1054 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire » du 22 novembre 2013.



© DR

La gendarmerie a donc créé plusieurs bases d'analyse sérielle portant sur des thématiques spécifiques et chacune faisant l'objet d'une déclaration de conformité à la CNIL à l'appui d'une analyse d'impact portant sur la protection des données. Ces déclarations précisent notamment les données collectées dans les bases sérielles, les durées de conservation associées ainsi que la liste des accédants.

En 2015 la gendarmerie modernise son dispositif de traitement du renseignement d'intérêt judiciaire en créant le Service Central de Renseignement Criminel (SCRC), héritier du Service Technique de Recherches Judiciaires et de Documentation (STRJD) fondé en 1976. Le SCRC assure non seulement une mission de contrôle de conformité des fichiers co-administrés avec la police nationale mais également des bases d'analyse sérielle créées au bénéfice des unités opérationnelles.

Dès sa création, le SCRC s'est doté d'un centre des sciences de la donnée (CSD) ayant pour mission de développer des solutions technologiques afin d'offrir aux unités opérationnelles de la gendarmerie nationale ou de la police nationale la possibilité de traiter des masses importantes de données à des fins judiciaires. Il développe ainsi, entièrement en interne et sans appel à des prestataires, des logiciels afin d'exploiter les bases de connaissance de la gendarmerie nationale. Pour réaliser ces missions, la gendarmerie s'est enrichie de personnels qualifiés dans ce domaine : des ingénieurs, des développeurs et des experts en intelligence artificielle, des analystes et des data scientist afin d'exploiter de la manière la plus efficiente possible l'ensemble des données collectées par la gendarmerie.

L'ensemble de ces développements techniques, dont certains sont développés dans le cadre de projets européens, permet aux analystes de tester et d'expérimenter des technologies issues de la théorie des graphes ou bien de l'intelligence artificielle dans une logique d'aide à la décision leur permettant d'effectuer des rapprochements judiciaires pertinents.

Deux bases d'analyse sérielle illustrent particulièrement cette approche.

– La base concernant des personnes disparues et les cadavres non identifiés (CADDIS) permet de réaliser des rapprochements automatiques à l'aide d'algorithmes développés par le CSD. Concrètement, le logiciel va comparer les éléments d'enquête et les caractéristiques physiques des individus faisant l'objet d'une enquête pour disparition inquiétante avec les mêmes informations concernant les individus dont les cadavres ont été retrouvés mais non identifiés. Lorsque le logiciel effectue un rapprochement entre une disparition et une découverte de cadavre, l'enquêteur approfondit le rapprochement pour le confirmer ou l'infirmer. Le programme informatique n'est qu'une aide à la décision et ne fait que proposer d'éventuels rapprochements à l'utilisateur.

– La base concernant la délinquance itinérante (BSDI) rassemble les informations judiciaires portant sur des dossiers de criminalité organisée en rapport avec la délinquance itinérante. Elle est exploitée par les analystes et enquêteurs de l'OCLDI qui bénéficient des outils de visualisation proposés par le logiciel afin d'optimiser l'exploitation des données et dynamiser les investigations en cours.

Outre le traitement des données des bases d'analyse sérielle, le CSD a conçu des outils permettant de traiter et de visualiser les données issues de procédures judiciaires particulièrement complexes. En effet, l'augmentation exponentielle de la quantité de données produites rend l'exploitation humaine de ces données particulièrement chronophage. Particulièrement opportun pour assurer une reprise d'enquête complexe, il s'agit de faire gagner du temps aux enquêteurs dans la détection des « centralités d'un dossier » afin que ceux-ci puissent se consacrer exclusivement au travail d'élaboration d'hypothèses d'enquête et à la relance d'investigations plutôt qu'à la recherche fastidieuse de l'information au sein d'une masse de données hétérogènes. C'est dans le cadre des logiciels de rapprochement judiciaires que ces outils sont de plus en plus régulièrement utilisés.

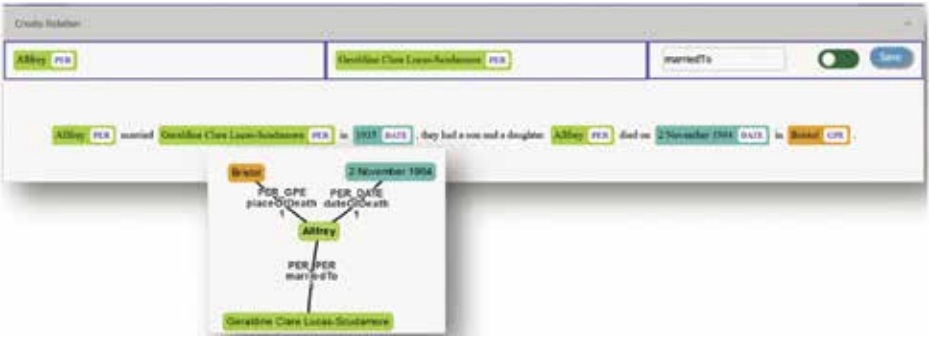
Par ailleurs, s'appuyant sur le décret n° 2015-1700 du 18 décembre 2015 modifié par le décret n° 2019-1602 du 31 décembre 2019, et à partir d'une vaste opération de captation de données informatiques visant principalement des groupes criminels organisés impliqués dans le trafic de produits stupéfiants, le CSD a développé un outil dédié au traitement d'une masse considérable de données brutes (plus de 120 millions de messages) pour les rendre exploitables par les enquêteurs qui, via une interface ergonomique et intuitive, ont pu accéder à l'intégralité des données interceptées. L'outil développé permettant de visualiser la donnée de manière différente (graphes relationnels, cartographies…) le travail des enquêteurs s'en est trouvé dynamisé et facilité notamment s'agissant de la matérialisation des infractions et de la mise en relation des protagonistes du dossier.

Dans le cadre de ce dossier d'envergure mondiale, cet outil, développé entièrement par le CSD, a été choisi spécifiquement par Europol pour le traitement des données captées et stockées. Il est encore aujourd'hui utilisé par de nombreuses forces de police à travers le monde dans le but d'exploiter l'immense quantité de données issue de cette opération.

L'augmentation de la quantité de données produites est exponentielle. Néanmoins, si l'on rentre dans les détails de cette augmentation et du type de données produites, on s'aperçoit qu'une partie importante de cette donnée est non structurée ou hétérogène à l'instar d'un texte libre ou d'une procédure judiciaire. Les enquêteurs et analystes traitent aujourd'hui de grandes quantités de données non structurées sous cette forme. Dans le but de structurer cette donnée et donc de la rendre utilisable par des outils de traitement de la donnée, la gendarmerie nationale a développé des techniques de traitement naturel du langage (NLP) dans le but de permettre aux machines de lire, déchiffrer et comprendre un langage humain grâce à l'intelligence artificielle.

Les développements du CSD permettent aujourd'hui l'annotation semi-automatique d'entités ainsi que l'extraction de relations sémantiques. Concrètement, il repère les entités d'intérêt (les dates, les personnes, les lieux, ainsi que tout autre type d'entité, qui peut être créé pour répondre à un besoin particulier) dans un texte et soumet son résultat à la validation de l'utilisateur qui effectue les corrections nécessaires, le programme tirant profit de ces corrections. Outre le fait qu'il repère une personne, un lieu et une date dans le texte, le logiciel va extraire aussi les relations entre ces entités : il va créer un graphe précisant que cette personne, ce lieu et cette date sont liés par une relation, par exemple que le lien entre trois entités X pour une personne, Y pour un lieu et Z pour une date sont que cette personne X est née à Y à la date Z.

Cette technologie d'intelligence artificielle permet d'extraire et d'analyser l'information de sources textuelles et constitue ainsi une économie certaine de temps pour l'enquê-



© DR

teur, la réalisation de cette mission manuellement étant particulièrement fastidieuse. Ce traitement de la donnée appliqué à des données hétérogènes permet de la structurer et donc de faciliter son exploitation ultérieure via des outils d'analyse (frise chronologique, schéma relationnel, cartographie…). L'exploitation des informations obtenues ainsi que la compréhension d'une procédure s'en trouve grandement facilitée ce qui permet, notamment lorsque les procédures sont particulièrement longues ou complexes, de dynamiser le travail d'investigation.

La Gendarmerie Nationale a su prendre en compte l'augmentation conséquente de la quantité de données produites ces dernières années, notamment en créant des unités dédiées au traitement de la donnée et en développant une doctrine d'emploi conforme aux cadres juridiques existants. Cet investissement s'est traduit par de nombreuses réussites opérationnelles dans des domaines variés. Les prévisions concernant l'évolution de la quantité de données produites, les différents formats que peut prendre cette donnée ainsi que l'explosion du nombre d'objets connectés dans notre quotidien, producteurs massifs de donnée, sont autant de paramètres que la gendarmerie prend aujourd'hui en considération dans ses travaux prospectifs. Les moyens déployés par la gendarmerie nationale pour le traitement de données à des fins judiciaires se sont révélés efficaces et l'expérience technique mais aussi judiciaire acquise par le traitement d'enquêtes judiciaires d'importance montre que la gendarmerie nationale possède les capacités d'appréhender les évolutions à venir dans le domaine du traitement de données de masse.

Le capitaine Guillaume CAZOTTES en bref :

Polytechnicien (promotion 2015), Guillaume Cazottes a d'abord dirigé la communauté de brigades de Castillon-la-Bataille en Gironde (33). Il est actuellement affecté au centre des sciences de la donnée en qualité d'adjoint depuis le 1er aout 2021.

L'ENJEU DE LA CONSERVATION DES DONNÉES DE CONNEXION

Les données de connexion, parfois appelées, métadonnées sont un ensemble de données techniques qui doivent être différenciées des données dites « de contenu ». Ces données techniques permettent de renseigner sur l'utilisation d'un support numérique connecté à un réseau de téléphonie mobile ou à un fournisseur d'accès à Internet. À l'inverse, les données de contenu comprennent comme leur nom l'indique la teneur ou le contenu des conversations, des données échangées. Par analogie avec un courrier postal, les données de connexion concernent l'enveloppe, les données de contenu concernent ce qui est dans l'enveloppe.

« *À l'ère numérique, la protection de la vie privée et des données à caractère personnel est une des garanties essentielles de nos libertés. Mais celle-ci doit être si absolue, ou ses limites doivent-elles être si contraintes, qu'elle primerait de fait sur la capacité des autorités publiques à protéger le droit à la sûreté et donc l'exercice de toutes les libertés ?*[1] ».

MATTHIEU AUDIBERT

Chef d'escadron, dirige le département partenariats et coopération au sein de la division Stratégie, Prospective et Partenariats au sein du commandement de la gendarmerie dans le cyberespace

Il est possible de distinguer trois catégories de données de connexion[2] :

– Les données d'identification : elles permettent de savoir a priori qui est titulaire d'un numéro de téléphone, d'un numéro de carte SIM, d'une adresse e-mail, d'une adresse IP ;

– Les données de trafic : elles renseignent sur l'utilisation du support numérique connecté. Il s'agit des factures détaillées, de la liste des contacts appelés, de la durée des appels, des appareils utilisés, de l'historique de l'envoi et de la réception des emails, la liste des adresses IP consultées à partir d'une adresse ;

– Les données de localisation : ce sont les zones d'émission et de réception d'une communication, la liste des appels ayant transité par une antenne relais, la localisation des téléphones portables en veille grâce aux déclenchements des relais téléphoniques.

Ces données sont donc par nature extrêmement sensibles puisqu'elles peuvent renseigner sur les habitudes d'un utilisateur, elles permettent de reconstituer un parcours ou encore de déterminer ses interlocuteurs. C'est la raison pour laquelle les opérateurs de communications

1 F. Molins, *La protection des citoyens européens dans un monde ultra-connecté*, Fondation Robert SCHUMAN, Question d'Europe, n°510, 8 avril 2019.

2 Articles R. 10-12 à R. 10-14 du code des postes et des communications électroniques.

électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonymes ces données relatives aux communications électroniques.[3]

Toutefois, à l'ère du tout numérique et à une époque où plus de 99 % de la population âgée de 15 ans ou plus est équipée d'un téléphone, fixe ou mobile[4], ces mêmes données représentent un ensemble d'informations extrêmement précieuses pour la recherche d'auteurs d'infractions et apporter des réponses à la détresse des victimes. À cet égard, la loi prévoit notamment une exception à la suppression des données de connexion.

Ainsi, les opérateurs de communications électroniques sont tenus de conserver pour les besoins des procédures pénales les informations relatives à l'identité civile de l'utilisateur[5], les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement[6]. Pour les besoins de la lutte contre la criminalité et la délinquance grave, ils conservent les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés[7].

3 Article L. 34-1 II du code des postes et des communications électroniques.

4 INSEE Focus, n°259, 24 janvier 2022.

5 Article L. 34-1 II bis 1° du code des postes et des communications électroniques.

6 Article L. 34-1 II bis 2° du code des postes et des communications électroniques.

7 Article L. 34-1 II bis 3° du code des postes et des communications électroniques.

En outre, pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constaté une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic[8] en complément de celles déjà conservées[9].

Ce cadre juridique complexe témoigne de l'extrême sensibilité que revêt la conservation des données de connexion. En effet il s'agit de concilier d'une part le droit au respect de la vie privée, principe à valeur constitutionnelle[10], et d'autre part la recherche des auteurs d'infraction, objectif de valeur constitutionnelle[11].

Or les décisions récentes de la Cour de Justice de l'Union européenne (CJUE)[12] ont entraîné de profondes inquiétudes chez les enquêteurs[13] et chez certains auteurs[14].

Dès lors, de la conservation à l'accès aux données de connexion, quel pourrait-être

8 Il s'agit de celles listées à l'article R. 10-13 V du Code des postes et des communications électroniques.

9 Article L. 34-1 III du code des postes et des communications électroniques.

10 Cons. const. 18 janvier 1995, n°94-352 DC ; Cons. const. 23 juillet 1999, n°99-416 DC.

11 Cons. const. 16 juillet 1996, n°96-377 DC.

12 CJUE, grande ch., Digital Rights Ireland, 8 avril 2014, C-293/12 et C-594/12 ; CJUE, grande ch., Tele2 Sverige et a., 21 décembre 2016, C-203/15 et C-698/15 ; CJUE, grande ch. La Quadrature du Net et a., 6 octobre 2020, C-511/18, C-512/18 et C-520/18.

13 M. Audibert, *La conservation des données de connexion, le droit français et la Cour de justice de l'Union européenne. Quelles conséquences pour les enquêtes judiciaires ?*, Veille juridique du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale, n°91, novembre 2020, pp. 13-29.

14 B. Nicaud, *CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données*, AJ Pénal 2020, p. 531.

ce nouvel équilibre, respectueux des droits et libertés et permettant d'identifier, de rechercher et de poursuivre les auteurs d'infractions ?

Considérant les réalités opérationnelles et l'état des cybermenaces, il apparaît nécessaire de maintenir une conservation généralisée et indifférenciée des données de connexion (I) tout en renforçant les modalités relatives à leur accès (II).

La nécessité d'une conservation généralisée et indifférenciée des données de connexion aux fins de lutter contre la délinquance

Dans ses arrêts, la CJUE a posé clairement l'interdiction pour les États membres de prévoir des mesures législatives prévoyant à titre préventif une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales[15].

En revanche, la CJUE a admis la possibilité de prévoir une telle conservation dans des situations où un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible[16].

De même, dans son arrêt Quadrature du Net, la CJUE admet l'hypothèse de la conservation ciblée, en amont, des données en fonction de zones géographiques prédéfinies pour des infractions relevant de la « criminalité grave ».

Elle envisage également d'hypothèse d'une conservation rapide des données permise par le droit européen[17].

Toutefois, comme l'a relevé le Conseil d'État, la solution suggérée par la CJUE de mettre en œuvre cette conservation ciblée des données de connexion n'est ni matériellement possible, ni opérationnellement efficace[18]. En effet, il n'est tout simplement pas possible de prédéterminer les personnes qui seront impliquées ultérieurement dans une infraction pénale qui n'a pas encore été commise. Le raisonnement est identique s'agissant du lieu de commission de cette infraction[19].

Saisissant cette infaisabilité opérationnelle, le Conseil d'État suggère de recourir à la conservation rapide autorisée par le droit européen en s'appuyant sur le stock de données conservées de façon généralisée et indifférenciée pour les besoins de la sécurité nationale. Ce stock peut ainsi être utilisé pour la poursuite des infractions pénales[20]. Autrement dit, le critère lié à la sécurité nationale devient le support juridique autorisant l'accès judiciaire à ces données sous deux réserves : la lutte contre la criminalité grave et une autorisation préalable délivrée par une autorité administrative indépendante ou un juge

15 CJUE, grande ch., Digital Rights Ireland, 8 avril 2014, C-293/12 et C-594/12 ; CJUE, grande ch., Tele2 Sverige et a., 21 décembre 2016, C-203/15 et C-698/15 ; CJUE, grande ch. La Quadrature du Net et a., 6 octobre 2020, C-511/18, C-512/18 et C-520/18.

16 CJUE, grande ch. La Quadrature du Net et a., c-511/18, c-512/18 et C-520/18, §139,168.

17 Articles 16 et 17 de la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001.

18 CE, Ass., French Data Network, 21 avril 2021, point 54.

19 M. Audibert, Conservation des métadonnées : le Conseil d'État préserve la majorité des enquêtes judiciaires, Lexbase Pénal, n°38, 20 mai 2021, pp. 85-87.

20 CE, Ass., French Data Network, 21 avril 2021, point 57.

indépendant ayant la qualité d'un tiers par rapport aux enquêteurs.

Ce dialogue complexe, sinon « rugueux »[21], des juges[22] et la position d'équilibre du Conseil d'État traduisent l'immense enjeu que représente la conservation généralisée et indifférenciée des données de connexion. Récemment, le Conseil constitutionnel a été amené à se prononcer sur la constitutionnalité de l'ancien régime juridique de conservation des données[23]. Dans une décision du 25 février 2022[24], le Conseil constitutionnel a déclaré contraire à la Constitution cet ancien régime juridique dans la mesure où la conservation générale et indifférenciée des données de connexion porte une atteinte disproportionnée au droit au respect de la vie privée[25].

Constatant d'une part que ces dispositions ne sont plus en vigueur et d'autre part que la remise en cause des mesures ayant été prises sur le fondement de ces dispositions déclarées contraires à la Constitution méconnaîtrait les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions et aurait dès lors des conséquences manifestement excessives, le Conseil énonce que ces mesures ne peuvent être contestées sur le fondement de cette inconstitutionnalité[26]. Si des interrogations subsistent concernant le régime actuel de conservation des données et les procédures en cours[27], il n'en demeure pas moins que le Conseil constate que cette conservation des données de connexion revêt un intérêt majeur.

En effet, d'un point de vue opérationnel, cette question est centrale. Les données de connexion sont massivement utilisées dans le cadre des enquêtes ou des informations judiciaires[28]. En pratique, il s'agit des réquisitions visant à obtenir des informations permettant l'identification d'un utilisateur, des données relatives aux équipements terminaux de communications utilisées, les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication[29], etc.

En 2020, plus de 85 % des enquêtes s'appuyaient sur ces données de connexion[30]. En volume, cela représente environ 2,5 millions de réquisitions judiciaires adressées aux opérateurs de communications électroniques[31]. Ces données permettent d'identifier l'auteur d'un cyberharcèlement, d'un revenge porn, de reconstituer le parcours d'un individu suspecté de meurtre, de croiser ses données téléphoniques avec celles

21 N. Hervieu, *Dialogue « rugueux »*, Gazette du Palais, n°34, 5 octobre 2021, p. 3.

22 M. Lassale, *Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE*, Recueil Dalloz, 2021, p. 406.

23 Article L. 34-1 du Code des postes et des communications électroniques en vigueur jusqu'au 31 juillet 2021 et issu de la loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

24 Conseil const. 25 février 2022, n°2021-976/977 QPC.

25 Ibid. cons. 13.

26 Ibid. cons. 16 et 17.

27 Au titre du principe de primauté du droit de l'Union sur le droit national.

28 Articles 60-1,60-2, 77-1-1, 77-1-2, 99-3 et 99-4 du Code de procédure pénale.

29 Article A. 43-9 du Code de procédure pénale

30 Alice Vitard, *Pourquoi la France entame-t-elle un bras de fer avec l'Europe sur la conservation des métadonnées ?*, L'Usine Digitale, 26 mars 2021.

31 Vie publique, *Données de connexion : leur conservation jugée conforme au droit européen*, 28 avril 2021.

de la victime pour pouvoir lui imputer les faits. Elles permettent également d'identifier ceux qui diffusent des contenus illicites sur Internet tels les contenus pédopornographiques, l'apologie du terrorisme.

Elles sont enfin indispensables pour identifier les co-auteurs ou complices d'une atteinte aux biens ou leurs éventuels receleurs.

Fort de ces constats, maintenir la conservation des données de connexion apparaît primordial. Toutefois, considérant la nécessité de maintenir un équilibre permanent entre le droit au respect de la vie privée et la nécessité de poursuivre les auteurs d'infractions, il apparaît nécessaire de redéfinir les modalités d'accès à ces mêmes données.

Vers une redéfinition de l'accès aux données de connexion afin de concilier le droit au respect de la vie privée et la nécessité de poursuivre les auteurs d'infractions

Cet accès par les autorités publiques aux données de connexion revêt nécessairement une sensibilité particulière puisque, comme cela a été démontré, celles-ci permettent de révéler les usages numériques d'un utilisateur ou encore de reconstituer a posteriori un parcours par le biais des données de localisation.

Le Conseil constitutionnel comme la CJUE ont apporté des précisions sur les modalités de cet accès s'agissant du contrôle de proportionnalité dans l'atteinte au droit au respect de la vie privée.

Dans une décision récente, le Conseil constitutionnel a jugé inconstitutionnel, dans le cadre de l'enquête préliminaire, la réquisition des données de connexion par le procureur de la République ou, sur autorisation de celui-ci, par l'officier ou l'agent de police judiciaire[32]. Examinant les garanties qui entourent cet accès, le Conseil constate qu'il y a une garantie procédurale constituée par l'autorisation donnée par le procureur de la République, magistrat de l'ordre judiciaire, mais qu'elle est la seule, cette seule garantie étant alors insuffisante. Ainsi, il ne remet pas en cause, en soi, l'accès aux données de connexion. Il exige en revanche d'autres garanties procédurales que le législateur doit prévoir considérant l'ingérence dans le droit au respect de la vie privée.

Considérant les enjeux immenses d'une abrogation immédiate, le Conseil a reporté au 31 décembre 2022 l'abrogation des dispositions contestées. Ce report d'une durée supérieure à un an implique que le législateur prenne la mesure des modifications substantielles de la procédure pénale à réaliser. Suivant les options implicitement présentées par le Conseil, le législateur pourrait limiter le champ d'application de cet accès à une typologie d'infractions, prévoir une autorisation limitée dans le temps du procureur de la République assortie d'une intervention du juge des libertés et de la détention au-delà d'un certain délai[33].

32 Cons. const. 3 décembre 2021, n°2021-952 QPC.

33 M. Audibert, *Inconstitutionnalité différée des réquisitions de données informatiques par le procureur de la République dans le cadre de l'enquête préliminaire : le jour d'après*, Lexbase Pénal, n°44, 23 décembre 2021

Tirant les conséquences de la décision du Conseil constitutionnel, le législateur a d'ores et déjà modifié les dispositions du code de procédure pénale afin d'encadrer et de limiter le recours aux réquisitions visant à obtenir des données de connexion. Ainsi, la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement prévoit un nouvel article 60-1-2 du code de procédure pénale. Les réquisitions portant sur les données de connexion ne seront possibles, à peine de nullité, si les nécessités de la procédure l'exigent, que dans les hypothèses suivantes : « la procédure porte sur un crime ou sur un délit puni d'une peine de trois ans d'emprisonnement ; la procédure porte sur un délit puni d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques et ces réquisitions ont pour seul objet d'identifier l'auteur de l'infraction ; ces réquisitions concernent les équipements terminaux de la victime et interviennent à la demande de celle-ci en cas de délit puni d'une peine d'emprisonnement ; ces réquisitions tendent à retrouver une personne disparue dans le cadre des procédures prévues aux articles 74-1 ou 80-4 du code de procédure pénale ou sont effectuées dans le cadre de la procédure prévue à l'article 706-106-4 »[34]. Nous avons donc ici des conditions supplémentaires prévues par le législateur et uniquement liées au périmètre infractionnel sur le critère de la gravité de la sanction pénale avec une disposition spécifique lorsqu'un réseau de communications électroniques a été utilisé par l'auteur de l'infraction.

34 Article 60-1-2 du Code de procédure pénale.

Toutefois, si le Conseil constitutionnel a demandé des garanties supplémentaires, il convient de noter que la CJUE a d'ores et déjà adopté une position plus tranchée.

Dans un arrêt du 2 mars 2021[35], la Cour déclare que le droit de l'Union européenne s'oppose à une législation nationale donnant compétence au ministère public, qui dirige l'enquête judiciaire et exerce, le cas échéant, l'action publique, pour autoriser l'accès par les enquêteurs aux données de connexion. Celle-ci explique en substance que l'autorité qui exerce le contrôle de proportionnalité préalable ne peut être la même que celle qui sollicite l'accès aux données de connexion[36]. Cette autorité ne doit pas être impliquée dans la conduite de l'enquête pénale.

Si le procureur de la République semble d'emblée exclu de cette faculté, par ricochet et dans la mesure où le juge d'instruction dirige l'information judiciaire[37] et peut requérir la communication de données de connexion[38], celui-ci voit cette prérogative directement remise en cause par la CJUE.

Ainsi, au travers de l'enjeu relatif à l'accès aux données de connexion, nous sommes en droit de nous interroger sur le fait de savoir si nous ne sommes pas à l'aune d'un basculement majeur de notre procédure pénale. Ce basculement pourrait consister en la création d'un juge de l'enquête : magistrat non impliqué dans la procédure

35 CJUE, Prokuratuur, 2 mars 2021, C-746/18.

36 M. Audibert, *La conservation et l'accès aux métadonnées dans le cadre des enquêtes judiciaires : vers un bouleversement dans la procédure pénale française ?*, Lexbase Pénal, n°36, 25 mars 2021, pp. 73-78.

37 Article 81 du Code de procédure pénale.

38 Article 99-3 du Code de procédure pénale.

et qui serait uniquement chargé, à la demande des enquêteurs, du procureur de la République ou du juge d'instruction, d'autoriser certains actes attentatoires à des droits et des libertés.

Ce basculement soulèverait de nombreuses questions capacitaires en matière d'absorption du volume de réquisitions et s'agissant de la nécessité de traiter rapidement les demandes émises par les enquêteurs, eu égard au risque de déperdition des preuves.

Le chef d'escadron Matthieu AUDIBERT en bref :

Officier de gendarmerie, le chef d'escadron Matthieu Audibert est juriste de formation, spécialisé en droit pénal et en procédure pénale appliqués à la cybercriminalité. Il est diplômé de l'université Paris Nanterre, de Sciences Po Aix en Provence, de l'université de Montpellier et de l'École des officiers de la Gendarmerie nationale. Il prépare une thèse de doctorat en droit privé et sciences criminelles portant sur le recueil de la preuve numérique en procédure pénale.

L'APPORT DU RENSEIGNEMENT CRIMINEL DANS LE TRAITEMENT DES DONNÉES EN MASSE

Les évolutions technologiques de ces dernières années ont eu pour conséquence d'augmenter le volume de *data*[1], stockés sur des serveurs ou sur des supports physiques devenus des objets de consommation courante. Parallèlement, les investissements dans les nouvelles technologies (notamment *data science*) effectués par l'Institution, ont permis de doter un grand nombre de militaires d'outils permettant l'appréhension des données informatiques et la création d'unités chargées de les développer[2]. Il en résulte une confrontation plus régulière des enquêteurs à des volumes importants de données à traiter, créant un enjeu pour l'exercice de la police judiciaire.

CLÉMENT BOUHIER

Maréchal des logis-Chef à la Division du renseignement au sein du département analyse stratégique du Service central de renseignement criminel de la Gendarmerie nationale

À compter de 2015, la Gendarmerie nationale a intégré un nouvel axe majeur : le renseignement criminel. Le traitement des données étant l'une des phases du processus d'exploitation de l'information[3], l'apport possible aux investigations judiciaires d'une méthodologie de renseignement criminel est à prendre en compte.

La pertinence d'une approche par le renseignement criminel

Sur les plans étymologique et juridique, les notions de renseignement et de police judiciaire se distinguent, en France, de par leurs objectifs et leurs moyens. Encourageant une méthodologie nouvelle pour les forces de sécurité, le renseignement criminel permet non seulement de mieux appréhender la criminalité et ses auteurs en vue d'agir sur les opportunités criminelles[4], mais également d'optimiser l'action judiciaire par une aide à la décision stratégique, tactique ou opérationnelle. Issu des théories de la criminologie environnementale[5], le renseignement criminel appréhende la criminalité sous trois angles : les faits (phénomènes, répétition), les individus (profils et groupes), et les lieux (géographie criminelle et flux). Ce modèle de police guidé par le renseignement (*Intelligence-led policing - ILP*) théorisé par Jerry Ratcliffe,

1 Une étude Statista de 2019 pour le Journal du net évalue le volume de données crées depuis 2010 (deux zettaoctecs) à 47 zettaoctects en 2020, et à 2142 zettaoctets en 2035, soit 2142 milliards de téraoctets. https://www.journaldunet.com/solutions/dsi/1424245-le-volume-de-donnees-mondial-sera-multiplie-par-45-entre-2020-et-2035-selon-statista/.

2 Le Service central de renseignement criminel (SCRC) possède son propre Centre des sciences de la donnée.

3 Bulinge Franck, *Maîtriser l'information stratégique*, De Boeck ADBS, Association des professionnels de l'information et de la documentation, 2014, p.65. L'auteur décrit ce processus comme reposant « *sur l'idée d'une transformation des données en information, puis en connaissances* ».

4 De Maillard Clément, *Le renseignement criminel dans les forces de police françaises*, Thèse, Université de Lausanne, 2017, p. 22, à propos de la théorie des opportunités criminelles (Felson & Clarke, 1998).

5 *Ibid.*, p.22.

invite à dépasser certaines caractéristiques du modèle traditionnel[6], freinant l'adaptabilité des institutions policières à l'évolution des menaces devenues globales et modernes[7].

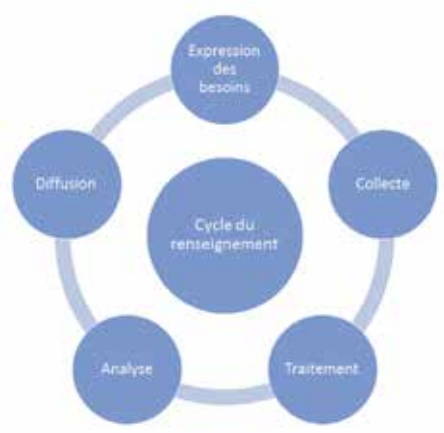
Ce modèle invite à la proactivité et au traitement continu de l'information[8]. La conception du renseignement criminel par la Gendarmerie nationale le rejoint : un processus global « *relatif au traitement de ces informations, qui englobe la collecte, l'élaboration et la diffusion du renseignement, dans le but final d'une exploitation par une unité d'enquête et/ou par un échelon de commandement* »[9]. À ce titre, appréhender le traitement de données en masse à travers un processus de transformation proposé par Ratcliffe (*Diki continuum*) souligne l'influence des outils et l'importance de la relation analyste-enquêteur sur l'orientation des investigations. Le renseignement criminel appliqué au traitement de données en masse permet d'ajouter, au raisonnement linéaire de l'investigation, un raisonnement circulaire basé sur une méthodologie de renseignement orienté vers la transformation de la donnée en information utile pour la police judiciaire en général, et pour l'enquête en particulier.

6 Ratcliffe Jerry, Intelligence-led policing, Routledge, Taylor & Francis Group, 2016, p.50. Il est question du caractère majoritairement réactif à l'événement, basé sur le traitement répressif du fait criminel, encourageant la compartimentation des connaissances par dossier au détriment d'un travail d'agrégation des connaissances et d'une adaptabilité aux menaces.

7 *Ibid.*, p.23.

8 Barlatier Jérôme, *Management de l'enquête et ingénierie judiciaire*, 2017, p.270.

9 Circulaire 175000/GEND/DOE/SDPJ/BPJ du 18 mai 2015 relative au renseignement criminel.



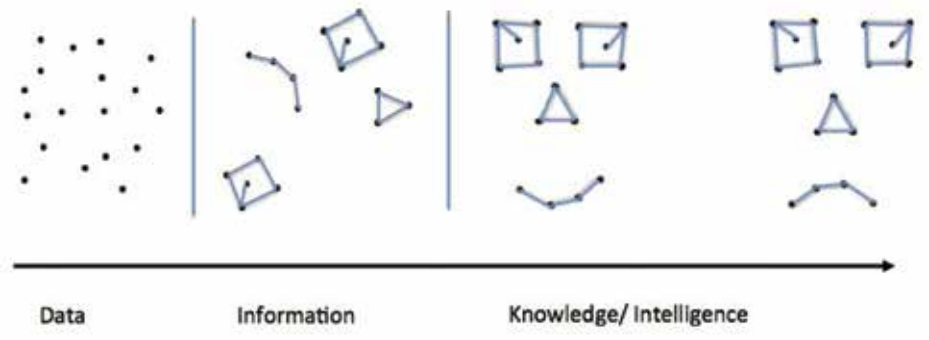
© Wikipédia

Le classique cycle du renseignement

La transformation de l'information : sciences et saillances de la donnée au service de la connaissance

Le *continuum DIKI*, pour *Data-information-Knowledge-Intelligence* (donnée – information – connaissance – renseignement) illustre la transformation des données en éléments de connaissance conduisant à la production de renseignement. Il est dérivé de la modélisation d'un processus régulièrement présent dans la littérature des sciences de l'information, où il est très souvent utilisé pour décrire les chaînes d'interactions cognitive[10]. L'une des caractéristiques du renseignement criminel paraît être l'ouverture d'esprit qu'il encourage, notamment avec l'aspect multidisciplinaire (au sens académique) du métier d'analyste qui en est le cœur nucléaire. Il permet d'associer à l'emploi d'outils de traitement de données, une méthodologie d'exploitation

10 Régulièrement représenté DIKW, *Data – Information – Knowledge – Wisdom* (sagesse).



© DR

De la donnée jusqu'à la connaissance et le renseignement en passant par l'information

de nature à révéler / optimiser le potentiel informationnel qui en émanent[11].

Au regard des sciences de l'information et de la communication, ce processus de transformation amène à dissocier, en dépit de leur nature consubstantielle, données et informations.

Selon certains auteurs, les données composent la « matière » de l'information[12]. Elles sont « *un objet théoriquement inerte, mais intrinsèquement signifiant* »[13]. Il semble qu'elles n'aient pas de charge informationnelle prédéterminée[14] : si « *l'information n'existe pas en tant que telle, elle n'existe que si elle est activement reçue* »[15]. Ce sont donc à la fois, la mise en relation de ces données à travers l'outil, et leur observation (enquêteur et analyste), qui en feront émaner le potentiel informationnel. Aussi, celui-ci sera conditionné tant par l'architecture de l'outil (forme et relations entre les données) que par les connaissances de l'enquêteur et de l'analyste (saillances et évaluations des informations).

L'enquêteur cherchera à confirmer ses hypothèses de travail ou à les reformuler. En effet, si l'information produit « *une modification de l'état de connaissance de celui qui la reçoit* »[16], l'enquêteur et l'analyste pourront constater des caractéristiques

11 Beau Francis, « Faire parler ses données : de la masse à la substance, le sens en question », *Rev. Commun. Organ. Société Savoir Inf.* COSSI, Méthodes et stratégies de gestion de l'information par les organisations : des « big data » aux « thick data », 2018, [en ligne]. « *Dans un monde dominé par la technique, il semble important de ne pas focaliser notre attention sur les seuls instruments que la technologie nous propose (voire parfois nous impose), en s'intéressant d'abord au besoin opérationnel qui donne sens à l'information dans l'action, et à la volonté qui l'anime.* »

12 Leleu-Merviel Sylvie et Useille Philippe, « Quelques révisions du concept d'information », in *Problématiques émergentes dans les sciences de l'information*, Lavoisier, 2008, p. 37, citant Luciano Floridi.

13 Bulinge Franck, *Maîtriser l'information stratégique*, De Boeck ADBS, Association des professionnels de l'information et de la documentation, 2014, p. 35.

14 Weaver Warren, « Recent Contributions to The Mathematical Theory of Communication », 1949, p.4 concernant les travaux de Claude Shannon et le risque de mésinterprétation du mot information : « *The concept of information applies not to the individual messages (as the concept of meaning would)* ».

15 Couzinet Viviane, Les connaissances au regard des sciences de l'information et de la communication : sens et sujets dans l'inter-discipline, *Sem. Connaiss.*, Université de NANTES, 2006, (colloque) p. 2, citant Jean Meyriat.

16 *Ibid.*,p.2.

inattendues ou inhabituelles, générant de nouvelles recherches et observations.

L'analyste cherchera à détecter comme un élément de pattern, c'est-à-dire de modèle criminel[17], une répétition (ou une anomalie) dans la donnée de masse.

De la connaissance au renseignement : l'analyse des données au service de l'enquête

Le renseignement criminel permet d'orienter les magistrats et enquêteurs dans leurs investigations (caractérisation d'infraction, recherches d'éléments probants, détection de sérialité, etc.). Aussi, le traitement automatisé peut concerner trois types de données :

– structurées (fichiers centraux et donnée institutionnelle) ;

– non-structurées (enquêtes judiciaires dont perquisitions en ligne ou non, données remises par les victimes, obtenues sur réquisitions, etc., souvent traitées par un logiciel de rapprochement des articles 230-20 et s. du CPP) ;

– hybrides (notamment fichiers d'analyse sérielle des articles 230-12 et s. du CPP, Application de traitement du renseignement criminel - ATRC) ;

Ces données sont « attendues », dans leurs nature et forme, (données structurées) ou « inattendues » (données non structurées/hybrides). Les informations qui en émanent sont donc attendues ou non. Selon cette approche, l'outil de traitement et l'analyste sont mutuellement « augmentés »[18]. Le dernier doit être associé à la conception du premier (besoin opérationnel, validation métier), pour optimiser son utilisation (exploitation des informations). Le caractère itératif du cycle du renseignement permet l'enrichissement perpétuel des connaissances au gré de ces utilisations : au-delà de l'exploitation d'une « *donnée primaire* » (directement recueillie), se dessine celle de « *données secondaires* » « déjà manipulées et transformées en information »[19]. Les bénéfices de cette approche s'observent aux niveaux macro et micro-judiciaire.

Pour le premier, les enjeux principaux semblent la détection, la modélisation criminelle, et l'orientation de la stratégie judiciaire. Concernant principalement l'exploitation des fichiers centraux et des bases sérielles, ces actions se déclinent en trois dimensions :

– détection et caractérisation de signaux faibles d'une menace criminelle ;

– détection de phénomène et répétitions criminelles : modélisation / *pattern* ;

– recoupement (données) et rapprochements (données modélisées, informations évaluées et recoupement

17 De Maillard Clément, *Le renseignement criminel dans les forces de police françaises*, Thèse, Université de Lausanne, 2017, p.40 à propos de la théorie des *pattern*.

18 Il n'est que trop régulièrement question de la seule analyse augmentée par l'outil ou l'algorithme.

19 Bulinge Franck, *Maîtriser l'information stratégique*, De Boeck ADBS, Association des professionnels de l'information et de la documentation, 2014, p.35. L'auteur précise que « *du point de vue de l'intelligence informationnelle, toute information ou connaissance transmise prend immédiatement le statut de donnée* ». Ce postulat illustre, d'une part, la représentation cyclique de l'élaboration du renseignement et, d'autre part, la réalité de la fonction d'analyste : comme l'exprime l'auteur, « *la notion de donnée prise au sens large désigne un intrant dans le système cognitif de l'analyste ou du décideur* ».

confirmés) aux niveaux intermédiaire et national.

Pour le second, les principaux enjeux semblent la contextualisation de l'affaire, (compréhension du modèle criminel), et l'orientation des investigations judiciaires. Ils se déclinent en trois dimensions :

– caractérisation, dans la donnée traitée, de modèles connus : orientation des investigations vers des profils d'auteurs ou des éléments probants et infractions particulières ;

– détection d'un élément de pattern de modèle inconnu ou d'une variation d'un modèle connu : enrichissement de la connaissance générale et orientation des investigations ;

– recoupement (données) et rapprochements (données modélisées, informations évaluées et recoupements confirmés) : orientation et optimisation des investigations.

Dans une logique de renseignement, les éléments de connaissance obtenus à chaque niveau enrichissent l'autre. L'apport du renseignement criminel à ces deux niveaux de l'action judiciaire légitime le dispositif « d'analyste embarqué » sans être un enquêteur supplémentaire, il est un vecteur d'ouverture du champ des connaissances.

Cet enrichissement mutuel se fait par l'analyse pour l'enquête (macro-micro), par l'enquête pour l'analyse (micro-macro), pour le présent et l'avenir (capitalisation de l'expérience). En cela, le cycle du renseignement criminel devient particulièrement vertueux : il favorise une naissance conjointe du savoir partagé entre enquêteurs et analystes.

Enjeux et prospective

La transparence est la clé de la viabilisation des connaissances, tant sur le plan du droit (protection des données personnelles, viabilité des preuves pénales) que sur les plans de la technique et de la méthode : elle garantit de ne pas être « *dépendant de logique calculatoires d'autant plus impérative qu'elles seront […] invisibles* »[20], générant des biais cognitifs.

La flexibilité des outils (accessibilité, modularité des interfaces) est la clé de la pertinence des analyses et de leur adaptabilité aux évolutions des phénomènes. Plus leur conception est réalisée en associant les analystes et les techniciens qui vont en assurer l'exploitation, plus celle-ci répondra au besoin opérationnel. Le choix fait par l'Institution de développer cette filière est plus que jamais un gage d'adaptation aux menaces.

20 Warusfel Bertrand, « *Perspectives sur l'algorithme, entre technique et droits* », *in* Jean-Pierre Clavier (dir.) L'algorithmisation de la justice, Larcier, 2021,p.21.

Pionnière dans la formation au métier d'analyste en renseignement criminel, la gendarmerie doit pouvoir continuer son effort de valorisation de cette mission singulière, parfois présentée comme l'avenir du renseignement[21].

Clément BOUHIER en bref :

Titulaire d'un Master 2 en droit privé (droit des affaires), menées en parallèle d'un engagement important dans la réserve opérationnelle de la Gendarmerie, Clément Bouhier est recruté au cabinet d'un sénateur, président de conseil général, en tant que collaborateur. Il intègre l'ESOG de Châteaulin (29) en 2012. En parallèle de son affectation à la Garde Républicaine il décroche un Master 2 de Droit public de la sécurité et de la défense (Paris II) en 2014, et intègre cette même année le Service de permanence et d'information du Palais de l'Élysée.Affecté à la BTA MERU (60) en mai 2016, il exerce des fonctions d'OPJ à compter de 2017 et développe une appétence pour la police judiciaire. Passionné par les questions juridiques et institutionnelles entourant l'interaction entre les domaines Il rejoint, fin 2018, la division du renseignement du Service central de renseignement criminel où il se spécialise dans l'analyse des contentieux économiques et financiers, et notamment les cyber-escroqueries de masse et les phénomènes de criminalité financière organisée.

21 Laurent Sébastien-Yves, « L'analyse, la ressource cachée du renseignement », Revue des Deux Mondes, 2016, p.65.

L'ENJEU DU TRAITEMENT DE LA PREUVE NUMÉRIQUE DANS UN ENVIRONNEMENT MARQUE PAR L'OMNIPRÉSENCE NUMÉRIQUE

Le traitement de la preuve numérique peut être schématiquement scindé en deux phases : la collecte de la preuve, et l'exploitation de la preuve ainsi collectée. Le choix est fait ici de se focaliser sur la première phase ; le lecteur pourra se référer à l'article sur le traitement des données de masse pour approfondir la question de l'exploitation de la preuve collectée, même si cette dernière ne s'y limite pas.

La numérisation galopante de nos vies quotidiennes et professionnelles induit naturellement une numérisation identique de la délinquance. Les violences faites aux femmes demeurent physiques mais s'étendent aussi à l'espace numérique (installation de logiciels-mouchards par les conjoints, « *revenge porn* »), les menaces contre les élus et le harcèlement scolaire s'expriment en ligne, le vol de véhicules s'opère désormais avec des tablettes de diagnostic électronique théoriquement réservées aux garagistes, les trafiquants de stupéfiants utilisent des réseaux de téléphonie sécurisée dédiés et blanchissent leurs avoirs criminels en cryptoactifs…

NICOLAS DUVINAGE

Colonel, chef de la division technique du COMCYBERGEND

Parallèlement, la multiplication des objets connectés (IoT[1]) fait pousser dans le monde physique une véritable « jungle de la preuve numérique », au milieu de laquelle l'enquêteur risque de se perdre. Alors que les ordinateurs, smartphones et autres clés USB sont bien dans la cible de tout gendarme lors d'une perquisition, il n'en est pas encore toujours de même des consoles domestiques avec assistant vocal (Google Home, Amazon Alexa/Echo, etc), des imprimantes 3D ou des systèmes multimédias embarqués dans les véhicules.

Les difficultés pour les enquêteurs sont multiples. Il convient tout d'abord d'avoir conscience de l'existence-même de ces objets, du fait qu'ils sont susceptibles de contenir des données ou d'en produire (les montres et les réfrigérateurs n'ont pas toujours été connectés !), et de la possibilité d'y être confronté en perquisition : c'est une question de culture générale personnelle, mais la gendarmerie doit accompagner cette acculturation par la formation initiale en école et par la formation continue (stages de qualification), ainsi que par la sensibilisation au quotidien (diffusion de notes d'information, *emails* d'alerte à tous les enquêteurs numériques, etc).

1 IoT, acronyme de *Internet of Things* (internet des objets), désigne aussi par métonymie tout objet connecté (« un IoT »).

Il peut certes exister un fossé générationnel entre des enquêteurs quinquagénaires et des gendarmes « *digital natives* », mais ce sont parfois les plus anciens qui font prendre conscience aux plus jeunes, simples consommateurs passifs dans leur vie privée, que leurs usages numériques du quotidien produisent des traces potentiellement intéressantes pour les investigations.

Même en ayant conscience de la diversité des objets numériques, il reste à l'enquêteur à déceler leur présence. Celle-ci peut être particulièrement furtive : une carte micro-SD, une carte nano-SIM peuvent être cachées n'importe où. Des clés USB existent depuis des années sous forme d'insert dans des objets décoratifs ou autres imitations d'objets de la vie courante, d'apparence parfaitement anodine. Aucune solution miracle n'existe, à part la curiosité, le sens de l'observation, la minutie de l'enquêteur en perquisition, et ses expériences antérieures.

Des caméras miniatures connectées dissimulées dans des faux-plafonds, des micro-espions, et une multitude d'IoT, ne sont parfois décelables et localisables qu'avec un véritable arsenal technologique (caméra thermique, détecteur de jonctions non linéaires, goniométrie radiofréquence, etc). Au regard du coût de certains de ces équipements, seul l'échelon central peut en être doté pour l'instant au sein de la gendarmerie.

Enfin l'enquêteur expérimenté n'oubliera pas l'ubiquité de ces objets : un suspect peut les avoir répartis entre son habitation, sa voiture (coffre, boîte à gants, *etc*), et son bureau.

Clé USB mimant l'apparence d'une clé de voiture, découverte lors d'une perquisition

Il est ensuite nécessaire de savoir si ces objets contiennent des données. La question est, même pour un spécialiste, loin d'être triviale : la diversité des IoT et de leur fonctionnement est telle que la seule cer-

titude e l'expert est...qu'il ne peut en avoir aucune et qu'il doit vérifier au cas par cas.

Certains IoT sont de simples émetteurs ne contenant rien d'autre qu'un identifiant unique (ex. : « *tags RFID*[2] » et autres « traqueurs Bluetooth », servant à géolocaliser un objet). D'autres produisent des données mais ne les stockent pas localement, les transmettant au smartphone de leur propriétaire, ou au serveur distant de l'industriel qui les a fabriqués. D'autres IoT enfin conservent localement les données qu'ils génèrent, en eux-mêmes ou sur une console domestique, sans rien transmettre à distance.

Il convient également de déterminer si ces données sont susceptibles d'intéresser l'enquête : l'IoT « vaut-il la peine » que l'enquêteur se penche sur lui ? Là encore, point de règle ! Ainsi un pèse-personne connecté, *a priori* anodin, peut venir corroborer un faisceau d'indices dans une enquête pour homicide (existence d'une pesée au moment fatal, conformité de la pesée au poids du suspect). De même, dans une affaire où un père suspecté d'infanticide dément la présence de ses enfants à son domicile, l'historique des chaînes de télévision sélectionnées sur une *box* peut devenir crucial, s'il démontre par exemple que plusieurs chaînes pour enfants ont été successivement sélectionnées au cours de l'après-midi du drame.

Il reste en outre à l'enquêteur à savoir extraire les données. L'extraction des données de l'objet lui-même peut, parfois, nécessiter des opérations de démontage physique, voire de dessoudage : dans les cas les plus extrêmes, un travail complexe de laboratoire est indispensable. L'extraction des données envoyées par un IoT sur un *smartphone* ou un ordinateur relève d'opérations ordinaires, avec l'équipement dont sont dotés les enquêteurs numériques locaux, mais peut présenter des difficultés (ex. : constructeur de l'IoT chiffrant les données dans l'application *smartphone* avec un mot de passe spécifique).

Enfin, lorsque les données sont stockées sur les serveurs distants du fabricant, peut se poser la question désormais classique de l'accès transfrontalier aux données détenues par un opérateur étranger non soumis aux obligations légales françaises.

Indépendamment de ce foisonnement d'objets physiques, on assiste à une multiplication des services en ligne, qu'il s'agisse de nouveaux réseaux sociaux (Instagram puis Snapchat et TikTok ont ringardisé Facebook), de services de communication (Signal, Discord et WeChat font désormais de l'ombre à Whatsapp), d'espaces de stockage de données multi-services (comptes Google, Apple, Microsoft, etc, associant emails, carnets d'adresses, albums photos, sauvegarde intégrale du contenu du *smartphone*...), de services « fintech[3] » (coupons PCS Mastercard, comptes Nickel, plateformes d'*exchange*, de *swap* ou de *staking* en cryptomon-

2 Étiquette (*tag*) électronique fonctionnant à base d'un dispositif d'identification radio-fréquences (RFID).

3 Contraction de *financial technologies* (technologies financières).

naies[4], *etc*) et de « néo-banques » (Revolut, N26…).

Ces services constituent un véritable « océan numérique » pour les enquêteurs. Le guichet unique téléphonie-internet (GUTI) du Commandement de la gendarmerie dans le cyberespace (COMCYBERGEND), chargé de la relation avec les opérateurs en ligne, fait lui office de « phare » : inlassablement, il recense ces entreprises françaises ou étrangères, identifie en leur sein un point de contact dédié, documente la nature des données conservées et leur durée – très hétérogène - de conservation, ainsi que les modalités procédurales d'obtention des données extraterritoriales (simple réquisition judiciaire ou demande d'entraide pénale internationale, selon la nature des données), et co-élabore avec ces entreprises les modalités pratiques (modèles de réquisitions bilingues, portails de type LERS[5], *etc*).

Cette « *cloudification*[6] » des données complexifie d'autant le travail des enquêteurs : certaines données que l'on trouvait autrefois dans le *smartphone* du suspect sont désormais stockées sur des serveurs à l'autre bout du monde. Au « simple » travail de perquisition physique s'ajoutent désormais ainsi d'autres actes d'enquête : réquisitions judiciaires à ces opérateurs de services, perquisitions informatiques en ligne (depuis le *smartphone* ou l'ordinateur du suspect, en sa présence et en utilisant ses identifiants/mots de passe, pour se connecter aux données stockées sur des serveurs distants), recherches et constatations en sources ouvertes sur internet et les réseaux sociaux, enquêtes sous pseudonyme et achats de confiance, etc.

À rebrousse-poil de cette omniprésence numérique, le risque est grand pour « l'enquêteur connecté » d'oublier un peu trop vite que la preuve numérique revêt encore, parfois, une dimension physique ou humaine. Des empreintes digitales ou des échantillons d'ADN peuvent ainsi être prélevés sur un objet numérique. Inversement, une photo numérique découverte dans un *smartphone* ou sur un compte de réseau social peut permettre d'identifier physiquement un suspect (ex. : reconnaissance faciale, empreintes digitales[7]). La réussite d'une saisie de millions d'euros en cryptoactifs repose parfois sur la découverte en perquisition d'un simple bout de papier où se trouve griffonnée l'indispensable *seed*[8].

Enfin la multiplication des lanceurs d'alerte, anonymes ou à visage découvert, divulguant des *leaks*[9] (ex. : Julian

4 Opérations de change entre monnaie fiduciaire et cryptomonnaies *(exchange*), de change entre différentes cryptomonnaies entre elles sans passer par une monnaie fiduciaire (*swap*), ou de mutualisation bloquée de fonds en cryptomonnaies afin de générer des dividendes (*staking*).

5 LERS : Law Enforcement e-Request System (portail en ligne de réquisitions judiciaires dédié aux enquêteurs de tous les pays).

6 De l'anglais *cloud* (nuage), utilisé pour désigner les services en ligne.

7 Voir par exemple https://www.liberation.fr/checknews/2019/10/07/risque-t-on-vraiment-se-faire-voler-ses-empreintes-digitales-en-faisant-le-v-de-la-victoire-sur-des-_1755832/ (publié le 7 octobre 2019).

8 « Graîne », également appelée passphrase ou phrase mnémonique : valeur aléatoire de 128 bits, souvent sous forme d'une suite de 12 à 24 mots, qui constitue la clé du *wallet* (coffre-fort numérique) où sont stockés les cryptoactifs.

9 Fuites de données personnelles ou sensibles, initialement confidentielles.

Assange / WikiLeaks, Edward Snowden / NSA leaks, Panama Papers, Frances Haugen / Facebook), rappelle régulièrement que les sources humaines de renseignement ne doivent pas être reléguées aux oubliettes et conservent toute leur pertinence même dans un monde numérique.

Le colonel Nicolas DUVINAGE en bref :

Polytechnicien et titulaire d'un mastère spécialisé de Télécom Paris, Nicolas DUVINAGE a alterné des postes techniques et des commandements opérationnels de terrain. Il a ainsi été commandant de peloton d'escadron de gendarmerie mobile (Besançon - 25), commandant de compagnie de gendarmerie départementale (Rezé - 44) et commandant de la gendarmerie du Finistère (2018-2021). Il a également été adjoint au chef de l'Office central de lutte contre les atteintes à l'environnement et à la santé publique (OCLAESP) de 2012 à 2015. Dans le domaine du numérique, il a été adjoint puis chef du département informatique-électronique de l'IRCGN (désormais Centre national d'expertise du numérique du COMCYBERGEND) de 2001 à 2009, chef du Centre de lutte contre les criminalités numériques (C3N) de 2015 à 2018.

DE L'ESSOR DE LA SÉCURITÉ TECHNOLOGIQUE À TECHNOLOGISATION DE LA SÉCURITÉ : UNE INTÉGRATION EUROPÉENNE PAR LA TECHNOLOGIE

L'engouement de l'Union en matière d'innovations et de solutions high-tech est indéniable. Il est possible d'identifier derrière ce constat deux mouvements distincts en interaction. Le premier, bien connu, est la technologisation de la sécurité qui se manifeste par un flux d'innovations applicables en la matière. Ce premier mouvement se traduit par un recours accru aux nouvelles technologies comme mode gestion des menaces. Quant au deuxième mouvement, il correspond à une intégration européenne par la technologie. Le postulat de cet article est que ce mouvement d'intégration politique s'effectue avec le consentement des États membres, voire sous leur impulsion en ce sens que, au lieu de s'opposer à l'empiètement de leurs compétences en matière de sécurité, ceux-ci se montrent favorables à un renforcement de l'intervention de l'Union, de par la valeur ajoutée qu'elle fournit, pour contrer des menaces transnationales qui s'adaptent quant à elles aisément aux innovations technologiques.

PIERRE BERTHELET

Docteur en droit spécialisé en droit de l'UE, chercheur associé sur les questions de droit et de sécurité à l'Université de Grenoble (CESICE), à l'Université d'Aix-Marseille (CERIC) et auprès du CREOGN

L'engouement de l'Union en matière d'innovations et de solutions high-tech est incontestable. Les travaux actuels portent notamment sur l'interopérabilité des bases de données européennes, la digitalisation de la coopération de la coopération policière locale, l'usage par Europol de dispositifs d'intelligence artificielle dans le cadre de son mandat, sans oublier l'identification et le suivi de technologies émergentes. En matière de recherche et d'innovation, l'Union soutient ainsi des projets de scanners implantés dans les aéroports européens, le développement de techniques de criminalistique de pointe, des outils numériques de surveillance et de lutte de la radicalisation en ligne, de même que des méthodes de collecte des preuves électroniques dans les affaires pénale[1].

En prenant du recul, il est possible d'identifier deux mouvements distincts mais qui interagissent. Le premier, bien connu, est l'essor de la sécurité technologique, ceci dans un contexte plus large de l'imposition du « Système technicien » - selon la célèbre formule de Jacques Ellul, dans sociétés contemporaines qui sacralisent le progrès technique[2].

1 COM/2018/845 final.

2 Jacques Ellul, *La technique : ou L'enjeu du siècle*, Paris, Économica, 2008.

Manifestation dynamique du développement de la sécurité technologique, la technologisation de la sécurité se traduit par une approche privilégiée aux nouvelles technologies comme mode gestion des menaces.

Quant au deuxième mouvement, il correspond à une intégration européenne par la technologie. En matière de sécurité, cette évolution peut sembler compréhensible, dans la mesure où les mutations des politiques en matière de sécurité ne sont que le reflet des mutations des politiques nationales. Au-delà, ce mouvement traduit une forme spécialisée d'intégration, une intégration technologique, qui actualise et questionne le rôle politique de l'Union (par exemple la souveraineté européenne en matière numérique[3]).

Cela étant, et c'est le postulat de cet article, le processus de technologisation de la sécurité intérieure européenne est une manifestation d'un mouvement d'intégration politique discret qui s'effectue avec le consentement des États membres, favorables à la mise en place de dispositifs plus ambitieux. Le coordinateur pour la lutte antiterroriste notait à ce sujet que « depuis 2015, et les attentats de *Charlie Hebdo*, du Bataclan et de Bruxelles, l'Union européenne s'est vraiment mobilisée, sans chercher à remplacer les États membres. Pourtant, j'observe une demande pour « plus d'Europe » de la part des services de renseignement, des services de police, ou des magistrats »[4]. Loin de montrer une opposition de principe quant à l'exercice par l'Union de ses compétences au nom de l'empiètement de leurs compétences en matière de sécurité, ils y sont plutôt enclins de par la valeur ajoutée qu'elle fournit, dans la lutte qu'ils mènent pour contrer des menaces transnationales qui s'adaptent aisément aux innovations technologiques. En écho avec le développement de systèmes experts au sein des sociétés contemporaines, cette forme d'intégration politique fait écho aux travaux de la régulation par l'expertise[5].

Un attrait de l'UE pour les nouvelles technologies liée aux mutations du paysage criminel

L'approche technologique de la sécurité observable en matière de sécurité intérieure s'explique par l'évolution de la menace qui tend, elle aussi, à devenir toujours plus technologique. Comme le précise la communication de la Commission du 24 juillet 2020 relative à la stratégie de l'UE pour l'union de la sécurité[6], les sociétés actuelles reposent sur des infrastructures et des technologies numériques, ce qui génère des dépendances technologiques accrues. Ces dépendances, renforcées par le phénomène des objets connectés, créent des fragilités au sens où le dysfonctionnement de ces infrastructures entraîne une paralysie de pans entiers de secteurs économiques.

À cet égard, si la pandémie de COVID-19 a suscité un intérêt croissant aux nouvelles

3 COM/2020/66 final.

4 Sénat, Audition de M. Gilles de Kerchove, coordinateur de l'Union Européenne pour la lutte contre le terrorisme, 12 novembre 2020.

5 Giandomenico Majone, *Regulating Europe : problems and prospects*, Working Paper, Florence : European University Institute, 1989.

6 COM(2020) 605 final.

technologies, elle a révélé en parallèle des faiblesses intrinsèques au monde numérique. Les récents rapports d'Europol sur la cybersécurité (iOCTA), ainsi que ceux produits par l'agence policière européenne au cours des années 2020[7], ont mis en exergue à cet égard une cybercriminalité particulièrement active.

La sécurité technologique apparaît dès lors comme une réponse à des menaces qui, selon l'office, s'accroissent et se complexifient. La propagande terroriste en ligne est un exemple. Le rapport d'Europol sur l'état de la menace terroriste (TE-SAT) note que les groupes terroristes ont recours aux nouvelles technologies pour diffuser la propagande en développant une communauté active de sympathisants. Cette communauté relaie des messages et des vidéos qui deviennent très vite viraux. Or, une telle diffusion si large – la décapitation de Samuel Paty l'illustre – et si rapide – les attaques de Christchurch sont également un exemple – constitue un défi pour les services répressifs nationaux.

Quant à la nouvelle stratégie de cybersécurité de l'UE en matière de sécurité du 16 décembre 2020[8], et approuvée par le Conseil le 9 mars 2021, elle insiste sur les effets délétères de la polarisation accrue dans le champ des relations internationales, sur l'intensification des campagnes de désinformation et sur l'accroissement des cyberattaques menées contre les infrastructures des États européens, les acteurs économiques, notamment les fournisseurs de services essentiels, ainsi que sur le fonctionnement des institutions démocratiques, en particulier la perturbation des scrutins.

Un intérêt ancien pour les nouvelles technologies, mais qui s'amplifie récemment

L'approche technologique de la sécurité européenne remonte aux années 1990, - il faut de se remémorer le Système d'information Schengen comme colonne vertébrale de la réponse au déficit de sécurité généré par l'ouverture des frontières extérieures -, mais elle s'intensifie au cours des années 2000, après les attaques du 11 septembre 2001. Depuis lors, elle ne cesse de se renforcer.

Un rapport d'Europol souligne à cet égard le fait que certaines des technologies émergentes, notamment l'intelligence artificielle (IA), l'informatique quantique, la 5G, les réseaux décentralisés alternatifs et les crypto-monnaies, l'impression 3D et la biotechnologie ont un impact profond sur le paysage criminel[9]. Cette mutation des menaces implique à cet égard une transformation des activités policières au plan national, et une adaptation de la coopération policière au niveau européen.

La gestion de l'information menée à partir du développement des systèmes d'informations nationaux et européens apparaît comme le fer de lance de ce processus de technologisation de la sécurité intérieure.

7 Catching the virus cybercrime, disinformation and the COVID-19 pandemic (3 avril 2020); Beyond the pandemic - How COVID-19 will shape the serious and organised crime landscape in the EU (30 avril 2020).

8 JOIN(2020) 18.

9 Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement (rapport du 18 juillet 2019).

Depuis de nombreuses années, l'Union développe des outils destinés à faciliter l'échange d'informations entre États membres, partant d'un double constat : l'importance de l'information numérique dans l'activité des services répressifs d'une part, et la persistance d'obstacles au partage transfrontalier dans ce domaine. Depuis les débuts de la « JAI » (Justice et affaires intérieures), les efforts se sont concentrés sur la création de bases de données européennes centralisées (SIS ou les bases d'Europol) et sur la circulation de l'information entre systèmes nationaux, sans création de bases européennes. Les décisions Prüm illustrent à cet égard l'approche décentralisée d'une circulation transfrontalière de données[10]. Si « la disponibilité » des informations était le paradigme dominant à la fin des années 2000, celui de l'interopérabilité l'est à la fin des années 2010. Partant du constant que les bases de données européennes en matière de sécurité et de gestion des flux migratoires ont été développées en silo, et identifiant un ensemble de lacunes structurelles, ce projet opère une refonte de leur fonctionnement, en rationalisant et en favorisant un accès direct et rapide des utilisateurs finaux[11].

Une tendance forte à la technologisation de la sécurité intérieure européenne

Cette diffusion de la technologie apparaît comme une tendance de fond au sens où l'action de l'Union est appréhendée sous un prisme technologique. Les travaux actuels concernant une approche unifiée du filtrage des migrants irréguliers débarqués sont une illustration. Le projet de règlement, présenté le 23 septembre 2020 et actuellement en discussion par le législateur européen, permet un passage aux fichiers de ces personnes, le but étant d'opérer un pré-tri destiné à identifier ceux qui ne représentent pas une menace pour la sécurité, et autorisés à ce titre à soumettre une demande d'asile[12]. À cette fin, une proposition de règlement modificatif du texte établissant le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN), a été présenté le 2 mars 2021[13]. Cette proposition actuellement examinée par le législateur européen met en évidence les ponts qui existent entre la dimension judiciaire (le traitement des données d'identification des ressortissants de pays tiers qui ont fait l'objet de condamnations dans les pays de l'UE), l'asile et l'immigration (dans le contexte du « pacte sur la migration et d'asile » de septembre 2020) et la sécurité (des frontières de l'Union) par les bases données (le projet dit « d'interopérabilité » des bases de données européennes).

À ce propos, dans la foulée de deux règlements de 2018 sur l'interopérabilité, un document de réflexion de la Présidence du Conseil a été publié le 22 novembre 2019 sur le rôle des nouvelles technologies en matière de sécurité[14]. Il insiste sur une approche de la sécurité axée autour de l'anticipation en donnant aux services répressifs de l'UE, grâce à ces nouvelles technolo-

10 Décision 2008/615/JAI et décision 2008/616/JAI.

11 Règlement (UE) 2019/817 et règlement (UE) 2019/818 du 20 mai 2019.

12 COM/2020/612 final.

13 COM/2021/96 final.

14 Doc. Du Conseil n° 14297/19.

gies, un rôle proactif dans la lutte contre un ensemble de menaces contre l'Union et ses États membres (criminalité transfrontalière, terrorisme d'extrême-droite, désinformation et menaces hybrides, "revenants" du Moyen-Orient, grande criminalité etc.) Il s'agit notamment de favoriser la participation et la coordination de ces services aux programmes de recherche et de développement financés par l'UE dans le domaine de la sécurité. Avant d'aborder ceux-ci, il importe d'évoquer la problématique de la question de l'équilibre liberté / sécurité en matière de sécurité intérieure européenne, dans la mesure où le droit de l'Union relatif aux nouvelles technologies, en particulier en matière de rétention des données, a connu des développements importants récemment.

L'essor des nouvelles technologies et la question délicate de l'équilibre liberté / sécurité

Le traitement des communications cryptées est un enjeu de premier plan sur le plan de l'efficacité des enquêtes, mais aussi du point de vue de la protection de la vie privée. Si d'un côté, il importe que les autorités répressives de l'UE disposent de moyens techniques et légaux pour y parvenir, de l'autre, la préservation des droits fondamentaux est également une priorité. En décembre 2020, le Conseil de l'UE a exprimé son souhait d'intensifier la collaboration avec l'industrie technologique et de parvenir d'un cadre réglementaire permettant une action opérationnelle efficace. Pour sa part, la Commission européenne a déclaré, dans la stratégie de l'UE pour lutter contre le crime organisé, aborder cette question d'un accès ciblé aux informations cryptées sans déboucher sur une surveillance aveugle.

Or, l'accès ciblé aux informations cryptées est une question juridique complexe. Dans une résolution sur le chiffrement, le Conseil de l'UE souligne l'importance de solutions techniques et opérationnelles ancrées dans un cadre réglementaire fondé sur les principes de légalité. L'observateur ne manquera pas de noter que ce cadre réglementaire, en cours d'édification, est encore incertain étant donné les solutions jurisprudentielles mouvantes. En effet, les règles octroyant la possibilité donnée aux autorités répressives et judiciaires d'intercepter, collecter et traiter des données chiffrées, tant en ligne que hors ligne, doivent respecter les libertés, en particulier l'article 8 de la Charte des droits fondamentaux. À cet égard, tant la Cour européenne de Strasbourg (CEDH)[15] que celle de Luxembourg (CJUE)[16] avaient interprété largement le droit à la vie privée en refusant le principe d'une surveillance de masse. Cette jurisprudence, particulièrement sévère depuis l'affaire Snowden, s'est émoussée depuis lors[17]. Il n'empêche, en dépit des inflexions récentes, le contrôle juridictionnel continue à encadrer strictement les mécanismes de

15 CEDH, 4 décembre 2015, Zakharov, Req. n°47143/06 ; CEDH., 12 janvier 2016, Szabo, Req.n°37138/14.

16 CJUE, 8 avril 2014, Digital Rights Ireland, C-293/12 & C-594/1 ; CJUE, 6 octobre 2015, C-362/14 ; *Tele2 Sverige* (21 décembre 2016, *Tele2 Sverige AB*, C-203/15 et *Secretary of State for the Home Department*, C-698/15.

17 CEDH, 25 mai 2021, n° 35252/08, Centrum för rättvisa, CEDH, 25 mai 2021, 58170/13, 62322/14 et 24960/15, Big Big Brother Watch et autre.

surveillance de manière à condamner tout usage abusif[18].

Or, le coordonnateur pour la lutte antiterroriste, critique de cette solution jurisprudentielle, déclarait à cet égard, que « personne ne conteste l'utilité du chiffrement. C'est la meilleure manière de protéger la vie privée et les libertés. Il est nécessaire dans un monde dominé par l'Internet des objets, mais nous ne pouvons pas accepter un système dans lequel les autorités de police n'ont plus accès aux contenus. La Cour de Justice de l'Union européenne (CJUE) a développé une jurisprudence restrictive sur la rétention des métadonnées. Le cumul du chiffrement et de l'absence d'accès aux métadonnées laisse les autorités aveugles »[19].

Pour autant, et c'est l'élément de complexité, le curseur n'est pas placé de la même manière selon les juges. La Cour de Justice de l'Union se montre ainsi soucieuse d'empêcher toute surveillance généralisée et indifférenciée tandis que certaines juridictions nationales se révèlent davantage enclines à autoriser l'accéder aux données à caractère personnel aux fins de lutte contre la criminalité grave. Ainsi, le Conseil d'État a estimé que les règles françaises de conservation des données de connexion ne constituent pas une atteinte à la vie privée[20]. S'accordant une autonomie d'interprétation, il définit un point d'équilibre différent entre l'ingérence dans la vie privée d'une part, et la sauvegarde de la sécurité nationale d'autre part.

Une nouvelle opposition UE-États membres concernant le droit des nouvelles technologies ?

Cette divergence d'interprétation peut s'analyser à première vue comme une opposition entre l'Union européenne et la France. D'un côté, cet arrêt révèle un clivage entre la CJUE et le gouvernement français concernant l'étendue de la conservation des données de connexion des citoyens aux fin de lutte contre la criminalité. D'un autre, il met en relief une ligne de fracture juridictionnelle, entre cette même Cour de Justice et le Conseil d'État qui considère que la sécurité relève avant tout du contrôle constitutionnel du juge national. Ce coin enfoncé dans le principe de primauté a été, au demeurant, élargi en octobre 2021 par la Conseil constitutionnel interprétant plus largement les principes inhérents à l'identité constitutionnelle de la France[21].

La décision du Conseil constitutionnel, rendue au moment où la prééminence du droit de l'Union est contestée sans détour par le tribunal constitutionnel polonais, tendrait à penser, de prime abord, à une articulation des systèmes juridiques perçus comme concurrents, dont l'enjeu central est un conflit de primauté, avec pour toile de fond, une opposition UE – États membres, le fossé s'élargissant toujours plus entre eux.

18 CJUE, 6 octobre 2020, Privacy international, C-623/17 ; CJUE, La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophone (aff. jointes C-511/18, C-512/18, C-520-18).

19 Coordonnateur pour la lutte antiterroriste, référence précitée.

20 Conseil d'État , 1er avril 2021, French Data Network et autres n° 393099, 394922, 397844, 397851, 424717 et 424718).

21 Décision n° 2021-940 QPC du 15 octobre 2021, Société Air France.

En réalité, cette description est exagérée, car le clivage UE-États membres a toujours existé. En premier lieu, il est consubstantiel à la construction européenne, puisqu'il incarne la tension permanente entre un projet intégrateur et un projet respectueux des souverainetés nationales. L'articulation des systèmes juridiques, y compris en France, est un défi depuis la création de l'Union et le recours aux réserves constitutionnelles ne sont qu'une étape supplémentaire. Une telle opposition n'est donc qu'une recomposition de cette opposition qui irrigue et structure la construction européenne. En deuxième lieu, il masque des clivages internes aux États membres. Par exemple, la question du placement du curseur entre liberté et sécurité fait l'objet de débats internes parfois intenses. Ainsi, en France, la question de la place de vidéosurveillance intelligente fait l'objet d'âpres discussions. La CNIL a ainsi appelé à la vigilance, le 20 juillet 2020, sur l'utilisation de la reconnaissance faciale ainsi que sur la tenue d'un débat démocratique sur ces nouveaux usages vidéo, ceci au regard des dispositions du règlement général sur la protection des données (RGPD)[22]. En troisième lieu, il tend à invisibiliser un ensemble de convergences de vues notables en matière de sécurité intérieure.

Recherche & innovation : une forte convergence politique UE-États membres

Il existe un ensemble de convergences importantes de vues, sur les questions relatives à la place de ces nouvelles technologies, y compris au moyen du droit. C'est le cas en matière de recherche et d'innovation.

Europol apparaît à cet égard comme le fer de lance dans ce domaine, puisqu'un « pôle d'innovation de l'UE pour la sécurité intérieure » a été créé en son sein chargés de gérer des projets de recherche technologiques[23]. Ces projets visent à répondre aux besoins opérationnels de la communauté des services nationaux utilisateurs. Il s'agit de développer, en liaison avec le Centre commun de recherche (CCR) de la Commission européenne et le Centre d'innovation de l'office de police, des solutions technologiques répondant à ces besoins, à partir des avancées de la recherche existante. Ceci étant dit, Europol n'est pas une agence de recherche proprement dite, mais un pôle collaboratif, c'est-à-dire une plateforme qui rassemble les laboratoires d'innovation d'autres agences de l'UE (par exemple l'agence eu-LISA ou Eurojust) et des États membres[24]. La stratégie d'Europol 2020+ souhaite à cet égard fournir un soutien aux États membres en faisant d'Europol, à travers cette structure, un point central pour l'innovation et la recherche en matière répressive[25].

En réponse, cet *Europol innovation hub* nouvellement créé surveille les technologies émergentes et les avancées technologiques dans certains domaines correspondant à certains besoins identifiés. Il coordonne des projets et il constitue

22 https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras.

23 Voir priorité stratégique n° 4 de la Europol Strategy 2020+.

24 Doc. du Conseil du 25 novembre 2019, WK n° 13266/2019 INIT.

25 Europol Strategy 2020+, approuvée par le conseil d'administration le 13 Décembre 2018.

une plate-forme de dialogue entre des experts de la recherche et de l'innovation en matière de sécurité intérieure issus des mondes divers : institutions et agences européennes, police et douanes, justice et garde-frontières.

La stratégie d'Europol 2020+ souligne une mutation dynamique du paysage de la sécurité, caractérisée par un développement technologique rapide. Cette situation place les services répressifs dans une position nouvelle au sens où d'un côté, ces mutations sont ambivalentes. Elles sont un défi pour eux, à savoir, disposer de compétences et d'outils actualisés à l'heure des restrictions budgétaires et d'acquisition coûteuse de nouvelles technologies, et d'un autre côté, elles constituent une opportunité, à savoir disposer de moyen high-tech pour contrer la menace, identifier les criminels et les arrêter. À cet égard, l'office européen de police ambitionne de fournir un support opérationnel agile en fournissant des capacités techniques mutualisées. Les récents efforts de l'agence s'orientent donc dans cette direction, à savoir la mise à disposition de solutions technologiques pour permettre aux services répressifs de mener à bien leurs activités. L'Europe de la sécurité s'inscrit dans ce mouvement de technologisation de la sécurité qu'elle prolonge et amplifie.

Pierre BERTHELET en bref :

Diplômé de l'Université de Harvard aux États-Unis en cybersécurité et de l'Université catholique de Louvain, Pierre Berthelet est docteur en droit spécialisé en droit de l'UE. Il est chercheur associé sur les questions de droit & sécurité à l'Université de Grenoble (CESICE), à l'Université d'Aix-Marseille (CERIC) et auprès du CREOGN.

Diplômé également auprès d'universités britanniques (Oxford & London School of Economics), membre également de l'Association du droit de la Sécurité et de la Défense (AFDSD), de l'IHEDN (AR08), ainsi qu'EURODEFENSE-France, il a fait un post-doctorat en criminologie & relations internationales à l'Université de Laval (Québec).

Ancien conseiller ministériel, il est l'auteur de nombreux travaux universitaires, dont plusieurs ouvrages. Il est intervenant à la faculté de droit de l'Université de Strasbourg et il l'a été pendant plusieurs années auprès de l'École nationale d'Administration (ENA).

L'UNION EUROPÉENNE EN QUÊTE D'UNE CYBERDÉFENSE

Depuis la directive NIS (2016) et, plus récemment, avec le règlement européen sur la cybersécurité (2019), l'Union européenne s'est engagée dans une politique de cyberdéfense venant compléter le dispositif de lutte contre la cybercriminalité. L'agression russe en Ukraine a démontré combien l'arme numérique était désormais intégrée dans toute opération militaire. L'Europe montre une solidarité inattendue qui pourrait être le moteur du renforcement d'une cyberdéfense collective renforçant celle des États membres.

MARC WATIN-AUGOUARD

Général d'armée (2S), fondateur du FIC, responsable de la majeure souveraineté numérique et cybersécurité de l'IHEDN

L'Europe s'est d'abord construite sur une ambition économique, initiée par la Communauté européenne du charbon et de l'acier (CECA) devenue Communauté européenne, avant de se muer en Union européenne.

Cela explique pourquoi l'intervention européenne dans le champ du numérique a principalement visé le soutien au Marché unique et la défense du citoyen-consommateur[1]. Après la libre circulation des personnes et des biens, il a fallu organiser la libre circulation des données. Le « Paquet Télécom », le règlement e-IDAS et le règlement général relatif à la protection des données à caractère personnel (RGPD) sont les textes les plus significatifs.

Protéger le consommateur, c'est aussi lutter contre la cybercriminalité. Outre sa participation très active à l'élaboration et au suivi de la Convention de Budapest sur

1 Directive cadre 002/21/CE (directive « cadre » Paquet Telecom) du Parlement européen et du Conseil du 7 mars 2002 ; Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ; Règlement (UE) No 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE Règlement e-idas ; Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union ; Règlement (UE) n°679/2016 relatif à la protection des données à caractère personnel RGPD. Directive (UE) du Parlement européen et du Conseil du 11 décembre 2018 instituant un code européen des communications électroniques.

la cybercriminalité (2001), l'Union européenne a créé deux agences qui, sans être exclusivement dédiées à la lutte contre les infractions cyber,

Issue d'une convention conclue en 1995 entre les États membres, Europol est devenue une agence européenne à la suite de la décision du Conseil du 6 avril 2009. Le traité de Lisbonne a permis de renforcer son efficacité et sa légitimité en communautarisant la coopération policière. L'unité cyber d'Europol (*European Cybercrime Centre* - EC3) constitue un dispositif de soutien aux services d'investigation des pays de l'UE. Les programmes EMPACT (*European Multidisciplinary Platform Against Criminal Threats*) concernent notamment la lutte contre les cyberattaques, les fraudes aux moyens de paiement non liquides et les atteintes aux mineurs. Eurojust est une agence instituée par la décision du Conseil 2002/187/JHA, amendée par la décision du Conseil 2009/426/JHA du 16 décembre 2008. Sa mission est de renforcer l'efficacité des autorités nationales chargées des enquêtes et des poursuites dans les dossiers de criminalité transfrontalière grave et de criminalité organisée pour traduire les criminels en justice de façon rapide et efficace. Eurojust met en œuvre les équipes communes d'enquête (ECE)[2]. De récents succès (Encrochat, Emotet, Revil, etc.) soulignent la qualité de la coopération entre États membres.

La lutte contre la cybercriminalité progresse, mais il faut la compléter par une politique de cyberdéfense, notamment dans le haut du spectre des cybermenaces. La cyberattaque ayant visé l'Estonie, en 2007, a sans doute été un déclencheur. La directive 2008/114/CE du Conseil du 8 décembre 2008 concerne le recensement et la désignation des infrastructures critiques européenne ainsi que l'évaluation de la nécessité d'améliorer leur protection. C'est une première étape suivie, à l'initiative de la France, par la directive du 6 juillet 2016[3] concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI ou NIS). Cette directive, qui devrait être prochainement renforcée (directive NIS2 en cours d'élaboration), s'inscrit dans la logique de la démarche française relative aux OIV et fixe des règles de protection des opérateurs de services essentiels (OSE) et des fournisseurs de services numérique (FSN). À Tallin, lors du Sommet européen des chefs d'État ou de gouvernement sur le numérique (29 septembre 2017), la décision est prise d'élaborer un « paquet cyber ».

La SSI est au programme avec l'élaboration de labels européens de cybersécurité pour les entreprises, la lutte contre la cybercriminalité également (traçabilité, lutte contre la fraude, poursuites pénales). Mais la cyberdéfense fait son apparition avec le règlement européen sur la cybersécurité[4], qui comprend comme éléments « phares », la pérennisation de l'Agence européenne

2 Article 13 de la Convention relative à l'entraide judiciaire en matière pénale conclue le 29 mai 2000.

3 Directive (UE) 2016/1148 du Parlement européen et du Conseil 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.

4 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification (Cybersecurity Act).

pour la cybersécurité (ENISA) et la création d'une « boîte à outils cyberdiplomatique ». S'agissant de l'ENISA, son appellation en anglais est *European Union Agency for Cybersecurity*. C'est donc une agence pour la cybersécurité et non de la cybersécurité. Le choix de la préposition n'est pas neutre en termes de souveraineté nationale. La France et l'Allemagne, en particulier, se sont opposées à toute velléité supranationale pouvant animer certains européistes. Les aspects les plus régaliens, en premier lieu la cyberdéfense, ne peuvent être transférés.

Le règlement du 17 avril 2019 relatif à la cybersécurité européenne consacre donc la prise en compte des enjeux par l'Union sans remettre en cause les prérogatives des États. Il s'agit davantage d'hisser tous les États membres à un niveau comparable, de partager l'information, l'expertise. Plus directement tournée vers la cyberdéfense, la « boîte à outil cyberdiplomatique » s'inscrit dans une posture de rétorsion, de sanction contre les auteurs de cyberattaques agissant hors de l'Union. Parmi les mesures prises, une décision relevant de la Politique étrangère et de sécurité commune (PESC)[5] et un règlement[6] prévoient des mesures restrictives (gel des avoirs financiers, interdiction d'accès ou de transit sur le territoire de l'UE).

Les cyberattaques constituant une menace pour les États membres sont notamment celles qui portent atteinte aux systèmes d'information en ce qui concerne, notamment

– les infrastructures critiques, y compris les câbles sous-marins et les objets lancés dans l'espace extra-atmosphérique, qui sont indispensables au maintien des fonctions vitales de la société, ou à la santé, la sûreté, la sécurité et au bien-être économique ou social des citoyens ;

– les services nécessaires au maintien d'activités sociales et/ou économiques critiques, en particulier dans les secteurs de l'énergie (électricité, pétrole et gaz), des transports (aériens, ferroviaires, fluviaux, maritimes et routiers), des activités bancaires, des infrastructures des marchés financiers, de la santé (prestataires de soins, hôpitaux et cliniques privées), de l'approvisionnement en eau potable et sa distribution, des infrastructures numériques et tout autre secteur essentiel pour l'État membre concerné.

Les menaces extérieures ont leur origine ou sont menées à l'extérieur de l'Union ; elles utilisent des infrastructures situées à l'extérieur de l'Union. Elles sont menées par toute personne physique ou morale, toute entité ou tout organisme établi ou agissant à l'extérieur de l'Union ou avec l'appui, sur les instructions ou sous le contrôle de toute personne physique ou morale, entité ou organisme agissant à l'extérieur de l'Union.

5 Décision (PESC) 2019/797 DU CONSEIL du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres.

6 Règlement (UE) 2019/796 du Conseil du 17 mai 2019, concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres.

À deux reprises[7], des sanctions ont visé des organismes russes, chinois et Nord-coréens et des ressortissants de ces pays. C'est, dans le contexte de l'époque, une affirmation de l'autorité de l'Union puisqu'elle sanctionne des personnes morales ou physiques en précisant leurs liens avec des organes officiels des États dont elles relèvent. Depuis la prise de sanctions à l'égard de la Russie, il y a fort à parier que les sanctions seront prises sans circonvolutions diplomatiques, sous réserve cependant que l'on puisse attribuer à la Russie toutes les cyberattaques ciblant l'Union européenne.

Le développement de la cybersécurité européenne devrait déboucher, selon Thierry Breton, sur un « bouclier européen ». Cette expression doit sans doute être reformulée, car elle laisse imaginer un « parapluie cyber » qui ne peut exister, dès lors que les cyberattaques, dans leur forme paroxystique, y compris les actions qui relèvent de la manipulation de l'information via internet, relèvent de la sécurité nationale et donc de la souveraineté des États membres. La « tortue romaine » serait l'image la plus adaptée. Chacun se protège directement et protège indirectement les autres. Les institutions de l'Union dédiées à la cybersécurité interviennent pour renforcer les plus faible et donner de la cohésion à l'ensemble. L'agression qui vise l'Ukraine est un défi pour l'Union européenne qui a montré sa solidité dans l'adversité.

Depuis la guerre du Kosovo, mais surtout à l'occasion de l'attaque de la Géorgie par la Russie, en 2008, le cyber dans la guerre est une réalité. « *La guerre cyber a bel et bien commencé. Nous ne serons ni naïfs ni aveugles, et nous allons nous y préparer* ».

Ainsi s'exprimait Florence Parly, lors du FIC, en janvier 2019. Aujourd'hui, pas une opération militaire ne se déroule sans être précédée, accompagnée et poursuivie par des cyberopérations. L'agression russe en est l'une des démonstrations les plus criantes.

Les « dividendes de la paix » n'ont jamais été encaissés. Les investissements pour la défense sont désormais urgents. La cyberdéfense, dans ses volets défensifs et offensifs, figurera parmi les actions prioritaires. Ce n'est pas à l'Union de faire la force de chacun, mais à chacun de contribuer à la force de l'Union. Aide-toi, le ciel t'aidera ! telle pourrait être le slogan qui sous-tend une Europe qui a aujourd'hui une voix à exprimer, une voie à tracer.

7 Décision du Conseil (CFSP) 2020/1127 du 30 juillet 2020 et décision (PESC) 2020/1537 du Conseil.

DIRECTEUR DE LA PUBLICATION

Général de Division **Jean-Valéry LETTERMANN**

RÉDACTION

Directeur de la rédaction :
Général de brigade (2S) **François DAOUST,**
Directeur du centre de recherche de l'EOGN

RÉDACTEUR EN CHEF

Lieutenant-colonel (R) **Mathieu FRACHON**

MAQUETTISTES PAO

Anne JOFFRE
SDG

DÉPOT LÉGAL

Raison sociale de l'éditeur :
CREOGN, avenue du 13e Dragons,
77010 Melun cedex
Général de brigade (2S) François Daoust
Imprimerie : SDG - 11 rue Paul Claudel
87000 Limoges
Avril 2022

ANCIENS NUMÉROS, PUBLICATIONS, ÉTUDES...

RETROUVEZ TOUTES NOS PRODUCTIONS SUR :

https://www.gendarmerie.interieur.gouv.fr/crgn/publications

et

https://www.gendarmerie.interieur.gouv.fr/notre-communication/publications-documentations