INTERNATIONAL >
L'Europe face aux défis de la sécurité

DOSSIER > Fuite de données : gestion de crise, mode d'emploi

DROIT > Security and privacy by design dans le droit

REVUE
de la gendarmerie nationale

REVUE TRIMESTRIELLE / DECEMBRE 2018 / N° 263 / PRIX 6 EUROS

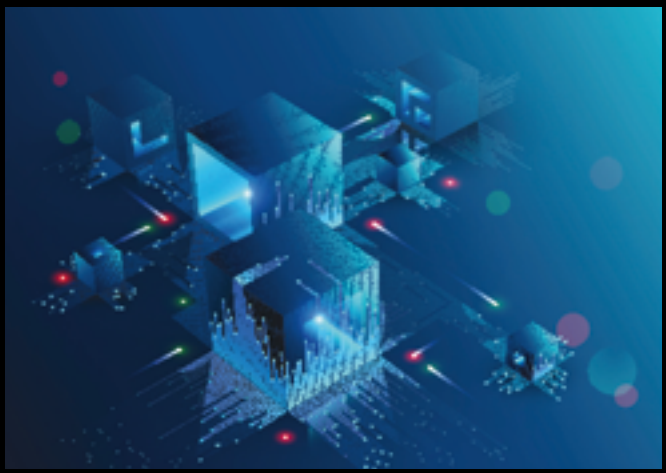
retour sur images NUMÉRO 262

© Gendarmerie nationale

GENDARMERIE ET PATRIMOINE

De nouveaux objets matériels et immatériels utilisés, transformés ou imaginés par les gendarmes pour les besoins de leur mission dans un contexte social et politique évolutif forment différentes pièces du patrimoine de la Gendarmerie nationale. Ils permettent d'illustrer comment l'institution, les gendarmes et leurs familles se sont adaptés et pourquoi d'un usage ou d'un objet on a fait un symbole ou un mythe. Le patrimoine des gendarmes, issu de la collectivité nationale et de la société civile, peut être considéré comme un bien commun national, constitutif de l'identité nationale.

RETROUVEZ EN PAGE 98 DE CE NUMÉRO DES DÉVELOPPEMENTS SUR LA BLOCKCHAIN. NOUVELLE TECHNOLOGIE DE STOCKAGE ET DE TRANSMISSION D'INFORMATIONS, SANS ORGANE DE CONTRÔLE ET ORGANISÉE AUTOUR DE BASES DE DONNÉES DISTRIBUÉES, ELLE PRÉSENTE UN HAUT NIVEAU DE SÉCURITÉ MAIS SUSCITE UNE PRATIQUE CYBERCRIMINELLE ET EN RETOUR UN NOUVEL ART DE L'INVESTIGATION DES FORCES DE POLICE JUDICIAIRE.



©AdobeStock_207011036_copyright_AndSus

La révolution industrielle de l'économie numérique, l'émergence du réseau social comme mode de communication et l'interconnexion généralisée des objets induisent de nouvelles pratiques relationnelles et économiques. Celles-ci génèrent également des activités illégales dont les auteurs démontrent un haut niveau de technicité tout en profitant des disparités juridiques entre les États. L'Union Européenne réagit à ce phénomène en coordonnant les ripostes, en harmonisant les législations et en assurant une fonction de conseil par des formations disposant d'une expertise de haut niveau.

La protection des données personnelles et la sécurité « *by design* » sont maintenant des sujets centraux. L'entrée en vigueur du RGPD et sa déclinaison par les États européens modifie la posture des acteurs des traitements qui doivent tenir compte des impératifs de sécurité dès la conception d'un produit et pour tout son cycle de vie. Le label « *by design* » devient un label de qualité qui infléchira les choix des clients et constituera rapidement un atout commercial.

L'authenticité, la disponibilité, l'intégrité et le cryptage des informations sont un facteur de sécurité de l'e-commerce et de la confiance du citoyen. La technologie de la Blockchain est une des réponses à cette préoccupation des acteurs économiques et politiques. Si elle offre des potentialités aux cybercriminels, elle ouvre la voie à de nouvelles techniques d'investigation pour les enquêteurs qui doivent maîtriser les techniques appropriées à l'extraction des flux frauduleux et des législations différentes.

COL(ER) Philippe Durand,
rédacteur en chef

SOMMAIRE

NUMÉRO 263

INTERNATIONAL

DOSSIER

FOCUS : BLOCKCHAIN

DROIT

DOSSIER

SÉCURITÉ SI et données personnelles

© Global communication network concept. Par metamorworks

LE CONSEIL DE L'EUROPE EST DÉTERMINÉ À PROTÉGER LES ÉTATS

Le Conseil de l'Europe promeut une approche de la lutte contre la cybercriminalité qui repose essentiellement sur le fonds juridique de la convention de Budapest, acte contraignant qui sert de ligne directrice pour élaborer des législations nationales, sur lequel peut se construire une coopération internationale cohérente.

Des structures comme le Comité T-CY, représentant les États parties à la convention, constituent un laboratoire d'idées qui permet d'aborder des mesures juridiques et des solutions lors de situations d'urgence. Il permet aux institutions judiciaires de faire face au défi de la garantie de l'État de droit dans le Cyberespace. De même, le Bureau du programme de lutte contre la cybercriminalité du Conseil de l'Europe (C-PROC) assiste tous les pays qui souhaitent renforcer leurs capacités en matière de justice pénale sur la base des normes de la Convention de Budapest au travers de programmes spécifiques et régionaux.

Le Conseil de l'Europe favorise le développement d'un modèle intelligent reposant sur l'anticipation des cyber-attaques, le renforcement des compétences, le partage et la coopération entre les États et la présence d'un cadre juridique international efficace et respectueux des Droits de l'homme.

Le Conseil de l'Europe
face aux défis de la lutte contre la cybercriminalité

Par Adel Jomni

La cybercriminalité constitue une menace réelle pour l'économie, la démocratie et les droits de l'Homme. Il est désormais acquis qu'aucun pays n'est capable de lutter seul contre cette nouvelle menace. Le Conseil de l'Europe apporte une contribution significative à la lutte contre la cybercriminalité au-delà même de l'espace européen. Il propose un cadre pour prévenir et réprimer les cyber-infractions suivant une approche globale favorisant l'harmonisation des législations internationales relatives au cybercrime, la coopération internationale et le renforcement des capacités des institutions judiciaires dans le monde entier.

ADEL JOMNI

UFR Droit & science politique
Université de Montpellier

Le développement croissant et rapide du numérique en général et du réseau Internet en particulier a changé radicalement la société. En effet, les innovations dans le domaine du numérique sont aujourd'hui omniprésentes. L'Internet des objets (IoT), le Big Data, le cloud computing, l'Intelligence Artificielle (IA), le machine learning, les crypto-monnaies, la Blockchain, l'informatique mobile… constituent le nouveau moteur de la croissance en Europe et dépassent le cadre technologique pour englober tous les secteurs d'activité.

Bien que l'usage presque généralisé de ces innovations numériques ait contribué à améliorer la productivité des entreprises et notre confort, il est également générateur d'une nouvelle délinquance, matérialisée par le développement de la Cybercriminalité.

La lutte contre la cybercriminalité, un enjeu majeur pour le Conseil de l'Europe

Ces dernières années ont vu une augmentation des menaces en matière de vols de données personnelles et d'infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques. Les pertes économiques dues à la cybercriminalité sont en nette hausse. La Commission européenne confirme qu'elles ont quintuplé de 2013 à 2017, et qu'elles pourraient encore quadrupler d'ici à 2019. On évalue à 80 % le pourcentage des entreprises européennes ayant connu un incident lié à la cybercriminalité en 2016. Au niveau mondial, on évalue l'impact économique des attaques à 400 milliards d'euros par an[1].

(1) Source Conseil européen : https://www.consilium.europa.eu/fr/policies/cyber-security/#

On peut également envisager l'exploitation de la vulnérabilité d'opérateurs d'importance vitale (OIV) par le lancement de cyberattaques massives et tenter de paralyser une entreprise ou un État dont la souveraineté peut être impactée par le développement de ces nouvelles armes virtuelles.

À cette situation s'ajoutent, depuis quelques années, de nouvelles formes d'attaques de déstabilisation « politique » constatées récemment lors des élections aux États-Unis en 2016 ou en Europe, notamment en France (2017). Pour Jean-Claude Juncker, président de la Commission européenne : « les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars[2] ».

(2) Discours sur l'état de l'Union, sommet de Tallinn, le 29 septembre 2017.

Depuis plusieurs années, le Conseil de l'Europe joue un rôle très important dans la lutte contre la cybercriminalité dans le monde. Il propose plusieurs formes d'aides, très souvent d'une manière conjointe avec l'UE, pour protéger les sociétés contre la cybercriminalité.

L'approche du Conseil de l'Europe repose essentiellement sur 3 axes

1- La Convention de Budapest sur la Cybercriminalité, une référence pour les institutions judiciaires dans le monde.

La Convention sur la Cybercriminalité du Conseil de l'Europe (CETS No.185), connue sous le nom de la Convention de Budapest (CdB) et son Protocole additionnel, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le

L'approche du Conseil de l'Europe repose essentiellement sur 3 axes

biais de systèmes informatiques, constituent le principal instrument international contraignant en matière de cybercriminalité. Il sert de ligne directrice pour tout pays souhaitant élaborer une législation exhaustive en matière de cybercriminalité (droit pénal matériel et droit procédural), mais aussi de cadre pour une coopération internationale. Le texte de la Convention, adopté en 2001, dépasse le seul cadre du Conseil de l'Europe. *« Ce texte permet, avant tout, de mener la bataille du droit et le Conseil de l'Europe est d'abord une organisation qui promeut les droits de l'Homme, l'état de droit et la démocratie »*, rappelle Alexander Seger, le directeur de C-PROC[3] et Secrétaire exécutif du Comité de la Convention de Budapest sur la cybercriminalité.

Soixante et un pays[4] ont adhéré à cette Convention dont les États-Unis, le Canada, le Japon, le Maroc, le Sénégal, etc. Cet élargissement vers des pays non-membres du Conseil de l'Europe lui confère un champ d'application territorial très large.

La Convention sert de référentiel pour plusieurs pays dans le monde qui cherchent à :

- adapter leur législation afin de prendre en compte les infractions spécifiques aux réseaux numériques,
- intégrer de nouvelles règles de procédures pénales pour accroître l'efficacité des enquêtes et des poursuites,
- améliorer, à travers un dispositif de coopération internationale, l'accès transfrontalier aux preuves électroniques.

2- Le Comité T-CY, « le laboratoire » d'idées sur l'évolution de la Convention

Le Comité de la Convention sur la cybercriminalité (T-CY[5]) représente les États parties. Il a pour vocation de faciliter l'usage et la mise en œuvre effective de la Convention de Budapest sur la cybercriminalité, l'échange d'informations et l'examen de toute proposition d'amendement ou de modification à apporter à ses dispositions. Le TC-Y est un organe de suivi de la

(3) Cybercrime Programme Office of the Council of Europe (Bureau du programme de lutte contre la cybercriminalité du Conseil de l'Europe). https://www.coe.int/fr/web/cybercrime/cybercrime-office-c-proc

(4) https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signaturesv

(5) https://rm.coe.int/reglement-interieur-du-t-cy-adopte-lors-de-la-10eme-reunion-pleniere-d/16802e7279

© Cybrain - adobe Photostock

Le Comité de la Convention sur la cybercriminalité (T-CY[5])

pratique de la Convention de Budapest et un laboratoire d'idées d'amélioration de la Convention et de ses protocoles additionnels, grâce aux facilités d'échanges et de discussions entre les États parties à la Convention.

De nouveaux sujets liés au traitement de la cybercriminalité sont apparus depuis l'élaboration de la Convention. Plusieurs questions ont été abordées par le TC-Y comme la nature du régime juridique à appliquer au Cloud, la détermination de mesures pratiques à privilégier dans le cadre de la coopération avec les fournisseurs de services à l'Internet, la distinction de solutions pour les demandes d'entraide en situation d'urgence. Les réponses apportées et validées par le Comité T-CY font l'objet d'une note[6] d'orientation publiée sur son site.

(6) Exemple de note d'orientation sur la question d'injonction de produire relatives à des informations sur les abonnés. https://rm.coe.int/16806f943d

Le Comité T-CY joue un rôle crucial pour répondre aux défis posés aux institutions judiciaires pour la sécurité et la garantie de l'État de droit dans le Cyberespace.

3- C-PROC : un rôle décisif dans le programme européen de renforcement des capacités

Le Bureau du programme de lutte contre la cybercriminalité du Conseil de l'Europe (C-PROC), à Bucarest, est chargé d'aider les pays du monde entier à renforcer leurs capacités en matière de justice pénale sur la base des normes de la Convention de Budapest. Le soutien de C-PROC touche essentiellement :

– l'adaptation et le renforcement de la législation sur la cybercriminalité et les preuves électroniques conformément aux normes de l'État de droit et des droits de l'Homme (y compris la protection des données),
– la formation des juges, des procureurs et des forces de l'ordre sur les thématiques : Cybercriminalité, preuves numériques et coopération internationale,
– l'amélioration de l'efficacité de la coopération internationale et des synergies entre les organismes publics et privés.

La mise en place de C-PROC fournit au Conseil de l'Europe l'infrastructure nécessaire pour répondre efficacement

aux demandes provenant du monde entier. Parmi les projets gérés par C-PROC et soutenus par l'UE, on note :

– ***Glacy+ : Action Globale sur la Cybercriminalité Élargie*** : C'est un projet conjoint de l'UE (Instrument contribuant à la Paix et à la Stabilité, IcPS) et du Conseil de l'Europe. Il a pour objectif de promouvoir des politiques et des stratégies cohérentes en matière de cybercriminalité et de cybersécurité en Europe et dans d'autres régions du monde. Ce projet vise[7] également le renforcement des capacités des États à disposer d'une législation efficace pour lutter contre la cybercriminalité et l'amélioration des compétences des institutions judiciaires dans les investigations, le recueil des preuves électroniques et la coopération judiciaire internationale. Six pays prioritaires en Afrique et dans la région Asie-Pacifique sont concernés par les actions prévues dans ce projet. Il s'agit de l'Île Maurice, du Maroc, du Sénégal, de l'Afrique du Sud, du Sri Lanka et du Tonga. En outre, les pays d'Amérique latine et des Caraïbes peuvent désormais recevoir un soutien dans le cadre de ce projet.

(7) https://www.coe.int/fr/web/cybercrime/glacyplusactivities

– ***IROCEEDS[8] (Targeting crime proceeds on the internet in South Eastern Europe and Turkey)*** : C'est un projet conjoint de l'UE (IAP II[9], programme d'actions multi-pays) et du Conseil de l'Europe. L'objectif du projet est de renforcer la capacité des autorités dans la région de l'IAP à rechercher, saisir et confisquer les recettes provenant de la cybercriminalité et à prévenir le blanchiment d'argent sur l'Internet. Il concerne les pays suivants : l'Albanie, la Bosnie-Herzégovine, le Monténégro, la Serbie, « l'Ancienne République yougoslave de Macédoine »[10], la Turquie et le Kosovo.

(8) https://www.coe.int/fr/web/cybercrime/iproceeds

(9) Instrument d'aide de préadhésion (http://ec.europa.eu/regional_policy/fr/funding/ipa/)

(10) République de Macédoine du Nord depuis le référendum de septembre 2018.

– ***PGG 2018 : Cybercrime@EAP – International and public/private cooperation*** : Ce projet entre dans le cadre du partenariat pour la bonne gouvernance entre l'UE et le Conseil de l'Europe dans la région du partenariat oriental. Les six pays du groupe des États de l'Europe orientale sont considérés comme des sources et des cibles importantes de la cybercriminalité et constituent donc une préoccupation majeure pour les États membres de l'UE et du Conseil de l'Europe. Le niveau de coopération constaté avec cette région est extrêmement limité, avec très peu de demandes d'entraide judiciaire en matière de preuves électroniques. Le projet vise à faciliter une coopération régionale et internationale efficace en matière de cybercriminalité et de preuves électroniques. L'amélioration du partenariat public-privé fait également partie des objectifs de ce projet étant donné l'importance du secteur privé dans le bon déroulement des enquêtes judiciaires et des investigations. Les pays

prioritairement concernés par ce projet sont : l'Arménie, l'Azerbaïdjan, le Belarus, la Géorgie, la Moldavie et l'Ukraine.

– ***CyberSouth – Coopération en matière de lutte contre la cybercriminalité dans les pays du Sud de l'Europe*** : Ce projet[11] conjoint de l'UE (Instrument européen de voisinage et de partenariat - IEPV) et du Conseil de l'Europe a pour objet d'aider au renforcement de la législation et des capacités institutionnelles dans le domaine de la cybercriminalité et de la preuve numérique dans la région du « Voisinage Sud ». Les pays prioritaires de ce projet sont : l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie.

(11) https://rm.coe.int/cybersouth-summary-of-the-project/1680731825

Des centaines de représentants des institutions judiciaires (magistrats, forces de l'ordre, représentants de gouvernements, etc.) ont bénéficié des quatre programmes cités ci-dessus.

C-PROC est devenu un acteur principal pour accompagner les efforts du Conseil de l'Europe dans sa stratégie face à la montée en puissance de la cybercriminalité dans le monde.

L'ambivalence du numérique, qui crée de nouvelles opportunités économiques, ouvre de nouveaux espaces de libertés, de créations et d'innovations tout en étant porteur de risques majeurs allant jusqu'à toucher la souveraineté des États. Elle exige une vigilance et de moyens importants pour anéantir ou limiter les cyber-risques.

Le Conseil de l'Europe a montré, à travers les actions présentées ci-dessus sa détermination à protéger les États en développant un modèle intelligent reposant sur l'anticipation des cyber-attaques, le renforcement des compétences, le partage et la coopération entre les États et la présence d'un cadre juridique international efficace et respectueux des Droits de l'homme.

L'AUTEUR

Monsieur Adel Jomni est enseignant-chercheur à l'UFR : Droit & science politique de l'université de Montpellier. Il est directeur du diplôme d'université : Cybercriminalité - droit, sécurité de l'information et informatique élargie et co-directeur de la session cybercriminalité et preuve numérique (École nationale de la magistrature-Paris). Expert international auprès du Conseil de l'Europe, il est membre de l'European Cybercrime Training and Eduction Group (ECTEG-Europol). Il est également membre-fondateur du Cecyf.

© EC3 europe – Gendarmerie nationale

UNE EUROPE DE LA CYBERSÉCURITÉ EN PLEINE CONSTRUCTION

L'Union européenne préconise une action basée sur trois piliers : la résilience, une cyberdissuasion et une coopération internationale. Elle conforte la confiance des citoyens par leur protection en ligne et permet un internet libre et réglementé qui favorise une confiance numérique.

À ce titre la promotion d'autorités nationales en la matière selon les prescriptions de la directive relative à la sécurité des réseaux et des systèmes d'information, la création d'un centre européen de cybercompétences vont dans le bons sens. Il en est de même quant à la conception d'exercices européens qui sont des facteurs de cohérence. La cyberdissuasion repose sur une architecture juridique dissuasive et à vocation probatoire. La directive cyberattaques du 12 août 2013 et une législation tendant à l'e-evidence entrent dans cette optique. Un dispositif relatif aux contenus illicites fait l'objet de recommandations dans un contexte de menaces hybrides. Il mérite une large réflexion quant à son champ et aux méthodologies à lui appliquer dans le cadre d'un partenariat avec les hébergeurs.

TOUR D'HORIZON

des principaux dossiers actuels de l'Europe de la cybersécurité

Par Pierre Berthelet

L'Europe de la cybersécurité est en pleine construction. Du côté de la cyberrésilience, il importe d'évoquer la mise en œuvre de la directive « sécurité des réseaux », le projet dit de « cyberact », le projet de centre et de réseau européens de cybercompétence et enfin l'accent mis sur le développement des exercices à grande échelle en matière de cybersécurité ; quant à la cyberdissuasion, il convient de mentionner les directives « cyberattaques », « cyberpreuves » et « fraude en ligne à la carte bancaire », sans oublier les récents développements en matière de lutte contre les contenus illicites sur la Toile, en particulier la propagande terroriste en ligne.

PIERRE BERTHELET

Chercheur associé Centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN)

Depuis plusieurs années à présent, l'Union européenne intervient dans le champ de la cybersécurité, notamment au nom de la protection des infrastructures critiques[1] d'information. Depuis lors, cette action s'est progressivement structurée au motif que la cybersécurité implique une réponse qui dépasse le cadre national.

(1) Voir communication de la Commission, du 30 mars 2009, instituant un plan d'action de l'UE en matière de protection des infrastructures critiques, plan évalué dans une communication du 30 mars 2011 intitulée : « Réalisations et prochaines étapes : vers une cybersécurité mondiale ».

Comprendre l'intervention de l'Union européenne requiert de prendre comme point de départ la stratégie du 19 septembre 217[2], élaborée conjointement par la Commission européenne et la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité[3]. Elle forme le document de référence de l'UE en

(2) JOIN (2017) 450 final

(3) Ci-après respectivement la Commission et la Haute représentante.

la matière. Elle note d'une part, que *« les risques se multiplient de façon exponentielle[4] et d'autre part que les incidents de cybersécurité se diversifient, en ce qui concerne aussi bien leurs auteurs que leurs objectifs. La cyberactivité malveillante constitue une menace non seulement pour nos économies et la progression vers le marché unique numérique, mais aussi pour le fonctionnement même de nos démocraties »*. Face à cela, elle préconise une action basée sur trois piliers, à savoir : assurer la résilience, créer une cyberdissuasion et renforcer la coopération internationale.

(4) Selon certaines études, l'incidence économique de la cybercriminalité a quintuplé entre 2013 et 2017. Elle pourrait quadrupler encore d'ici à 2019.

L'objectif de cet article est de présenter de manière synthétique quelques chantiers actuels de l'Europe de la cybersécurité[5], en se focalisant sur deux des piliers identifiés par la stratégie sur la cybersécurité de 2017, à savoir la cyberrésilience (1) et la cyberdissuasion (2). Les travaux actuels sont menés dans l'optique des conclusions du sommet numérique de Tallinn ayant eu lieu en septembre 2017, au cours duquel les chefs d'État et de gouvernement ont exprimé le vœu de faire de l'Union *« un acteur mondial de premier plan dans le domaine de la cybersécurité d'ici à 2025, afin de s'assurer de la confiance de nos citoyens, consommateurs et entreprises, d'assurer leur protection en ligne et de permettre un internet libre et réglementé »*.

(5) Ceux-ci sont nombreux au demeurant et cette étude, à l'ambition modeste, entend se focaliser seulement sur certains d'entre eux, même si d'autres mériteraient d'un examen plus attentif, comme l'établissement d'un cadre européen de certification pour les produits et services relatifs aux technologies de l'information et de la communication (TIC).

Un premier axe : la cyberésilience

La stratégie sur la cybersécurité de 2013, document directeur précédant la stratégie de 2017, incluait déjà une dimension « résilience ». La version de 2017 reprend cette dimension en spécifiant d'un côté que l'action menée doit être transsectorielle et multiniveaux et d'un autre côté qu'elle doit être non seulement collective mais aussi de grande envergure.

Plusieurs mesures sont préconisées comme le renforcement de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour en faire une : *« Agence européenne pour la sécurité des systèmes d'information »*, par l'octroi d'un mandat permanent[6]. Son rôle est notamment étendu à l'appui à la création de centres d'échange et d'analyse d'informations dans les secteurs critiques ainsi qu'à l'articulation entre les initiatives sectorielles et à la sécurité des réseaux et des systèmes d'information. Trois

(6) Une telle agence ne doit pas être confondue avec une agence de l'Union : EU-LISA. Cette dernière, créée en 2011 et établie à Talinn (avec un centre opérationnel à Strasbourg), est chargée de gérer les systèmes d'information de l'espace de liberté, de sécurité et de justice de l'UE. Ayant fait l'objet d'une réforme en 2018, son mandat, qui concernait l'administration du Système d'information Schengen et du Système d'information sur les visas et d'EURODAC, est étendu à des systèmes en cours de réalisation : l'ETIAS (le système d'autorisation des ressortissants non UE désireux de se rendre dans un État membre), le Système Entrée-Sortie

(qui vise à lutter contre l'immigration clandestine en mesurant les flux d'entrée et de sortie du territoire européen) et l'ECRIS-TCN (destiné à interconnecter les casiers judiciaires nationaux au sujet des ressortissants non UE).

chantiers peuvent être évoqués avec davantage de précision : la mise en œuvre de la directive « sécurité des réseaux », le projet de centre et de réseau européens de cybercompétence et enfin le développement des exercices à grande échelle en matière de cybersécurité.

Bilan de la mise en œuvre de la directive « sécurité des réseaux et des systèmes d'information »

Comme le précisent les conclusions du Conseil européen des 19 et 20 octobre 2017, « la confiance est nécessaire dans le monde numérique. Elle ne peut être instaurée que par l'assurance d'une sécurité plus proactive dès le stade de la conception dans toutes les politiques numériques », et d'insister sur l'importance de renforcer « notre capacité à prévenir, dissuader et déceler les cyberattaques ainsi qu'à y répondre ».

(7) Directive 2016/1148.

(8) Pour une présentation du texte, voir Myriam Quéméner, « La directive NIS, un texte majeur en matière de cybersécurité », Sécurité et Stratégie, vol. 23, n° 3, 2016, p. 50-56.

La directive relative à la sécurité des réseaux et des systèmes d'information, appelée également « directive SRI » (ou NIS) entend précisément répondre à cet objectif[7]. Présentée en parallèle à la stratégie de cybersécurité de 2013, elle a été adoptée par le législateur européen le 6 juillet 2016. Cette directive vise à renforcer les capacités nationales en matière de cybersécurité, notamment en demandant aux États membres de désigner des autorités nationales en matière de sécurité des réseaux et des systèmes d'information et en déterminant une « Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information (SNCS) ». Elle prône aussi l'amélioration d'une culture de la gestion des risques et du signalement des incidents au profit des principaux acteurs économiques en soumettant les opérateurs de services essentiels (OSE) à des notifications d'incidents de sécurité[8].

(9) COM (2017) 476 final.

Le délai de transposition a été fixé au 9 mai 2018 et reporté au 9 novembre 2018 pour ce qui est de l'identification des opérateurs de services essentiels (OSE). Pour la Commission, qui a procédé à l'évaluation du texte en octobre 2017, les États membres de l'UE sont incités à étendre les standards y figurant aux secteurs hors champ d'application du texte[9]. Il est à noter que la France s'est engagée dans cette voie depuis longtemps avec l'extension, par la loi du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019, du champ de compétence de l'ANSSI aux opérateurs d'importance vitale (OIV), plus précisément leurs systèmes d'information d'importance vitale (SIIV). Pour la France, la difficulté de la transposition de la directive SRI venait de

la bonne articulation entre le dispositif OIV et la nouvelle catégorie des OSE.

Vers un centre et un réseau européens de cybercompétence

Une autre mesure préconisée porte sur la mise en place d'un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et d'un réseau de centres nationaux de coordination… Plus exactement, il s'agit d'instituer un centre européen de recherche et de compétences en cybersécurité destiné à mutualiser l'expertise existante au sein de l'Union dans le secteur de la recherche. La stratégie sur la cybersécurité de 2017 précise à ce propos que « ce réseau et ce centre stimuleraient le développement et le déploiement de technologies dans le domaine de la cybersécurité et compléteraient les efforts de renforcement des capacités dans ce domaine au niveau national et de l'Union ». Elle ajoute que : *« la mise en commun et la configuration des efforts de recherche seraient au cœur des préoccupations initiales du centre et du réseau. Pour soutenir le développement des capacités industrielles, le centre de compétences pourrait agir en tant que gestionnaire pour s'occuper des projets multinationaux. Cela donnerait également un nouvel élan à l'innovation et à la compétitivité de l'industrie de l'Union sur la scène mondiale »*.

(10) Voir notre étude : « La coopération public-privé à l'échelle de l'UE : l'émergence d'un « État régulateur » européen en matière de cybersécurité », Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale, note n° 29, décembre 2017.

Une analyse d'impact a été lancée par la Commission le 1er février 2018. Elle constitue le prolongement des travaux effectués dans le cadre du partenariat public-privé sur la cybersécurité (cPPP ou *contractual Public-Private Partnership on cybersecurity*), lancé en 2016 et richement doté (avec un effet démultiplicateur estimé à 1,8 milliard d'euros), dont le rôle est précisément de stimuler l'innovation et à la compétitivité de l'industrie de l'Union[10].

(11) Il s'agit d'une proposition de règlement instituant un programme européen dénommé « Digital Europe ». Doté d'une enveloppe de 9,2 milliards d'euros, il entend stimuler les investissements en matière numérique, notamment dans le domaine de la cybersécurité (un cinquième du fonds étant consacré à ce thème).

(12) P8_TA-PROV (2018) 0258.

L'instauration de cette structure est désormais financée par le programme pour une Europe numérique, présenté par la Commission le 6 juin 2018[11]. Ce futur centre aurait pour tâche de définir des normes en matière de formation des professionnels. C'est d'ailleurs un aspect mis en exergue par le Parlement européen qui, dans sa résolution du 13 juin 2018 sur la cyberdéfense, insiste sur la qualité de la formation sur le thème « La cyberdéfense », notamment en établissant des plateformes techniques et en créant une communauté d'experts européens[12].

Le constat dressé par la Commission européenne est l'existence d'une communauté scientifique encore trop fragmentée, et des liens entre cette dernière et les milieux industriels à parfaire. La situation actuelle entrave la compétitivité de l'Union en matière de cybersécurité. L'instauration d'un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et d'un réseau de centres nationaux de coordination entend donc relever ce défi. Il s'agit, outre le renforcement des capacités industrielles pour favoriser l'innovation et le développement d'une expertise dans le domaine de la cybersécurité de nature à resserrer les liens entre la communauté scientifique et des milieux industriels, d'améliorer les processus de normalisation et de certification. À cet égard, la création de ce centre et de ce réseau s'inscrit dans le sillage du « *Cyberact* » dont l'ambition est de créer un nouveau schéma européen de certification[13]. Concrètement, l'objectif est d'avoir un cadre harmonisé pour la certification de sécurité des produits et services informatiques, précisément pour éviter un phénomène de multiplication des systèmes de certification dans l'Union. La proposition présentée en février 2018 entend réviser le mandat actuel de l'ENISA, de manière à faire de cette agence un centre d'expertise apportant un appui aux États membres (et à la Commission) dans le domaine de la certification de cybersécurité.

(13) COM (2017) 477 final.

© Composite image of spy in black hoodie Par vectorfusionart

L'organisation d'exercices d'envergure renforce la synergie et l'interopérabilité des acteurs dédiés à la lutte contre les cybermenaces.

L'importance des exercices européens

(14) https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/

La stratégie sur la cybersécurité de 2017 souligne le rôle joué par l'ENISA dans la facilitation de la cohérence de l'action entreprise par les divers acteurs chargés de la cybersécurité (ENISA, CERT-EU, Europol, et les CSIRT[14], c'est-à-dire les centres nationaux de réponses aux urgences informatiques). Surtout, elle insiste sur son rôle d'appui dans le développement d'une cyberdéfense européenne en favorisant le partage d'informations, la conscience situationnelle, le renforcement de l'expertise et des réactions coordonnées. Il s'agit notamment, pour ce centre, de « servir de plateforme permettant aux États membres de définir les priorités de l'UE en matière de cyberdéfense, de rechercher des solutions communes, de contribuer à l'élaboration de stratégies communes, de faciliter la formation et la réalisation d'exercices et d'essais en cyberdéfense ».

(15) Voir : https://www.cyber-europe.eu/

Des exercices d'envergure européenne ont déjà lieu. Il s'agit des exercices *Cyber Europe* coordonnés par l'ENISA. À ce propos, un exercice paneuropéen en matière de crises cybernétiques s'est déroulé les 6 et 7 juin 2018. Le cinquième du genre, il avait pour thème la cybersécurité aérienne[15] et il a rassemblé près d'un millier de participants. Si la cyberrésilience, à laquelle contribuent activement les exercices *Cyber Europe*, est un pilier de la stratégie de 2017, la cyberdissuasion en est un autre et non des moindres.

Deuxième axe : la cyberdissuasion

(16) Sur ce thème, voir Marc Watin-Augouard, « La cybercriminalité, criminalité du XXIe siècle », in Gohin, O., Pauvert, B. (dir.), Le droit de la sécurité et de la défense en 2014, Presses Universitaires d'Aix-Marseille, 2015, p. 359-375.

D'après la stratégie sur la cybersécurité de 2017, la dissuasion est orientée avant tout vers la cyberdélinquance. Une cyberdissuasion requiert, d'après ce document, un ensemble de mesures crédibles et dissuasives à cet égard. Il est vrai que le rapport d'Europol 2017 sur la cybercriminalité (iOCTA) souligne un accroissement de la cyberdélinquance[16]. Il s'inscrit dans le sillage du rapport de 2016 notant que celle-ci est davantage agressive, en particulier pour ce qui est des attaques contre les systèmes d'information. Quant au rapport 2018, il confirme la tendance selon laquelle la cybercriminalité se caractérise essentiellement par l'usage récurrent de rançongiciel, par le recours accru aux *cryptomining malware* (malwares qui minent des cryptomonnaies à l'insu des utilisateurs), et par la montée en puissance de nouvelles techniques comme la compromission du *Remote Desktop Protocol* (RDP) et le *brute-forcing* (technique par laquelle l'accès à l'ordinateur de la victime est obtenu grâce à l'emploi de moyens visant à craquer, grâce à multiples tentatives effectuées, des mots de passe faibles)

Plusieurs travaux importants doivent être mentionnés, destinés à établir un cadre juridique européen de manière à éviter que les cybercriminels ne tirent profit des différences sur les plans légaux et techniques entre les États membres de l'UE[17] : les directives « cyberattaques », « e-evidence » et « fraude en ligne à la carte bancaire ». L'accent doit être mis aussi sur la lutte contre les contenus illicites, en particulier la propagande terroriste en ligne, manifestation de l'importance du contrôle de la couche sémantique de l'espace numérique[18].

(17) Voir l'article de Grégory Mounier (chef d'unité au centre européen de lutte contre la cybercriminalité (EC3) d'Europol) : « Enquêtes internationales et poursuite des cybercriminels – État des lieux et défis juridiques », L'Observateur de Bruxelles, n° 105, juillet 2016, p. 14-18.

(18) Voir Marc Watin-Augouard, « La couche sémantique de l'espace numérique : espace de liberté ou d'asservissement ? », Revue de la Gendarmerie nationale, n° 260, décembre 2017, p. 53-56.

Directive « cyberattaques » et la preuve numérique

L'une des premières réponses de portée majeure de l'Union a trait à l'adoption de la directive dite « cyberattaques »[19]. Adoptée le 12 août 2013 et transposée au plus tard par les États membres le 4 septembre 2015, elle établit un socle juridique commun pour ces États afin de sanctionner les attaques contre les systèmes d'information. Un rapport de la Commission, du 13 septembre 2017, dresse un bilan positif de la mise en œuvre de cette directive destinée à élaborer une définition commune des attaques et à harmoniser les niveaux de sanctions[20]. Elle considère en effet que ce texte « a permis d'accomplir des progrès substantiels en matière de criminalisation des cyberattaques à un niveau comparable dans tous les États membres, ce qui facilite la coopération transfrontière entre les autorités répressives qui enquêtent sur ce type d'infractions ».

(19) Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

(20) COM (2017) 474 final.

Cela étant, comme le fait remarquer le rapport d'évaluation, cette directive constitue le premier maillon d'un droit pénal européen spécialisé sur les questions liées à la cybercriminalité. Elle mentionne que pour faciliter les enquêtes criminelles concernant ce type d'attaques, une législation doit être élaborée et destinée à faciliter l'accès transfrontière aux preuves électroniques. C'est dans ce contexte qu'a été présentée, le 17 avril 2018, une **directive** et un **règlement** dénommé « e-evidence » visant à s'attaquer au problème d'accès transfrontalier à la preuve numérique[21].

(21) Propositions de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale et de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (resp. COM (2018) 226 final et COM (2018) 225 final).

La difficulté à laquelle se heurtent les autorités judiciaires des États membres de

l'UE est double : d'une part, accéder à des données, de nature à servir de preuves, qui sont stockées sur des serveurs situés dans des pays tiers à l'Union ou qui sont détenus par des fournisseurs de services, essentiellement les GAFA ; d'autre part, rendre compatibles les preuves collectées par ces autorités des différents États membres. En effet, les obligations imposées à ces fournisseurs varient d'un pays à l'autre, posant la question de la recevabilité de ces preuves.

(22) Doc. du Conseil du 9 juin 2016, n° 10007/16.

Cette initiative de la Commission fait suite aux conclusions des ministres de la Justice du Conseil de juin 2016. Elle est destinée à faciliter la détermination, dans le cadre des enquêtes pénales, de la localisation des preuves numériques et de l'origine de ces cyberattaques[22]. Elle entend améliorer l'accès transfrontière aux preuves numériques : la proposition de règlement, complétée par le dispositif prévu par la directive, institue une injonction judiciaire. La directive vise à imposer aux opérateurs proposant leurs services dans l'Union européenne de désigner un représentant légal dans l'Union (pour la réception, le respect et l'exécution des décisions et injonctions émises par les autorités compétentes des États membres à des fins de collecte de preuves en matière pénale). Concrètement, cette injonction émise par une autorité judiciaire nationale permet de demander à un fournisseur (réseaux sociaux et fournisseurs de communications électroniques en particulier), qu'il se trouve dans l'Union ou non, de conserver des données ou de les transmettre, en vue de les produire à titre de preuve dans une procédure judiciaire, et ce, quelle que soit la localisation de ces données.

Fraude en ligne par carte bancaire et propagande terroriste en ligne

(23) COM (2017) 489 final.

Cette nouvelle législation sur les cyberpreuves (« e-evidence ») entend permettre au droit de s'adapter aux évolutions technologiques et à l'usage que fait la criminalité de celle-ci. Il en est de même pour la proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[23]. Une telle proposition, présentée le 13 septembre 2017, entend moderniser le droit existant, en l'occurrence la **décision-cadre du 28 mai 2001**. Il importe de noter à cet égard que la criminalité relative à la fraude aux cartes bancaires et de paiement sur internet s'était adaptée entretemps et que la mise à jour de ce texte était impérative. Parmi les nouveautés prévues figure la prise en compte de certains comportements délictueux comme l'hameçonnage (*phishing*) et le trafic d'authentifiants bancaires volés (*carding*). En outre, la proposition actuellement en cours de négociation par le Conseil et le Parlement européen harmonise les infractions relatives au piratage d'appareils

électroniques destinés à rediriger l'utilisateur vers de faux sites webs en vue de détourner le paiement réalisé vers un compte bancaire contrôlé par le fraudeur.

La volonté d'adapter la répression aux évolutions de la criminalité se traduit également par une meilleure coopération en matière de lutte contre la propagande terroriste sur internet. Europol constitue l'enceinte pertinente chargée de détecter ce type de contenu et de centraliser les signalements opérés par les États membres. À cet égard, un récent rapport, dressant un état de la sécurité à l'échelle de l'Union, note un accroissement du nombre de signalements à l'attention des entreprises du web, en particulier Twitter et Facebook[24]. Selon ce même texte, l'unité d'Europol chargée de les traiter, dénommée EU-IRU[25], a émis plus de 8 000 signalements lors du quatrième trimestre de 2017, qui ont abouti au retrait du contenu incriminé dans 89 % des cas (chiffre globalement stable depuis plusieurs années). Au cours du premier trimestre de 2018, ce chiffre s'élevait à 5 700 signalements.

(24) COM (2018) 470.

(25) Acronyme de EU Internet Referral Unit.

Les défis à venir de la lutte contre les contenus illicites

Toujours d'après ce texte, datant du 13 juin 2018, le taux de retrait par les entreprises de taille modeste est sensiblement plus faible (61 %) et l'un des défis actuels consiste à l'améliorer. Il en existe d'autres comme l'optimisation du retour d'information sur les signalements (par exemple la confirmation de prise de mesures), la mise en place de mécanismes de rechargement des pages supprimés (*reupload*) ainsi qu'une meilleure détection des contenus illicites par les entreprises du web elles-mêmes.

À ce stade, il n'est pas encore question de produire une législation contraignante élaborée au niveau l'UE. La Commission a présenté le 1er mars 2018 une recommandation précisant les obligations des hébergeurs[26]. Elle fait écho à une demande du Conseil européen, des 22 et 23 juin 2017, désireux d'empêcher la diffusion d'une propagande terroriste en ligne. La Commission a défini en particulier un mécanisme de collaboration entre les entreprises du web et les États membres, les uns et les autres devant désigner des points de contact chargés des questions concernant les contenus illicites en ligne. En outre, la recommandation préconise le recours par ces entreprises à la détection automatique de contenus. Enfin, elle envisage des procédures accélérées pour ce qui est de la propagande terroriste, ces contenus devant être supprimés en une heure à compter du signalement. En effet, la recommandation vise tout type de contenus illicites, au-delà de la propagande terroriste. Cela étant, l'action de l'Union est encore plus large en visant les contenus

(26) C (2018) 1177 final.

(27) Voir COM (2018) 236 final et JOIN 2018/16 final.

qui ne sont pas susceptibles, en tant que tels, de constituer une infraction pénale. Il s'agit du phénomène de la désinformation qui est appréhendé par l'Union dans le contexte de la gestion des menaces hybrides[27].

(28) COM (2018) 640 final.

Un projet de règlement relatif à *« la prévention de la diffusion en ligne de contenus à caractère terroriste »* a, quant à lui, été publié le 12 septembre 2018[28]. Cette proposition de la Commission marque le succès du travail d'influence que la France mène depuis un an avec ses partenaires européens, britanniques et allemands. Le projet de texte prévoit d'imposer le retrait, par tout opérateur ayant un lien avec l'Union européenne, d'un contenu terroriste dans l'heure, à la demande d'un État membre. Le texte prévoit par ailleurs une obligation générale de prévention par des mesures proactives, l'obligation de désigner un point de contact disponible 24h/24 (pas nécessairement situé sur le territoire de l'Union) et un représentant légal situé sur ce territoire, mais aussi des sanctions et enfin l'obligation de présenter un rapport de transparence annuel. La Commission a pour ambition de faire adopter ce règlement avant la fin de cette mandature.

(29) Voir George Hilary, « Nouvelles complexités, nouvelles menaces », Revue de la Gendarmerie nationale, n° 260, décembre 2017, p. 53-56.

En conclusion, deux remarques peuvent être formulées : la première a trait au fait qu'il existe une volonté politique forte de la part, tant des institutions européennes que des États membres de l'UE, de faire avancer ces divers chantiers. La seconde, dans le prolongement de la première, tient au fait qu'il s'agit d'un domaine à croissance rapide. L'action de l'Union se structure et se diversifie dans un laps de temps court. Il est intéressant de noter que les dispositions des traités (TUE et TFUE) sont interprétées de manière à ce qu'elles ne constituent pas un obstacle au déploiement d'une intervention de l'Union, régie par l'impératif de l'urgence et d'une réaction ferme à des menaces en constante évolution[29].

CONSEIL DE LECTURE

Taillat, S. et al., La cyberdéfense, Armand Colin, coll. U, 2018
https://www.armand-colin.com/la-cyberdefense-politique-de-lespace-numerique-9782200621292

L'AUTEUR

Docteur en droit, Pierre Berthelet est chercheur associé au CESICE (Université de Grenoble), au CERIC (Université Aix-Marseille) et auprès de la Gendarmerie nationale (CREOGN). Il est titulaire d'un doctorat de droit d'un postdoctorat en sécurité à l'Université Laval (Québec). Il est membre de l'Association française de droit de la sécurité et de la défense (AFDSD) et du comité de rédaction des Cahiers de la sécurité et de la justice. Il anime le blog : securiteinterieure.fr

© Adobe Stock

LUTTE CONTRE LES CYBERMENACES : UN BESOIN DE COORDINATION ET DE PARTENARIATS

Une feuille de route a été demandée par le ministre de l'Intérieur au Délégué aux industries de sécurité

et à la lutte contre les Cybermenaces (DMISC). Elle vise un plan de renforcement des actions de lutte contre les cybermenaces. Le développement des objets connectés et de nouvelles pratiques numériques augmentent la surface d'attaque des cybercriminels et en conséquence les phénomènes criminels se sont multipliés et diversifiés. Pour les circonscrire et les anticiper, on relève un besoin de centralisation et de coordination au niveau européen mais aussi national autour de véritables stratégies identifiées et structurantes. Il convient de favoriser l'élaboration de statistiques et de marqueurs fiables de ces phénomènes afin de les appréhender objectivement et enfin de rechercher l'implication de tous les acteurs institutionnels et privés de la chaîne.

Les enjeux économiques, sociétaux et juridiques sont tels qu'une politique volontariste doit être menée au niveau européen pour obtenir un niveau de résilience suffisant et une coopération fructueuse.

La gestion de la menace
cybercriminelle en France et en Europe

Questions à Thierry Delville

À l'occasion de son intervention au 10e Forum international de cybersécurité (FIC), M. Gérard Collomb, ministre d'État, ministre de l'Intérieur, a confié à M. Thierry Delville, délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), le soin d'élaborer des propositions visant à l'établissement d'une feuille de route cyber. Dans ce cadre, la délégation a procédé à une comparaison européenne et internationale de la gestion de la menace cybercriminelle, avec l'appui de la direction de la coopération internationale (DCI).

THIERRY DELVILLE

Consultant cybersécurité chez PwC.

Quel est l'état de la menace liée au numérique en France ?

La société française connaît aujourd'hui une phase de transformation numérique de grande ampleur et l'ensemble de nos systèmes sont de plus en plus interconnectés. Les attaques informatiques ne constituent plus un simple risque conjoncturel mais sont devenues systémiques. L'adaptation des moyens de lutte doit être permanente pour faire face à l'évolution des cybermenaces. L'implication de la chaîne des acteurs institutionnels et privés doit être recherchée et la société doit renforcer sa résilience. Les enjeux sont économiques, sociétaux et juridiques.

Les usages ont évolué. Ainsi, le taux de pénétration de l'Internet continue de progresser en France (87 %) et dans le Monde (54 %) ; il en est de même pour les réseaux sociaux. Depuis quelques années, le smartphone, qui s'impose comme plateforme multi-usages, est la cible de nombreux logiciels malveillants. L'évolution de l'usage des cryptomonnaies doit être suivie avec attention, car elles sont largement utilisées par les cybercriminels (anonymisation, minage clandestin, attaques de

L'évolution des acteurs et des formes de menaces cyber force les États à coordonner les réponses dans une perspective stratégique et à mobiliser des partenariats dépassant la sphère étatique.

plateforme d'échanges, levée de fonds ICO[1]…). Du fait de leur développement, les objets connectés et les espaces intelligents augmentent considérablement la surface d'attaque pour les cybercriminels. Enfin, de nouvelles pratiques telles que les *fake news*, *hoax* et *swatting*, se développent sur Internet.

(1) ICO - Initial Coin Offering, levées de fonds en monnaie virtuelle.

Les phénomènes criminels se sont également multipliés et diversifiés. Les rançongiciels sont devenus une menace majeure, comme les attaques ciblées (y compris le cyber-espionnage) ou les attaques visant les systèmes bancaires et de paiement (*jackpotting*…). Tout un écosystème facilitant la mise en œuvre d'attaques cyber par des groupes criminels s'est mis en place, induisant la notion de « crime-as-a-service ». La mise hors ligne des sites *AlphaBay* et *Hansa Market* à l'été 2017 a porté un coup d'arrêt à deux des plus grands sites de revente de produits illicites sur les *darknets*. La France est particulièrement touchée par le vol des données personnelles, qui reste l'objectif principal des intrusions dans les systèmes de traitement automatisé de données. Le phénomène de l'exploitation sexuelle des mineurs en ligne est toujours inquiétant. Des résultats encourageants sont cependant à saluer : les contenus de provocation et d'apologie du terrorisme signalés à la plate-forme

PHAROS ont connu une baisse significative pour la deuxième année consécutive et, en matière d'escroquerie, l'année 2017 a vu un net recul des faux ordres de virement internationaux (FOVI).

Le ministère de l'Intérieur s'est depuis longtemps mis en ordre de bataille pour faire face aux cybermenaces et s'adapte continuellement. Le délégué ministériel aux industries de sécurité et à la lutte contre les cyber menaces (DMISC) joue un rôle de pilotage stratégique en matière de lutte contre ce phénomène. Une feuille de route a été demandée par le ministre de l'Intérieur, visant un plan de renforcement des actions de lutte dans ce domaine, qu'il s'agisse de la prévention, du renseignement, des enquêtes, de la gestion de crise, de la gouvernance ou de l'innovation.

Un état complet et précis de la menace liée au numérique est consultable et téléchargeable sur le site internet de la documentation française[2].

(2) http://www.ladocumentationfrancaise.fr/rapports-publics/184000391/index.shtml
Ce rapport a été établi, de manière collaborative, par l'ensemble des services du ministère de l'Intérieur sous la direction de la DMISC.

Quel est l'état de la menace liée au numérique dans les autres pays de l'Union européenne ?

Tous les États constatent une augmentation exponentielle des menaces et des infractions cyber sur leur territoire. Tous notent le caractère hétérogène de la menace allant d'une agression très élaborée par un autre État sur des intérêts vitaux jusqu'aux escroqueries privées et aux rançongiciels, en passant par l'utilisation d'internet (sans grande compétence) à des fins de propagande terroriste et l'activisme politique de groupuscules plus ou moins virulents contre les symboles de l'État. L'Allemagne, en particulier, y ajoute la menace sévère de « désinformation » (*fake news*).

Seul le Royaume-Uni semble disposer pour l'heure de statistiques précises sur l'ampleur du phénomène puisque sont établis des états chiffrés des contenus prohibés découverts, des délais de traitement par les sites et les plateformes, du nombre et du suivi des plaintes déposées ainsi que des incidents et attaques de toutes natures par le vecteur cyber.

Les autres pays européens sont-ils plus avancés que la France dans la gestion de la menace cyber ? La stratégie française de lutte contre les cybermenaces est-elle différente de celle des autres pays européens ?

Pour des raisons diverses, certains États semblent à peine avoir commencé à appréhender la question ; d'autres n'ont pu finaliser un dispositif qui paraît éclaté et morcelé. Ainsi, l'étude de la stratégie nationale publiée en décembre 2017 souligne pour l'Espagne, dont les efforts embrassent pourtant l'ensemble de la menace cyber,

des difficultés rencontrées en matière d'action de coordination des services.

Il est à noter plusieurs similitudes entre la stratégie française et celle de nos voisins européens.

D'une part, on relève un réel besoin de centralisation et de coordination. En Italie, le NSC (*Cybersecurity Unit*) qui dépend de l'Information *Security Department* pilote ainsi toutes les unités concourant à la défense du pays, les CERT, le *Joint Cyber Commando* (Defense) et le CNAIPIC (Police). Au Royaume-Uni, le NCSC (*National Cyber Security Center*) est chargé de la gestion et de l'expertise des cyber incidents nationaux. Il est rattaché au GCHQ (*Government Communications Headquarters*) et coordonne toutes les forces répressives amenées à intervenir. En Allemagne, l'agence ZITIS a été créée en 2017 et compte aujourd'hui 60 personnes (objectif 400 en 2022). Sans compétence opérationnelle, elle offre un conseil et une expertise centralisés à tous les services de police sur l'ensemble des champs cyber : recherche numérique, surveillance des moyens de communication, cryptoanalyse, big data… Par ailleurs, le Centre National de Protection Cyber (niveau fédéral) réagit aux crises et implique les Länder dans des solutions communes. Aux Pays-Bas, le *National Cyber Security Centrum* (NCSC) coordonne toute l'activité contre les menaces cyber, sous l'autorité d'un coordonnateur national pour le cyber et l'antiterrorisme. Son activité est complétée par le *Cyber Security Council* qui regroupe des représentants de haut niveau d'entreprises privées, de la Police et de la Justice.

D'autre part, on observe l'élaboration et la mise en œuvre d'une véritable stratégie nationale identifiée et structurante. Le Royaume-Uni a ainsi publié son *« livre vert – Internet Safety Strategy »* ; cette stratégie interministérielle a été présentée, en octobre 2017, par le secrétaire d'État pour le numérique, les médias et la culture. La dernière version de la stratégie globale italienne et espagnole date de 2017.

Les Pays-Bas ont publié en juin 2017 leur stratégie globale, le CSAN (*Cyber Security Assessment Netherlands*), dont l'ambition est clairement orientée vers l'aide au secteur économique. Elle a été récemment actualisée.[3]

(3) https://translate.google.com/late?hl=fr&sl=en&u=https://www.ncsc.nl/english/current-topics/Cyber %2BSecurity %2BAssessment %2BNetherlands/cyber-security-assessment-netherlands-2018.html&prev=search

Qui sont les acteurs de la lutte contre les cybermenaces dans les autres pays européens ?

Les acteurs institutionnels, bien sûr, figurent en première ligne. On relève également un recours de plus en plus approfondi au partenariat public/privé pour faire bénéficier les États des compétences techniques les plus modernes. Ainsi, l'Italie pilote de nombreux partenariats public/privé dans ce domaine tandis que l'Allemagne annonce la mise

© EC3

Les organismes européens fournissent une expertise technique et juridique transverse qui permet de soutenir les procédures engagées par les forces de police des États européens.

en place d'une plateforme d'échanges d'informations entre l'État et les entreprises privées au sujet des cyber attaques. Au rang des priorités, les Pays-Bas ont créé un « *Digital Trust Center* » destiné à susciter des alliances public/privé pour dynamiser la création d'un écosystème national favorable à l'émergence de produits de sécurité. Les perspectives industrielles sont clairement affichées. Le Royaume-Uni investit directement dans la filière cyber sécurité et développe en plus un programme spécifique de protection cyber pour les entreprises privées travaillant dans le secteur de la défense (Defence Cyber Protection Partnership).

Par ailleurs, l'appui des chercheurs et du monde universitaire est de plus en plus sollicité. Ainsi l'Allemagne envisage la création rapide d'un Institut allemand pour la Cyber sécurité, destiné à faire progresser la sécurité globale en rassemblant des chercheurs et des universitaires, tandis que le Royaume-Uni a instauré une académie de la Cyberdéfense destinée à devenir un centre d'excellence très orienté vers la défense.

Enfin, certains États européens ont identifié des partenaires privilégiés. Par exemple, le Royaume-Uni s'est largement associé au FBI sur cette thématique.

Le soutien direct d'EUROPOL est également désormais systématiquement recherché par les États membres de l'Union européenne, au travers de l'European Cybercrime Centre (EC3) ou encore de l'**EU Internet Referal Unit** (unité de référencement sur les contenus terroristes).

Quelles sont les voies de progrès de la France et des autres pays européens en matière de lutte contre les cybermenaces ?

La plupart des pays consultés déplorent la faiblesse numérique des ressources humaines compétentes sur le sujet, ce manque étant perçu comme le véritable frein à l'élaboration d'un dispositif efficace.

Partout, la formation est un enjeu vital ; le Royaume-Uni et l'Allemagne la font figurer en priorité absolue et viennent de réformer toute l'offre de formation spécialisée.

La France n'est pas en reste et le ministère travaille à la consolidation de la gouvernance stratégique cyber. Une politique globale de lutte contre les cybermenaces permettrait en effet une meilleure coordination des différentes entités du ministère, mais aussi une visibilité accrue dans l'écosystème, notamment sur ses relations avec les partenaires institutionnels et privés, français et étrangers. La mesure de la cybercriminalité, la prévention ou encore la prospective et l'innovation sont autant de défis à relever au cours des prochaines années : autant de sujets sur lesquels les équipes du ministère de l'Intérieur sont et resteront mobilisées.

L'AUTEUR

Thierry Delville est diplômé de l'École Nationale Supérieure de Police (ENSP) de Lyon en 1994.
Après avoir été chef de Circonscription dans le Val d'Oise et en Seine-Saint-Denis jusqu'en 1998, il devient adjoint puis chef du bureau des systèmes d'information et des télécommunications à la direction centrale de la Sécurité Publique (DCSP).
En 2005, Thierry DELVILLE est chargé de créer le Service des Technologies de la Sécurité Intérieure (STSI) de la Police nationale. Il contribue à ce titre au pilotage des grands projets technologiques (réseau Acropol, modernisation des centres d'information et de commandement), à la mise en place de partenariats et à développer l'implication de la Police Nationale dans la Recherche en sécurité.
En 2009, il devient Directeur des services techniques et logistiques de la Préfecture de Police de Paris.
En 2014, Thierry DELVILLE devient Délégué ministériel aux industries de sécurité puis, par décret paru le 24 janvier 2017, voit ses attributions étendues avec la création de la délégation aux industries de sécurité et à la lutte contre les Cybermenaces (DMISC).

Couverture du dernier rapport sur l'état de la menace liée au numérique réalisé par la DMISC avec le concours des services opérationnels du ministère de l'Intérieur.

PENSER UNE DÉMARCHE PRÉVENTIVE DÈS LA PHASE DE CONCEPTION D'UN PROJET

Le droit au respect de la vie privée, propre à l'intimité et à l'épanouissement de l'être humain, et la protection des données personnelles peuvent être soumis au régime des risques liés à l'usage des technologies de l'information. Les traitements des données personnelles et la circulation de l'information doivent faire l'objet d'une analyse d'impact qui suppose en amont la sensibilisation de tous les acteurs aux prescriptions légales.

Cela implique une politique globale de gouvernance de mise en conformité dès la conception des systèmes techniques. Il faut obligatoirement satisfaire des obligations de licéité, de loyauté et de transparence. La certification qui en découle est le gage de l'instauration de la confiance propre à une relation sociale ou économique pérenne.

La notion
de Data Protection by Design

Par CLAIRE LEVALLOIS-BARTH

Data Protection by design, security by design, privacy by design, data protection by default… **Autant de notions et d'interrogations sur ce que recouvrent exactement ces concepts appliquant l'adage « Mieux vaut prévenir que guérir ». La notion de protection des données, dès la conception, entend agir en amont au niveau des travaux préparatoires de l'architecture des systèmes techniques. Elle a été intégrée en droit positif par le Règlement Général sur la Protection des Données (RGPD) [1].**

CLAIRE LEVALLOIS-BARTH

Maître de conférences en droit à Télécom ParisTech

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données): JOUE L119/1 du 4 mai 2016.

Une démarche globale

Le législateur européen s'inspire en cela de la démarche dite ***Privacy by design*** apparue à la fin des années 1990 sous l'impulsion d'Ann Cavoukian[2], la Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada). Cette approche part du constat que le cadre légal n'intervient qu'*a posteriori* pour corriger les abus. La Commissaire propose alors de traiter le problème à la source en intégrant le respect de la vie privée directement dans la conception et le fonctionnement des systèmes techniques, et ce, pendant toute la période d'utilisation des données personnelles jusqu'à leur obsolescence informationnelle. Cette forme de régulation *ex ante* consiste donc à agir en amont de l'utilisation abusive des données, en concevant des systèmes techniques qui,

(2) Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information and Privacy, Commissioner of Ontario, Canada, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

dans leur design même, sont capables soit de prévenir les abus potentiels, soit de rendre explicites leurs modalités de fonctionnement et d'orienter les choix des utilisateurs vers une meilleure protection.

En octobre 2010, ce concept est repris lors de la 32e Conférence internationale des Commissaires à la protection des données et de la vie privée[3]. Selon la résolution adoptée sur proposition d'Anne Cavoukian, *« la protection intégrée de la vie privée [constitue] un concept global pouvant s'appliquer à l'ensemble des activités d'une organisation de bout en bout, y compris à la technologie de l'information, aux pratiques administratives, aux procédés, à la conception matérielle et aux réseaux »*. Il s'agit, via des mesures préventives, de « faire de la protection [des données personnelles] le mode implicite de fonctionnement de toutes les organisations, tout en assurant une fonctionnalité intégrale ».

(3) 32e Conférence internationale des Commissaires à la protection des données et de la vie privée, Résolution sur la protection intégrée de la vie privée, du 27 au 29 oct. 2010, Jérusalem, Israël.

La résolution invite également les Commissaires à *« favoriser l'intégration des principes fondamentaux… dans des politiques et textes de loi sur la protection de la vie privée dans leur territoire de compétence »*. Cette invitation a été entendue des deux côtés de l'Atlantique : dès 2012, la Commission fédérale étasunienne pour le commerce (*Federal Trade Commission* – FTC) recommande que les entreprises adoptent une approche *Privacy by design*[4] tandis que le législateur européen l'intègre dans le droit positif en 2016.

(4) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Une reconnaissance législative européenne

Ainsi, l'article 25-1 du RGPD introduit l'obligation de ***Data protection by design***. Le responsable de traitement[5] de données personnelles doit implémenter au cœur même de chaque système d'information des mesures à la fois techniques et organisationnelles pour mettre effectivement en œuvre les principes-clés définis par le règlement *« compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques »*.

(5) Défini par l'article 4-7 du RGPD comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Pour sa part, l'article 25-2 du RGPD codifie le concept de protection des données par défaut (***Data protection by default***). Par défaut, l'entité doit garantir le plus haut niveau possible de protection des données personnelles, notamment ne traiter que les

données *« qui sont nécessaires au regard de chaque finalité spécifique du traitement » et s'assurer qu'elles « ne sont pas rendues accessibles à un nombre indéterminé de personnes sans l'intervention de la personne physique concernée »*. L'objectif est ainsi d'éviter une exploitation abusive par le responsable de traitement ou des tiers, ainsi qu'une réutilisation à d'autres fins que celles pour lesquelles les données ont été collectées.

Dans le même temps, le législateur prévoit qu'une violation des principes de protection des données dès la conception et par défaut peut faire l'objet d'une amende administrative pouvant s'élever jusqu'à 10 000 000 euros ou, dans le cas d'une entreprise, jusqu'à 2 % de son chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu[6].

(6) Dans ce sens, voir le Groupe de travail Article 29, Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement UE 2016/679 du 3 oct. 2017.

L'article 25 du RGPD retient donc la notion de *« data protection by design »*. Les juristes distinguent en effet deux droits fondamentaux, le droit au respect de la vie privée et le droit à la protection des données personnelles, respectivement reconnus par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[7]. La distinction se retrouve également en droit constitutionnel.

(7) Charte des droits fondamentaux de l'Union européenne : (2000/C 364/01) : JOCE C 264/1 du 18 déc. 2000, http://www.europarl.europa.eu/charter/pdf/text_fr.pdf.

De plus en plus d'États membres de l'Union européenne modifient en effet leur Constitution pour reconnaître un droit à la protection des données personnelles autonome à côté du classique droit au respect de la vie privée.

© Personal data protection concept Par Jakub Jirsák

Respect de la vie privée et protection des données personnelles forment deux droits fondamentaux qui ne peuvent être emportés par des considérations commerciales, politiques ou de simple facilité technique.

Plus ancien, **le droit au respect de la vie privée** est notamment consacré par l'article 12 de la Déclaration universelle des droits de l'Homme de 1948 et l'article 8 de la Convention européenne des droits de l'Homme de 1950. De façon générale, il correspond à « tout ce qui n'est pas la vie publique de l'individu » pour reprendre les propos de Robert Badinter[8], c'est-à-dire le droit de ne pas voir révélées des informations liées à son intimité (sphère physique mais aussi expression d'une relation avec autrui) et à

(8) In « Le droit au respect de la vie privée », JCP 68, doctrine 2136, avant de poursuivre « Cette définition négative a le mérite de mettre l'accent sur la primauté de la vie privée, celle-ci, interdite à toute intrusion indiscrète, étant pour chacun le sort commun, le reste, c'est-à-dire la vie publique, ouverte à la curiosité de tous, étant l'exception ».

son identité pour permettre à la personne de s'épanouir. Ce droit fondamental entend protéger l'opacité de l'individu.

Le droit à la protection des données personnelles correspond à un droit essentiellement préventif en protégeant l'individu par rapport à un risque lié à l'usage des technologies de l'information. Ce droit entend encadrer la collecte, l'utilisation et la transmission des données personnelles. Cet objectif est atteint, d'une part, par la limitation du traitement des données personnelles effectué par le responsable de traitement et, d'autre part, en permettant à la personne de maîtriser la circulation de son image informationnelle.

Différent mais complémentaire du droit au respect de la vie privée, le droit à la protection des données personnelles contribue également à préserver d'autres droits et libertés comme la liberté d'expression et d'information, la liberté de pensée, de conscience et de religion, la liberté de réunion et d'association et la liberté d'entreprise. Il participe surtout à la lutte contre la discrimination.

Encore convient-il qu'il soit implémenté concrètement dans les systèmes techniques.

L'inscription dans les systèmes techniques

Afin de déterminer les mesures appropriées, le respect de l'obligation de protection des données dès la conception implique en amont de mener une analyse d'impact des opérations de traitement envisagées sur les données personnelles.

(9) Groupe de travail Article 29, Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, adoptées le 29 nov. 2017, WP260 rev.01, version révisée et adoptée le 11 avril 2018, point 60, https://www.cnil.fr/sites/default/files/atoms/files/wp260_guidelines-transparence-fr.pdf.

Selon une approche au cas par cas, le fabricant d'un objet (montre connectée, voiture), le prestataire de services (assureur, banque) et le producteur d'applications ou de logiciels (Apple, Google, Microsoft) peuvent être conduits à anonymiser, pseudonymiser ou chiffrer les données personnelles, à réduire leur nombre ou dégrader la précision d'une donnée (géolocalisation à un kilomètre près au lieu de quelques mètres). Leur analyse doit également porter sur les mécanismes de transparence à mettre en œuvre *« afin que toutes les sources de données personnelles reçues par une entreprise puissent être suivies et retracées jusqu'à leur source à tout moment pendant le cycle de vie du traitement des données »*[9]. Cette analyse inclut préalablement à tout traitement la sensibilisation des salariés de ces acteurs aux prescriptions légales ainsi que l'instauration de procédures. Pour

(10) Voir Chaire Valeurs et Politiques des Information Personnelles, Signes de confiance – l'impact des labels sur la gestion des données personnelles, coordonné par Claire Levallois-Barth, janvier 2018, https://cvpip.wp.imt.fr/2018/03/19/2018-01-signes-de-confiance-limpact-des-labels-sur-la-gestion-des-donnees-personnelles/.

l'essentiel, ces dernières doivent permettre de s'assurer que toutes les directions (métier, juridique, systèmes d'information, des risques…) implémentent le RGPD et que l'analyse est revue régulièrement. Les connaissances techniques comme le traitement évoluant (ajout d'une nouvelle fonctionnalité, modification d'un logiciel), une politique globale de gouvernance doit être mise en place, pour inclure par exemple une validation externe de la conformité sous la forme d'un audit ou d'une certification[10].

Autant de mesures destinées à inscrire au cœur des systèmes techniques les principes-clés de protection des données personnelles, notamment le principe de sécurité. En ce sens, il existe un lien entre les concepts de *Security by design* et de *Data Protection by design*. Les deux notions cependant ne se confondent pas : la seconde vise à intégrer par construction les obligations de licéité, loyauté, transparence, limitation des finalités, minimisation et exactitude des données, pour n'en citer que quelques-uns.

(11) Lawrence Lessig, Code is Law: On Liberty in Cyberspace, Harvard Magazine, January-Februay, 2000, https://www.harvardmagazine.com/2000/01/code-is-law-html.

Dans son célèbre article de 2000 intitulé « Le code fait loi – De la liberté dans le cyberespace »[11], Laurence Lessing constatait que le cyberespace possédait sa propre régulation, le code ou architecture du réseau, qui constituait une menace pour nos libertés individuelles. L'auteur expliquait alors : *« S'il n'existe aucune incitation à protéger la vie privée – si la demande n'existe pas sur le marché, et que la loi est muette – alors le code ne le fera pas »*[12].

(12) "If protecting privacy is not an incentive--if the market has not sufficiently demanded it and if law has not, either--then this code will not provide it".

En imposant à l'architecture de protéger nos données personnelles dès la conception, l'Union européenne cherche à s'assurer que les codeurs intègrent les valeurs qui constituent le fondement même de notre démocratie. Reste aux entreprises et aux États l'obligation d'implémenter concrètement les principes-clés définis par le RGPD et, si besoin, aux autorités de protection des données de sanctionner les mauvais élèves volontaires.

L'AUTEUR

Claire Levallois-Barth est Coordinatrice de la Chaire Valeurs et politiques des informations personnelles créées par l'Institut Mines-Télécom en 2013 et Maître de conférences en droit à Télécom ParisTech. Elle a coordonné l'ouvrage « Signes de confiance : l'impact des labels sur la gestion des données personnelles » paru en janvier 2018. Claire Levallois-Barth est éditrice associé des Annals of Telecommunications, membre du Data Privacy Expert Panel d'AXA et membre du comité scientifique du Forum International de la Cybersécurité (FIC).

DOSSIER

Sécurité SI et données personnelles

Parallèle entre règles
d'hygiène de santé et protection des systèmes d'information

Par Philippe Loudenot

« Les hommes n'acceptent le changement que dans la nécessité et ne voient la nécessité que dans la crise ». Cette maxime d'un des pères de la construction européenne, Jean Monnet, se mesure tous les jours sur différents sujets. En matière numérique, les différents incidents révélés, qui émaillent depuis ces dernières années les médias, démontrent régulièrement que la cyber sécurité n'est finalement prise en compte qu'à l'issue d'une crise qui peut malheureusement être majeure, pouvant contribuer à la disparition d'un organisme. Les risques liés au numérique sont passés en quelques années du fait de son essor, du développement des objets connectés et de nouvelles méthodes de travail, d'une dimension quasi anecdotique à une menace multiple, structurée et organisée. Ils peuvent provoquer des dégâts techniques, d'image de marque, juridiques et financiers considérables, pouvant mettre potentiellement en jeu la vie de personnes. Présenté comme cela, c'est très inquiétant. Mais, au-delà de faire peur, il est beaucoup plus important de sensibiliser, de faire prendre conscience un organisme de la menace des impacts potentiels et ainsi de pouvoir rebondir. Le point positif, c'est que l'on sait comment faire, mais encore faut-il le faire…

PHILIPPE LOUDENOT

Fonctionnaire de la sécurité des systèmes d'information (FSSI)
Ministère des Affaires sociales, de la Santé et des Droits des femmes

Il est possible de comparer le numérique au monde de la santé : il est à noter que de nombreux termes ou concepts lui sont empruntés. Mais en matière de sécurité, à l'instar de la santé, les problèmes ne sont encore trop souvent vus que dans l'urgence et le curatif. Pour preuve, en médecine, on admire bien plus un chirurgien capable d'un

exploit médiatique qu'un Ignace Philippe Semmelweis, médecin obstétricien hongrois, qui œuvra pour l'hygiène. Il démontra l'utilité du lavage des mains, après la dissection d'un cadavre, avant d'effectuer un accouchement. Ses travaux, permettant de faire du préventif, ont malheureusement mis quelques années avant d'être adoptés. En médecine, son cas est régulièrement cité en exemple d'une situation où le progrès a été freiné par une inertie bien en place. En matière de sécurité numérique, l'hygiène doit être de mise.

Au-delà de l'hygiène, il peut être fait une comparaison hasardeuse concernant la prophylaxie. En médecine, une prophylaxie désigne un processus actif ou passif ayant pour but de prévenir l'apparition, la propagation ou l'aggravation d'une maladie. Elle est au centre des campagnes de **prévention**, selon le principe qu'il « vaut mieux prévenir que guérir ». Cela vaut pour un patient comme pour la société. En matière de prophylaxie, il est distingué 4 stades de prévention. Les mesures de prévention qui y sont associées reposent sur tout un ensemble d'outils, depuis l'information et l'hygiène jusqu'à la remédiation, en passant par l'immunisation, le **dépistage** précoce et la quarantaine pour aboutir éventuellement à un ensemble de mesures palliatives ou d'abandon si le rapport bénéfices/investissements est en trop grand déséquilibre. À ce titre, les campagnes de mise à jour systématique — patchs, signatures anti-malware, etc. — la déclaration des incidents (ANSSI, ACSS Santé, cybermalveillance…), ainsi que les démarches de prévention diverses d'hygiène SSI, le dépistage précoce de certaines exploitations, vulnérabilités — nouveau malware, par exemple — sont autant d'entreprises prophylactiques.

Si l'on reporte les 4 stades de prévention au numérique, cela pourrait donner :

• **une prévention primaire** par la mise en œuvre de moyens devant permettre de garantir :
  – la sensibilisation, la formation, la mise en place de bonnes pratiques (ex : rédaction de guides, recommandations) ;
  – le fonctionnement nominal des systèmes et d'empêcher l'apparition de l'exploitation de vulnérabilités sur les SI ;
  – la protection des données de l'entreprise et son patrimoine immatériel ;
  – la sécurisation de la relation avec les tiers (autres entreprises-administrations, fournisseurs, sous-traitants) ;
  – la sécurisation de la relation avec les bénéficiaires (citoyens, patients, clients).

Dans le cadre de la prévention primaire, le RSSI doit être force de proposition de produits connectés et/ou services connectés sécurisés ; nous sommes bien sur une phase de « *Security by design* ».

• **La prévention secondaire** vise à réduire la gravité de l'exploitation de vulnérabilités, notamment par la détection (dépistage), la prise en charge (mise en place de mesures organisationnelles et techniques), la remédiation et l'alerte.

(1) Plan de Reprise/ Continuité d'Activité (PRA-PCA). Un plan de reprise d'activité (PRA) est une procédure qui permet d'assurer la reprise des activités, en mode dégradé ou à plein régime en cas de sinistre (inondation, coupure électrique, incendie, destruction de données vitales…). Un Plan de Continuité d'Activité (PCA) est une procédure qui permet d'assurer la continuité des activités, sans perte de données et qui offrira un accès au SI sans rupture d'exploitation.

• **La prévention tertiaire** concerne l'évitement des complications d'attaques déjà manifestes et la mise en place de procédures de remédiation (PCA/PRA[1] ; Forensic…).

• **La prévention quaternaire** : en matière numérique ce stade va reposer sur un retour à des procédures fortement dégradées. L'investissement technique peut s'avérer peu approprié, trop coûteux au regard des systèmes d'information impactés.

Pour rester dans le domaine de la santé, mais cela est valable pour la quasi-totalité des secteurs d'activités, l'avènement du « tsunami digital » est un fait constaté tous les jours. Source de progrès et d'augmentation de chances pour les patients (et nous en sommes tous, avérés ou en devenir), il est désormais impossible d'éviter le débat sur les dépendances aux technologies numériques. Le numérique se trouve partout et même là où il n'était pas attendu :

– Systèmes hospitaliers d'information,
– Dispositifs biomédicaux,
– Systèmes centralisés de gestion technique ou de bâtiment,
– Objets connectés.

Types de prévention			Côté Cybersécurité Attaque / incident majeur Absence	Présence
Côté Organisme / Entreprise	Attaque / Incident majeur	Absence	Prévention primaire (pas d'attaque, pas d'incident, fonctionnement nominal des SI) Ensemble des mesures pour protéger les SI - Étude risques - Bonnes pratiques, règles d'hygiène - Elaboration PCA/PRA - Sensibilisation / formation - Threat intelligence	Prévention secondaire (attaque ou exploitation de vulnérabilité) Déceler, à un stade précoce, des maladies qui n'ont pas pu être évitées par la prévention primaire. - Détection - Remédiation / Patching - Alerte
		Présence	Prévention quaternaire (peu ou aucune mesures SSI) Avec l'ancienneté de certains SI, il n'est pas nécessairement opportun de faire de l'acharnement SSI ; les vulnérabilités augmentent et le rapport bénéfice/coût d'une remédiation peut entraîner l'abandon de tel ou tel SI. - mise en œuvre de procédures dégradées pour sauver ce qui peut l'être. - envisager tout ou partie des SI que l'on peut (doit) sacrifier - envisager de passer en mode manuel	Prévention tertiaire (attaque en cours) Ensemble des moyens mis en œuvre pour éviter la survenue de complications et de nouvelles exploitations des vulnérabilités - Isolation - PCA/PRS en œuvre - Remédiation

Tableau des 4 types de prévention prophylactiques

Ces différentes composantes sont aujourd'hui, peu ou prou, interconnectées, de plus en plus ouvertes. Avec leur propre historique et une architecture particulière à chacune d'entre elles, elles posent la problématique de la maîtrise des processus, des informations qui y circulent et de la prise en compte de la sécurité numérique.

L'évolution des traitements de l'information, la mise en place de convergences technologiques : ordinateurs, réseaux, protocoles d'échanges, appareils biomédicaux, font des systèmes d'information numériques autant de cibles ; des incidents et des attaques sont régulièrement déclarés[2]. Ces dernières sont lancées non seulement par des individus ou des groupes d'individus, guidés par l'appât du gain mais peuvent être aussi menées par des États ou de grandes organisations pour déstabiliser un pays. Par chance, aucun incident d'ampleur équivalente à ce qui est arrivé en 2017 en Angleterre - avec l'arrêt d'activités pendant plusieurs jours d'établissements de santé et l'évacuation d'une partie de leurs patients - n'est arrivé chez nous. Mais, légitimement nous pouvons nous poser la question : encore combien de temps ?

(2) Depuis le premier octobre 2017, Le secteur de la santé fait l'objet d'une obligation, inscrite dans le code de la santé, aux établissements de santé, organismes et services exerçant des activités de prévention, de diagnostic ou de soins, de signalement des incidents de sécurité des systèmes d'information (Art L. 1111-8-2 CSP)

Au-delà de ce focus « santé », à l'heure de l'interconnexion globale des réseaux de communication, de la convergence numérique et de l'accroissement exponentiel de la puissance des moyens utilisés dans les technologies de l'information, chacun est confronté à des changements rapides, porteurs de nouvelles opportunités, mais également à de nouveaux risques qu'il est de plus en plus difficile de percevoir. Dans un monde numérique banalisé et en constante évolution, la sécurité de l'information reste un concept difficilement assimilé et accepté par tous. Comme nous l'avions déjà indiqué : le point positif, c'est que l'on sait comment faire, mais encore faut-il le faire…

Les enjeux de la sécurité des systèmes informatiques représentent un défi majeur dans des environnements et des technologies qui changent constamment. Il est donc impératif de bien comprendre que la cybersécurité n'est pas qu'une question technique ou qu'un sujet d'organisation et/ou de communication. Cela nécessite un réel changement de vision.

Quel que soit le secteur d'activité, il est essentiel de mettre en place une véritable gouvernance de la sécurité adaptée à la culture de l'organisation et capable de fédérer l'ensemble des actions. La sécurité ne peut pas être considérée comme une pratique à part : elle doit s'intégrer dans la stratégie de l'organisation.

La gestion des risques liés aux SI, la sécurité des SI et la confiance numérique sont étroitement liées. La première est une démarche pour appréhender les risques auxquels l'organisation est exposée via ses systèmes d'information numériques, la deuxième se rapproche des moyens mis en œuvre pour défendre le patrimoine informationnel de l'organisation, tandis que la dernière correspond à une démarche qui doit permettre à l'organisation de tirer parti de la chaîne de valeur liée aux dispositifs mis en place pour assurer la confiance. Aujourd'hui cela est encore trop vite instrumentalisé, considérant que ce n'est qu'un problème technique. La cyber sécurité doit être au cœur de la stratégie des entreprises.

Le responsable de la sécurité des systèmes d'information (RSSI) doit bénéficier d'une marge de manœuvre qui dépend essentiellement de son positionnement hiérarchique. Un organisme tirera avantage de rapprocher le RSSI du pouvoir décisionnel, voire d'organiser son rattachement à la direction. Cela implique des décisions stratégiques, qui relèvent bien de l'autorité de la direction. Le RSSI quant à lui doit renforcer la culture de la sécurité avec l'ensemble des responsables des directions fonctionnelles, techniques, et les parties prenantes de l'organisation (Utilisateurs clés, décideurs, directions « métier », direction informatique, maîtrise d'ouvrage, maîtrise d'œuvre, etc.).

Le rapprochement du RSSI de la direction est notamment rappelé dans la revue stratégique de cyberdéfense, présentée par le secrétariat général de la défense et de la sécurité nationale (SGDSN) au mois de février 2018 : *« Le niveau de risque portant sur les systèmes d'information… doit à tout moment être connu et accepté par la direction de l'entité. Pour l'assister dans ce suivi, elle peut nommer un RSSI… Il est primordial que cette chaîne fonctionnelle de sécurité des systèmes d'information ne soit pas soumise à l'autorité hiérarchique de la direction des systèmes d'information de l'entité ».*

Mettre en œuvre une gouvernance SSI de façon performante et peu coûteuse, c'est possible ! Cela permet en outre de réellement commencer à faire du préventif et non du curatif, de limiter les surcoûts directs ou indirects – et de très loin supérieurs – induits obligatoirement par tout incident ou piratage d'un système d'information. La meilleure façon de se protéger consiste à adopter un processus de gestion des risques dans une démarche d'amélioration continue, en prenant en considération les vrais besoins en matière de sécurité. Cette approche reste bien la mieux adaptée aux besoins réels, la plus efficace et la moins chère. Une telle mise en œuvre permet de faire de la cybersécurité une véritable source de création de valeur et ne plus être identifiée comme une contrainte légitime mais pesante. Elle a pour objectif de satisfaire les exigences

d'une direction. Elle permet d'expliquer, quel que soit le type d'organisation, à l'ensemble des acteurs, autour d'un minimum d'échanges, les risques concernant les systèmes numériques, les enjeux de la cybersécurité, de concilier les visions, d'harmoniser les actions, d'évaluer et contrôler ces dernières. Elle est le prérequis permettant d'assurer une sécurité efficiente des systèmes d'information. Si cela est mis en œuvre, si l'intégration de la sécurité est intégrée dès les phases de réflexion et à haut niveau pour conduire leur transformation numérique, les directions d'entreprise et d'organismes s'apercevront rapidement que la sécurité, loin d'être un centre de coût, peut être un véritable levier de performance.

L'AUTEUR

Après une carrière au sein du ministère de la Défense à différents postes, Philippe LOUDENOT devient responsable national de la sécurité des systèmes d'information du service de santé des armées. Il devient ensuite, FSSI-adjoint dans le service du Haut fonctionnaire de défense et de sécurité pour les ministères chargés des affaires sociales. Il rejoint les services du Premier ministre en 2011. Il participe à la création et à la mise en place du service du Haut fonctionnaire de défense et de sécurité. Il en est nommé fonctionnaire de sécurité des systèmes d'information et conseille les autorités des services du Premier ministre, juridictions autorités administratives indépendantes en matière de cybersécurité. Il rejoint à nouveau le service du Haut fonctionnaire de défense et de sécurité des ministères chargés des affaires sociales comme FSSI.
Chargé de cours SSI au profit de différentes universités et écoles d'Ingénieurs, Philippe LOUDENOT est également présent dans la vie associative des experts en Sécurité du Système d'Information : il est administrateur du CESIN, membre du club EBIOS et de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information.

Le poste de travail Linux
en gendarmerie, pilier de la sécurité en profondeur du système d'information

Par Sébastien Hamel

Au début des années 2000, le système d'information de la gendarmerie nationale était composé de solutions propriétaires organisées en silos « métiers » qui communiquaient difficilement entre elles. L'extension de l'Intranet à 100 000 gendarmes ne pouvait être assumée financièrement qu'en adoptant une stratégie centralisatrice de réduction des technologies, basée sur le respect des normes et standards, dans une logique d'urbanisation. Respectueuse de la sécurité, une innovation selon des technologies et des coûts maîtrisés a ainsi accompagné l'évolution du système d'information pour nos gendarmes. Représentant plus de 90 % du parc informatique, les 75 000 postes « Linux », déployés dès 2014, pour accéder aux applications, concrétisent l'aboutissement de cette stratégie.

SÉBASTIEN HAMEL

Lieutenant-Colonel de Gendarmerie
Chef de bureau
Chargé de projets informatiques
Direction générale de la gendarmerie nationale

Un environnement complexe qui conduit à une centralisation poussée

Si le maillage territorial de la gendarmerie (4 300 sites géographiques en métropole et outremer) facilite la proximité avec nos concitoyens, il représente un défi technologique complexe pour garantir le fonctionnement des applications sur les postes informatiques répartis au sein d'un réseau, reliant des petites brigades en milieu rural comme des états-majors régionaux, au travers de liens à débits limités. Cela a conduit à privilégier la centralisation des compétences et des applications, poussant à l'extrême l'automatisation, pour garantir l'état de l'art technologique de l'intégralité du système d'information et renforcer sa sécurité. Chaque composant technique est conçu pour être interopérable et peut être remplacé pour des raisons technologiques ou financières.

Le poste Linux, rouleau compresseur de l'urbanisation du SI

Porte d'entrée du système d'information, le poste Linux, sous distribution « Ubuntu », obéit parfaitement à ce modèle de conception modulaire et maîtrisé en central. Conçu et maintenu par deux techniciens, il est banalisé et permet aux personnels d'accéder depuis n'importe quelle unité de gendarmerie aux applications métiers autorisées. L'importante présence territoriale de la gendarmerie, qui engendre certes un risque de sécurité accru en multipliant les points d'accès, représente in fine un véritable atout pour la résilience. En cas de perte de matériels, voire d'une brigade, un mode de fonctionnement dégradé efficace consiste en un simple déplacement des personnels dans l'unité la plus proche pour garantir la continuité d'activité sans impact majeur. Composé d'éléments simples au regard de la stratégie d'emploi quasi systématique des technologies et applications Web : un antivirus, un navigateur, une bureautique complète (couplée au logiciel de rédaction des procédures), un client de messagerie et divers utilitaires, il est parfaitement maîtrisé puis mis à jour des évolutions technologiques et de sécurité pour assurer la cohérence et la sécurité du système d'information afin de réduire le risque dû à sa dispersion.

Dès lors, il appartient aux applications de prendre en compte une configuration unique du poste informatique et non l'inverse, de manière à éviter les incompatibilités de configurations multiples des postes reposant sur des logiciels dépréciés vulnérables. Chaque évolution s'inscrit dans un processus de qualification par les chefs de projets techniques qui, à partir de machines de référence virtualisées, provisionnées à la demande, s'assurent de l'absence de régression fonctionnelle avant tout déploiement. Le cas échéant, ils procèdent aux modifications.

Le poste informatique représente la brique technique incontournable du socle, associée aux systèmes centraux d'authentification, de gestion des accès, d'échanges de données, d'exploitation des traces, qui guide et contraint les applications dans leurs choix technologiques.

L'aboutissement d'une politique orientée « logiciel libre »

Pour respecter les principes fondateurs, le choix des logiciels libres, qui garantissent mieux le respect des standards en permettant la modification du code, s'est imposé. Les chefs de projets ont été accompagnés dans cet objectif de cohérence globale du système d'information par l'échelon central avec la mise à disposition d'un cadre de cohérence technique et d'un règlement des développements qui recensent les technologies validées et décrivent la façon de les intégrer.

Pour réduire les adhérences logicielles sur le poste informatique, un inventaire des développements locaux a permis de remplacer

certains logiciels et d'intégrer des besoins majeurs au sein des projets centraux, dans le but de respecter la politique logicielle de l'institution. Les échelons locaux s'inscrivent désormais dans un processus de demande de validation des logiciels et chacun doit demander l'autorisation d'utiliser une application. Un premier filtre est réalisé par le support informatique local qui procède d'initiative à l'installation du logiciel ou saisit l'échelon central pour prise de décision. Le cas échéant, une alternative est proposée. L'inventaire des applications autorisées est disponible dans une application de demande et suivi des logiciels « ADSL ».

L'utilisateur étant familier des logiciels du poste informatique, le remplacement du système d'exploitation propriétaire s'impose naturellement dès 2008 avec le choix de Linux « Ubuntu » qui met à disposition tous les 2 ans une version « LTS » intégrant un support évolutif et correctif sur 5 ans, gage de stabilité. Le gain du remplacement des logiciels est estimé à plus de 10 M€ par an en droits d'usage et maintenance.

Un poste informatique Linux performant a d'abord été déployé pour le chargé d'accueil dans toutes les brigades de gendarmerie, apportant le service de partage des fichiers et acculturant les personnels avec une conduite du changement réalisée par les services SIC décentralisés et centraux, associant le centre national d'assistance aux utilisateurs. Un facteur clé de succès pour accompagner chaque évolution du poste Linux consiste également à fournir une plus-value (arrivée du e-learning, accès Internet via Firefox, fonctionnalités étendues, matériels plus performants, formation à la bureautique « OpenOffice »).

Le remplacement de « Windows » par « Ubuntu » s'est ensuite accéléré pour atteindre 72 500 postes en 2014. Cette évolution se poursuit en 2019 où le parc « Windows » sera réduit à 7 000 machines.

Maîtrise du parc et automatisation des mises à jour

Les mises à jour du système d'exploitation et logiciels sont déployées en quelques jours en central sur le parc informatique de manière automatisée, après les phases de conception et de qualification décrites supra. Les correctifs de sécurité sont déployés sans préavis.

Pour limiter le risque de saturation des réseaux, une architecture de redistribution supervisée sur 4 300 sites permet de déployer massivement sur tout le parc Linux en quelques heures via l'outil système « APT » à coût maîtrisé. Une forte expertise technique, un outillage adapté et une réelle capacité de décision, associant commandement, architectes, chefs de projets applicatifs et techniciens décentralisés, permettent de réagir rapidement pour résoudre tout dysfonctionnement dû aux déploiements : prouesse technique nécessaire pour déployer un correctif fonctionnel ou de sécurité en urgence.

Une représentation cartographique accessible par la chaîne SIC permet aussi aux équipes informatiques de vérifier l'état du parc et de pointer d'éventuels dysfonctionnements qui, s'ils ne sont pas documentés dans le wiki technique interne, sont remontés en central pour analyse et résolution.

Qualité et unicité des données d'authentification / contrôle des accès

Les « ressources humaines » et « l'organisation » sont propriétaires et responsables de la qualité des données de référence, répliquées chaque nuit automatiquement dans les bases centrales d'authentification et de contrôle d'accès, pour que les utilisateurs qui se connectent depuis un poste banalisé disposent chaque jour des droits conformes au strict besoin d'en connaître. Certains sont prévus légalement, en fonction de leur unité d'affectation, de leur qualité hiérarchique et judiciaire. L'authentification forte (carte à puce et code personnel) répond également aux exigences de sécurité pour contrôler les accès aux postes et applications les plus sensibles, et être en mesure de pouvoir les imputer. Conservées légalement, les traces de connexion sont exploitables par l'inspection générale dans un cadre judiciaire ou de contrôle hiérarchique.

Actualité et perspectives

La gendarmerie a initié la mise en conformité des applications Web respectant ainsi l'obligation légale de rendre accessible le système d'information (référentiel général d'accessibilité des administrations). Depuis quelques semaines, le poste Linux est rendu accessible aux personnels en situation de handicap visuel avec retour vocal, zoom par loupe, curseur cible, couleurs inversées.

Pour réduire les risques de sécurité, un antivirus centralisant les alertes, déployé en 2018, permet de déceler les comportements anormaux et de réagir. Des actions de sécurisation ont également été réalisées avec l'appui des experts de l'agence nationale de sécurité des systèmes d'information et l'homologation de sécurité du poste Linux s'inscrit désormais dans un cycle d'amélioration continue. La remontée des actions réalisées sur le poste informatique par chaque utilisateur devrait encore renforcer la sécurité en 2019.

Enfin, la transformation numérique de la gendarmerie nationale, qui donne aux gendarmes d'unité opérationnelle une vraie capacité d'action en mobilité permettant de renforcer le contact avec la population et évitant aussi d'inutiles déplacements, fait évoluer le modèle du poste de travail avec le déploiement de 70 000 smartphones individuels et le déploiement de nouvelles applications mobiles. Dans le respect des principes fondateurs, ce virage stratégique et technologique donne aujourd'hui les moyens de repenser l'exécution du métier sur le terrain pour s'ancrer dans la modernité.

Threat Intelligence,
le renseignement sur les menaces au service de la cybersécurité en entreprise

Par Barbara Louis-Sidney

NDLR: La notion de renseignement évoquée dans cet article comprend une sémantique propre au monde l'entreprise et à son environnement cyber. Elle doit être distinguée du renseignement criminel et administratif qui met en œuvre des concepts et des méthodologies spécifiques et usant d'une terminologie différente.

La *threat intelligence* peut se définir comme un processus visant à fournir du renseignement actionnable et contextualisé sur les cybermenaces et les groupes d'attaquants informatiques ciblant une organisation. Il s'agit d'un véritable outil d'aide à la prise de décision (stratégique) et à l'action (opérationnelle) pour améliorer son niveau de cybersécurité. La *threat intelligence* (TI) reste toutefois en proie aux buzz words et aux abus de langage générés par les approximations de vendeurs de cybersécurité. Le renseignement sur les menaces est en réalité une matière à démystifier.

BARBARA LOUIS-SIDNEY

Analyste en *threat intelligence*
Société SEKOIA

Les produits estampillés « TI » proposent souvent un contenu décorrélé de la réalité de l'entreprise, de ses besoins et de ses enjeux. Il s'agit parfois d'une veille de luxe, où de nombreuses données sont collectées en sources ouvertes, sans mise en perspective. Il peut s'agir d'analyses de tendances généralistes qui, bien que stimulantes intellectuellement, n'apportent rien aux challenges quotidiens du RSSI. Les « *feeds* » ou flux d'indicateurs de compromission sont souvent bruts et non contextualisés. S'ils constituent un matériau prêt à consommer, ils sont régulièrement fournis en vrac et sans priorisation. Les alertes qui en sont issues sont alors trop nombreuses et de piètre qualité (problématique des faux-positifs).

Élitiste, inutilisable ou dépourvue de contexte, la *threat* intelligence pêche encore à convaincre certains de son utilité au quoti-

dien. Il s'agit là d'une mauvaise application de la matière. Le renseignement sur les menaces est essentiel à l'entreprise qui souhaite prendre les devants sur celles qui l'entourent. Les produits dits de « TI » doivent être accessibles, sur-mesure, et donc utiles à leur destinataire, dans une véritable logique de « renseignement ».

De la donnée au renseignement

L'objectif du renseignement sur les menaces est de convertir les efforts de collecte d'information et d'analyse de l'équipe interne dédiée ou du prestataire de threat intelligence en recommandations concrètes et personnalisées, afin d'améliorer la compréhension de la menace, la détection des incidents et, plus globalement, l'état de cybersécurité du client final.

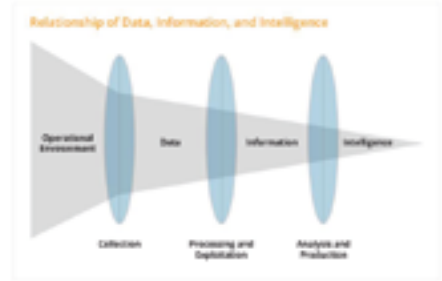
Le cycle traditionnel du renseignement est constamment ressassé. Nous en oublions cependant trop souvent les fondamentaux et confinons la *threat intelligence* aux étapes de collecte, d'analyse et de dissémination. Toutefois, les besoins du client sont au cœur du cycle de renseignement, aux étapes « d'expression des besoins » et « d'ajustement ». Ce sont ces besoins qui conditionnent la collecte et qui influencent l'analyse.

Les activités de recherche et d'investigation en *threat intelligence* sont les plus connues. Le *hunting* à partir de sources ouvertes (OSINT) permet la collecte d'informations sur les groupes d'attaquants, les modes opératoires et les différentes campagnes d'attaques. Mais ces productions ne suffisent pas à elles seules à qualifier une démarche de threat intelligence. Bien qu'intéressant, un rapport sur une campagne ne ciblant ni votre secteur d'activité, ni de potentiels partenaires ou sous-traitants, ni votre zone géographique ou aucune des technologies et équipements que vous managez, ne vous apportera que peu d'éléments concrets au quotidien. La veille et la capitalisation de ces données sont elles aussi insuffisantes, si elles ne se réalisent pas dans l'objectif de vous fournir des pistes d'action.

Pour convaincre, la *threat intelligence* doit gagner en valeur intrinsèque et proposer, comme son nom l'indique, du renseignement.

Le terme « renseignement » est régulièrement employé pour décrire les données factuelles collectées sur un adversaire hostile. Le terme peut cependant se définir comme le résultat d'un processus de collecte, d'analyse, de mise en perspective, d'évaluation et d'interprétation de données à la lumière des réalités du destinataire car ce qui est du renseignement qualitatif pour l'un ne sera qu'une donnée sans valeur ajoutée pour un autre. Le produit final est donc un ensemble d'informations qui, une fois analysées, fournissent des pistes concrètes d'amélioration du niveau de cybersécurité. C'est une aide à la prise de décision.

Une telle définition contredit l'idée d'une *threat intelligence* élitiste ou simplement constituée de feeds ou de rapports sur des précédentes campagnes, annexés d'IOCs, sans mise en perspective, sans recommandations concrètes, voire sans inputs du client.



JP 2-0, Joint Intelligence, 22 octobre 2013, US Department of Defense

De la threat intelligence informative à la threat intelligence appliquée

La *threat intelligence* n'est pas – ou ne devrait pas être – un produit de luxe. Toute entreprise ou institution, quelle que soit sa taille ou ses moyens, de la jeune pousse à la multinationale, peut tirer profit de la connaissance de son environnement et des risques cyber la concernant. Mais pour cela, l'extraction d'informations doit s'appuyer sur plusieurs critères :

– Les critères dits « **objectifs** » sont ceux qui permettent d'identifier et de prioriser les données et les informations qui seront utiles : zone géographique, secteur d'activité, nature du marché, description des logiciels et équipements gérés, exposition médiatique de l'entreprise…
– Les critères dits « **subjectifs** » qui permettent d'ajuster le produit aux besoins et au niveau de maturité du récipiendaire : moyens humains et organisationnels de consommation de la *threat intelligence*, moyens financiers, objectifs de l'organisation, politique de sécurité des systèmes d'information, contraintes légales, nature du capital à protéger…

La *threat intelligence* ainsi cadrée abonde en faveur d'une forme de ruissellement où le renseignement sur les menaces impacte la stratégie de cybersécurité de l'entreprise de façon globale. Elle irrigue l'ensemble des métiers et des acteurs impliqués dans la stratégie de cybersécurité du client final.

Le renseignement sur les menaces cyber peut interférer dans les enjeux business et renouveler le management du risque traditionnel. Loin des indicateurs de compromission et des rapports sur diverses campagnes d'attaques, la *threat intelligence* a vocation à apporter des pistes de réflexion et des éléments de réponse aux questions suivantes :

– À quelles menaces mon entreprise est-elle exposée ? À quels risques faisons-nous face ? Quelles décisions dois-je prendre pour améliorer l'état de cybersécurité de mon entreprise ? Quel est l'impact potentiel de ces menaces sur mon activité, mes investissements, mes partenariats ?

L'anticipation des dégâts engendrés par un rançongiciel sur le système d'information, l'identification de risques accrus dans une zone géographique en proie à des attaques informatiques destructrices, l'occurrence d'incidents ou d'acte de cyber espionnage chez un partenaire ou sous-traitant… sont autant d'informations pouvant peser dans la prise de décisions, le choix de budgets et de polices d'assurances ou encore l'engagement d'investissements en matière de solutions de sécurité.

Dans ce cas précis, la *threat intelligence* est, à l'image de l'intelligence économique ou de la veille concurrentielle, une source d'informations supplémentaire sur l'écosystème d'un organisme. Elle peut se matérialiser par l'évaluation de probabilités de risques, de coûts associés à l'occurrence de ces risques (remplacement, remédiation…). La connaissance des groupes d'attaquants et de leurs capacités, des tendances et des attaques précédentes, permet de réduire les incertitudes et d'anticiper un certain nombre de scénarios, en faveur d'une gestion active des risques. La résilience et la continuité d'activité sont ici nourries par la démarche de *threat intelligence*, qui intègre pleinement la stratégie commerciale de l'entreprise.

Le management de vulnérabilités à l'aune du renseignement sur les menaces est également un enjeu primordial. Le nombre de vulnérabilités rendues publique chaque jour est considérable. La gestion du *patching* de ces vulnérabilités est décisive en matière de cybersécurité opérationnelle. Se renseigner sur les menaces, les acteurs et leurs capacités peut éclairer sur le statut et la criticité d'une vulnérabilité. Est-elle publique ? exploitée activement par un ou des groupes d'activité ? Si oui, lesquels ? Ces groupes d'activité sont-ils susceptibles de s'attaquer à mon secteur d'activité ? La priorisation dans l'application de correctifs peut permettre un gain de temps et d'efficience considérable.

La sécurité des systèmes d'information d'une organisation doit s'adapter à la connaissance de la menace. Qu'il s'agisse de la mission d'architecture sécurité, ou des différents contrôles mis en place, ceux-ci peuvent bénéficier d'une orientation supplémentaire afin de répondre aux risques identifiés. La politique de sécurité des systèmes d'information ainsi que les vagues de sensibilisation peuvent également être ajustées afin de coller aux réalités des menaces actuelles.

Le *Security Operation Center* et l'activité de détection font partie des principaux bénéficiaires du renseignement technique sur les menaces. La contextualisation des données permet une meilleure qualification des alertes et diminue le nombre de faux positifs. L'intégration de flux d'indicateurs de compromission contextualisés en est la première étape pour une détection périphérique mais c'est une stratégie globale

de collecte de logs qui peut être envisagée. L'utilisation d'un modèle de standardisation oriente vers la détection comportementale et en profondeur. L'utilisation d'outils de collecte plus précis que Windows Event Manager, autorise la confection d'algorithmes de détection sur-mesure en réponse aux modes opératoires connus. Ces outils dont un point de départ intéressant pour une démarche de threat intelligence, qu'il convient de compléter au fil du temps par ses propres données et analyses.

La *threat intelligence* devrait idéalement permettre d'**anticiper** les différentes attaques pouvant survenir. Cette matière n'a malheureusement pas pour objectif de prédire le futur et l'analyste n'est pas devin. Il collectera et mettra en perspective nombre d'éléments (modes opératoires et signaux faibles et forts) afin de fournir un panorama complet des risques en présence. Certains signaux peuvent alerter : hausse du nombre de *typosquatting*, reprise d'anciens domaines ou encore fuites de données contenant des identifiants d'utilisateurs du système d'information. L'anticipation est un véritable challenge. L'analyse et la connaissance des différents acteurs, groupes d'activité et campagnes peut donner des indices sur les intentions et mobiles de certains groupes.

Lorsqu'un incident survient, qu'il ait été anticipé ou non, **l'analyste en *threat intelligence* peut fournir des éléments cruciaux aux équipes de réponse à incident.** Quel groupe d'activité attaque ? Pourquoi, et dans quel contexte ? Dispose-t-on d'indicateurs, d'observables et de règles YARA permettant de rechercher les traces supplémentaires de l'attaquant ? Existe-t-il des informations en sources ouvertes, sur les réseaux sociaux, au sujet de cette attaque ? Mon organisation est-elle la seule touchée ? L'attaque est-elle ciblée ou globale ? Des *samples* du maliciel utilisés sont-ils disponibles en ligne et analysés ?

Le renseignement sur les cybermenaces peut transformer la démarche traditionnelle de *pentest* en véritable *Red Teaming*. Les scénarios de simulation basés sur une réelle connaissance des groupes d'activités ciblant notre secteur d'activité, des risques pesant sur notre entité, gagnent en réalisme, et donc en pertinence dans l'évaluation de la couverture défensive. Rien ne vaut une mise en situation dans des conditions réelles. Il est possible, en se concentrant sur quelques acteurs, ou quelques modélisations, de construire des simulations très pertinentes, reproduisant fidèlement les TTPs d'un cluster d'activité, ou panachées selon l'appréciation de l'analyste.

Enfin, **le partage est la clé de voûte d'une démarche de *threat intelligence* réussie**. Dialoguer, échanger avec ses pairs, dans des cercles de confiance,

permet d'enrichir sa base de connaissance en renseignement technique, opérationnel et stratégique. C'est également l'occasion de collecter des indicateurs contextualisés, ainsi que de nombreux retours d'expérience.

Toutes ces applications concrètes sont accessibles, adaptables. Elles challengent une t*hreat intelligence* jusque-là paradoxalement éloignée des préoccupations de son principal consommateur. En somme, il s'agit simplement de s'adapter aux risques existants et de faire des choix éclairés, priorisés et rationalisés, non plus « par défaut ». La *threat intelligence* est à la portée de tous ; elle a le pouvoir de révolutionner la SSI et l'analyse de risques traditionnelle en y apportant un nouveau souffle. De cette démarche évidente ne pourra ressortir qu'une amélioration de la cybersécurité des organisations.

Données personnelles et collectivités territoriales : usages actuels et recommandations

Par Anne le Henanff

Cette étude, réalisée avec la collaboration de Didier Danet et Gérard de Boisboissel, est présentée au titre de la Chaire Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales.
https://www.chaire-cyber.fr/Donnees-personnelles-et-collectivites-territoriales

Les Collectivités territoriales collectent depuis toujours des données ce qui permet d'assurer à leurs habitants des compétences de proximité de très nombreux services. Ces pratiques, souvent non écrites et formalisées, sont l'héritage du fonctionnement des services.

Les collectivités locales sauront rebondir et faire d'une contrainte supplémentaire une opportunité. Nous sommes cependant encore loin d'une politique exemplaire de protection et de gestion de la donnée. Le chemin sera long et l'accompagnement des collectivités locales indispensable. Les données des Français constituent le patrimoine de notre pays et les protéger est une obligation au regard des risques majeurs d'attaques cyber et de vols de données.

ANNE LE HENANFF

Vice-Présidente de l'association nationale Villes-Internet

La gestion des données dans les Collectivités territoriales : une pratique généralisée mais des niveaux d'exigence inégaux et diffus

La gestion des données n'est pas un sujet nouveau pour les collectivités locales. Leurs activités spécifiques, les relations permanentes qu'elles entretiennent avec les citoyens sur de multiples sujets de leur vie

quotidienne et l'archivage des informations collectées font qu'elles maîtrisent parfaitement et depuis longtemps le sujet de la donnée. Les agents territoriaux recueillent, gèrent et conservent toutes ces informations pour le besoin des services au public.

Il est difficile pour une collectivité locale d'exercer pleinement ses compétences sans ce travail préalable de collecte d'informations. Les pratiques en la matière, diffuses et très variées d'une structure à l'autre, dépendent de son histoire, de sa taille, du nombre de services à la population mais aussi des règles de gouvernance et de fonctionnement imposées par le secrétaire de mairie ou le directeur général des services.

Avant l'arrivée de l'informatique, les données étaient recueillies sous un format papier. Le numérique et la dématérialisation des procédures permettent désormais un lien direct entre la mairie et le citoyen. Les données s'inscrivent directement dans un fichier « métier » sans intervention humaine. Quelques exemples : l'inscription des enfants à la cantine et aux activités de loisirs sans hébergement, l'ouverture d'un compteur d'eau, la demande d'attestation d'état civil, etc.

Il est bon de rappeler également que la collecte de données et leur gestion dans les collectivités territoriales sont soumises à une charte de bonnes pratiques que chaque agent signe à son arrivée dans l'organisation. Cette charte insiste sur l'importance du respect de la vie privée des citoyens et la non-divulgation de leurs informations en dehors de la finalité pour laquelle elles sont collectées. Ceci n'évite cependant pas certaines dérives que le RGPD, nous le verrons ultérieurement, limite et rectifie.

Sur les politiques de gestion des données et de conservation dans les collectivités territoriales : un constat alarmant.

Le nombre de données collectées par les collectivités locales est énorme et croît au gré des nouvelles applications et des services aux citoyens. Les agents territoriaux sont soucieux de respecter de bonnes pratiques de traitement et de conservation de ces données. Ceci ne signifie cependant pas qu'elles soient adaptées et appropriées. Elles proviennent souvent de règles non écrites, que le ou la responsable de services fait appliquer et dont l'objectif est le niveau de qualité du service rendu.

Même si cette pratique en silo, déconnectée d'une politique générale de la donnée, est contestable, il est indéniable qu'elle aura finalement été l'une des meilleures protections contre les transmissions injustifiées ou fuites de données à caractère personnel.

Peu de communes, petites ou moyennes, mettent en œuvre une véritable politique

de protection des données applicable par tous et connue de tous. Il existe plusieurs explications :

a) La loi informatique et Libertés, de 1978, a protégé les informations personnelles dès lors qu'elles étaient collectées dans le cadre d'un service spécifique et informatique. Dans les communes, moyennes et petites, nombre de traitements n'ont pas été systématiquement informatisés et n'ont donc pas donné lieu à des déclarations à la CNIL quant à leurs modalités ou leurs finalités. Les informations collectées sont stockées en archives « papier » dans une pièce dédiée de la mairie, souvent sans règles de limitation ou de contrôle d'accès. Aujourd'hui, nous estimons que dans les petites collectivités, un double archivage (papier et numérique) est toujours pratiqué dans 80 % des cas.

b) La politique de sécurité n'est pas une priorité pour les communes, faute de moyens humains, de ressources financières mais aussi de connaissance des risques. Les élus sont sur tous les fronts, leurs dotations se réduisent, les services s'accroissent et il leur est demandé une compétence sur de multiples sujets. La protection des données est assurée *a minima* et ce sont les agents qui en sont généralement les garants.

c) La gestion des données est confiée à des prestataires informatiques extérieurs qui en assurent la sauvegarde. Les petites communes n'ont pas d'informaticiens au sein de leurs équipes et les traitements de la donnée sont confiés à des « experts techniques ».

Le RGPD et les attaques cyber : une petite révolution dans les Collectivités Territoriales et une réelle opportunité pour la sécurité numérique

Quand la collectivité devient une cible pour les cyber-attaquants et qu'elle n'en a pas conscience !

De nombreuses collectivités, petites et grandes, ont subi des attaques cyber du type Ransomware depuis 2014, d'autres des défaçages de leur site internet. Les collectivités territoriales deviennent une cible, situation que les élus et les agents pouvaient difficilement imaginer. Certaines d'entre elles ont perdu des données, d'autres ont subi une atteinte à leur image et à celles de leurs élus. La prise de conscience a d'abord eu lieu, logiquement, dans les communes attaquées. C'est à partir de ce moment que les actions de sensibilisation se sont multipliées sur les territoires auprès des DSI, des élus et des DGS/Secrétaire de mairie.

La Réserve Citoyenne Cyber, l'ANSSI, le CREOGN et d'autres organismes organisent des colloques en Province et à Paris. L'enjeu est clairement de faire

prendre conscience que les Collectivités locales sont devenues des cibles et que le sujet de la protection des systèmes d'information et des données collectées est stratégique. En janvier 2018, le Forum International de cybersécurité (FIC) l'intègre à part entière dans son programme du salon.

Les communes ayant subi des attaques prennent conscience que les données qu'elles collectent ont de la valeur et attisent des convoitises. Les démarches pour mieux les protéger débutent partout en France mais de manière disparate, individuelle. Les communes se sentent bien seules et démunies…

L'arrivée du RGPD : un booster pour les collectivités locales

Un second phénomène permet aux élus et dirigeants des collectivités de prendre conscience des enjeux autour des données : le RGPD.

Même si les élus et les agents ont pris en main tardivement l'application du RGPD dans les collectivités territoriales, ce nouveau règlement européen a été un véritable accélérateur de la mise en œuvre des bonnes pratiques de la gestion des données et plus largement d'une politique de la sécurité des systèmes d'information.

Perçu d'abord, non pas sur le fond mais sur la forme, par l'ensemble des élus comme une contrainte supplémentaire, le RGPD devient finalement une opportunité de mettre en œuvre des bonnes pratiques. Les élus ont dû se préparer en très peu de temps avec le sentiment d'être livrés à eux-mêmes, de ne pas être accompagnés par l'État et de devoir trouver des financements imprévus alors même que les collectivités territoriales subissent des réductions de ressources importantes.

Le RGPD apporte toutefois une nouvelle philosophie de la gestion des données. Le règlement européen aura permis :

– D'analyser la finalité de la collecte des données et de remettre de l'ordre dans ses modalités. Le RGPD introduit davantage de notions de transparence et de transversalité dans les pratiques,

– De mettre à plat les relations avec les fournisseurs informatiques, partenaires directs et interdépendants des communes, quant à la mise en conformité des processus et de leurs enjeux,

– De sensibiliser les agents à leur responsabilité sur le cycle de vie de la donnée, de sa collecte jusqu'à sa suppression et les accompagner dans cette gestion.

– D'engager des démarches transversales afin de positionner la politique de gestion des données au plus haut niveau décisionnel.

La gestion des données dans les collectivités : perspectives et priorités

Le constat de ces derniers mois est clair : nos communes sont de véritables coffres-forts de données publiques et du citoyen. Les informations personnelles de chaque français reposent entre les murs des communes : données familiales, sociales, de santé, pratiques sportives et associatives, etc. Une mine d'informations pour des personnes malveillantes, et ce, à portée de main !

L'étude commandée par le CREOGN au Centre de Recherche des Écoles de Saint-Cyr Coëtquidan, en septembre 2016, et les échanges lors du plateau-télévision sur les enjeux des données dans les Collectivités locales (FIC 2018) l'ont bien mis en évidence : ne pas se préoccuper MAINTENANT de la bonne gestion des données et des systèmes de protection mis en œuvre par les collectivités territoriales pourrait rapidement s'avérer une énorme faute !

Heureusement, en moins d'un an, les communes et autres collectivités locales ont été positionnées au même niveau d'importance que les PME/PMI sur le sujet des risques cyber et donc de la protection des données à caractère personnel. C'est une avancée suffisamment majeure pour la souligner et s'en féliciter. Dorénavant, il faut accompagner et modifier la gouvernance globale de la donnée dans les collectivités territoriales. Trois pistes de réflexion permettent d'en dessiner ses modalités :

En s'appuyant sur des structures existantes et en renforçant les expertises et les moyens.
Il est indispensable d'intégrer fortement l'accompagnement à la conduite du changement auprès des agents. Ces derniers produisent de la donnée à caractère personnel et leur adhésion aux nouvelles pratiques est nécessaire. Si la défaillance humaine représente le facteur de risque le plus fort dans les organisations en ce qui concerne les risques de cyberattaques, il en est de même dans le cadre de la mise en œuvre d'une politique de protection des données à caractère personnel efficace.

Pour cela, il semble opportun de s'appuyer sur des structures existantes ou des expériences territoriales efficaces, ayant fait leurs preuves et qui suscitent la confiance des communes. Il s'agira de leur proposer une organisation capable de les accompagner dans les changements de pratiques et dans leur mise en œuvre auprès des agents des collectivités territoriales.

En affichant au niveau du gouvernement des structures en charge de la protection et de la gestion des données, privées et publiques.
On peut considérer que 3 niveaux d'intervention sont possibles :

A – **National** : La notion d'une structure portant une « organisation nationale de référence », clairement affichée par le gouvernement, est très importante. Elle pourrait être rattachée au 1er Ministre et bénéficier d'un champ

interministériel d'actions. Elle positionnerait le sujet et annoncerait les missions, les cibles et les moyens mis en œuvre. Il s'agirait d'un partenaire de confiance.

B – **Régional** : Un guichet unique, clairement identifié, indépendant et bien intégré sur le territoire régional, aurait vocation à accompagner la mise en conformité de la gestion et de la protection des données des organisations territoriales. Ses missions viseraient à soutenir les communes ou les intercommunalités pour la formation des agents, la sensibilisation aux obligations imparties aux élus et aux dirigeants, la formalisation des préconisations d'organisation interne et de gouvernance, la mutualisation du DPD (Délégué à la protection des données), la mise à disposition d'un « kit clé en main » de la mise en œuvre de la sécurité numérique, la fourniture d'une liste de prestataires informatiques référencés par territoire géographique…

C- **Territoires** : l'intercommunalité semble l'échelon le plus pertinent. Elle permettrait notamment la mutualisation des DPD et le partage des bonnes pratiques entre plusieurs communes d'un même territoire.

La sollicitation d'autres partenaires extérieurs est également envisageable. Il peut s'agir des centres de gestion, du CNFPT (Centre national de la fonction publique territoriale) et de prestataires informatiques. Un point de vigilance concerne ces derniers. Les communes confient souvent leurs données en toute confiance à des prestataires locaux sans avoir expressément prévu des points sur la sécurité numérique tels que la conformité au RGPD, les conditions et le lieu de stockage des données. Il est attendu par les collectivités un cahier des charges référentiel, utilisable lors de la passation des marchés avec les prestataires et qui permettrait de limiter les risques pour les communes.

Le cœur de la sécurisation des politiques de données des collectivités : la formation des personnels

La bonne pratique des collectivités territoriales en matière de gestion des données repose en très large partie sur les agents de la structure. Leur formation semble bien le meilleur moyen de protéger les données des citoyens. L'intégration dans le plan de formation individuelle d'une session de sensibilisation à la gestion des données est recommandée.

La sensibilisation aux bonnes pratiques et leur mise en œuvre sont au cœur d'une politique sérieuse et efficace de la donnée dans les collectivités territoriales. C'est un investissement qui, de prime abord, peut paraître lourd mais qui ne pèse guère au regard des conséquences d'une attaque

cyber et de la perte du patrimoine informationnel de la collectivité.

De plus, les conséquences induites peuvent être dramatiques à bien des égards : l'image du maire et de sa municipalité, le choc psychologique pour l'agent collecteur de la donnée (souvent l'hôtesse d'accueil dans une petite commune), le risque de rupture de la continuité du service public, la perte de confiance du citoyen vis-à-vis de sa commune et de ses dirigeants.

La mise en œuvre d'une vraie politique de la gestion de la donnée est dorénavant stratégique pour une collectivité territoriale, tout autant que l'entretien d'une voie publique, l'accessibilité des bâtiments pour tous les publics, l'accès aux services pour chaque citoyen, l'éclairage sur les voies, la sécurité physique sur l'ensemble de la commune, et la liste est bien longue !

L'AUTEURE

Anne Le Hénanff, dirigeante d'entreprise, est Maire-adjointe à Vannes (56) et conseillère communautaire à « Golfe du Morbihan - Vannes Agglomération ». Elle est en charge du numérique des Systèmes d'information et de la communication. Réserviste citoyenne cyber, elle est Vice-Présidente de l'association nationale Villes-Internet.

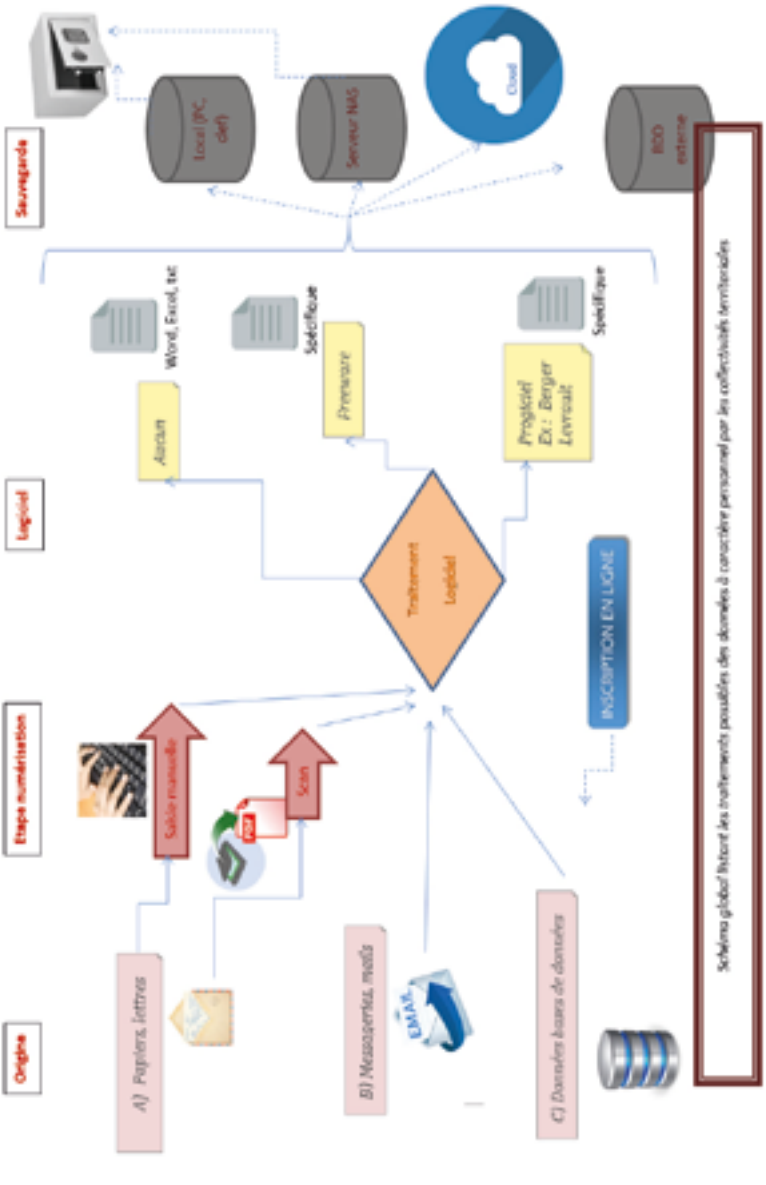


Schéma global listant les traitements possibles des données à caractère personnel par les collectivités territoriales

Fuite de données :
gestion de crise, mode d'emploi

Par Guillaume Tissier

C

« Ce qui ne me tue pas me rend plus fort ». Friederich Nietzsche

Toutes les organisations seront tôt ou tard victimes d'une crise d'origine « cyber » ou intégrant une dimension « cyber ». La question n'est donc pas de savoir « si » mais « quand » cette crise arrivera. Au hit-parade de ces crises : les fuites de données, c'est-à-dire les pertes de données confidentielles, d'origine malveillante ou non. Qu'elles concernent Facebook, Google Plus, Equifax, Yahoo, Ashley Madison, Target, mais aussi plus près de chez nous FDJ, FastBooking, Groupama…, l'actualité nous le rappelle sans cesse : ces crises peuvent déstabiliser durablement les organisations victimes et ne concernent pas que les grandes plateformes web. 742 fuites de données ont ainsi été déclarées à la CNIL entre le 25 mai 2018, date de l'entrée en vigueur du RGPD, et le mois d'octobre 2018. Si l'on part du principe -salutaire- que les dispositifs de prévention des risques sont nécessairement faillibles et qu'il faut toujours se préparer au pire, il est donc essentiel que les organisations se préparent à la gestion de crise.

GUILLAUME TISSIER

Directeur général
CEIS

Les 10 caractéristiques clés d'une fuite de données

Chaque crise possède des caractéristiques propres. Il en va de même pour les fuites de données.

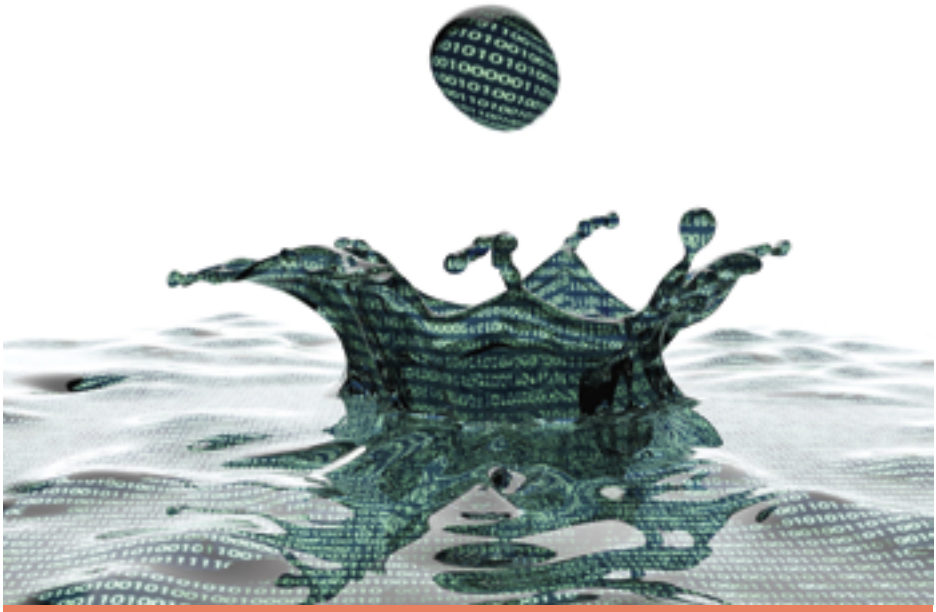
1. **Des crises globales.** Les crises « cyber » ou impliquant une dimension « cyber » ne sont pas de simples crises techniques, IT ou SSI. Leur impact est d'abord « business ».
2. **L'exigence d'une approche pluridisciplinaire.** Les fuites de données exigent

une réponse globale associant une réaction technique à des réponses « métier », juridique, assurantielle etc. La plupart des fonctions de l'organisation doivent donc être impliquées dans le dispositif, au premier rang desquelles la direction générale.

3. **Des crises imprévisibles.** Même si les capacités d'anticipation et de détection s'améliorent, l'asymétrie traditionnelle entre attaquant et défenseur rend les fuites d'origine malveillante difficiles à prévoir.
4. **Une temporalité différente.** Contrairement à des crises traditionnelles dont les effets sont généralement limités dans le temps ou obéissent à des règles de propagation à peu près établies, les crises « cyber » n'obéissent à aucune règle. La fuite peut être découverte et avoir des effets des mois après l'intrusion dans le système d'information.
5. **Une « sous-information » chronique.** La nature technique de l'environnement numérique, le « brouillard » qui l'entoure, la multiplicité des causes et la durée des investigations techniques expliquent que les organisations mettent longtemps avant d'identifier les causes réelles de la crise, ce qui complexifie les actions de communication.
6. **Une viralité importante.** Les fuites de données sont fortement médiatisées et bénéficient d'une forte viralité en raison de la sensibilité croissante des utilisateurs à la protection de leurs données. Au point qu'il y a parfois un véritable décalage entre la réalité de la crise et sa perception par les acteurs externes.
7. **Des impacts difficiles à évaluer.** Les crises « cyber » sont des crises systémiques avec des effets multiples en cascade et non limités géographiquement. Point clé : les impacts « métiers » qui se traduisent nécessairement en pertes financières et en atteintes à l'image de marque, plus difficilement quantifiables mais bien réelles. La confiance se gagne dans la durée mais se perd en quelques minutes…
8. **Une judiciarisation croissante.** La sensibilité croissante de la société civile à la protection des données personnelles et l'émergence de cadres législatifs et réglementaires en matière de protection des données débouchent sur une judiciarisation croissante des fuites de données, et la nécessité pour les organisations de mettre en place, en amont, une approche de conformité.
9. **Des arbitrages complexes entre continuité et réponse juridique.** Le besoin de geler la « scène de crime » pour les investigations, préalable indispensable à toute action judiciaire et à la mise en œuvre d'une éventuelle police d'assurance, se heurte souvent à la volonté des organisations de faire redémarrer au plus vite leurs activités pour limiter l'impact de la crise.
10. **Une capacité de réponse affaiblie.** L'impact de la crise sur le système

d'information et la mise en œuvre de mesures conservatoires entravent souvent les capacités de réponse et de continuité des organisations. Difficile, par exemple, de mettre en œuvre une communication vers les clients lorsque les canaux de communication traditionnels ont été coupés ou lorsqu'une partie des systèmes d'information est momentanément paralysée.

Les spécificités des crises résultant de fuite de données impliquent donc **d'adapter le dispositif de gestion de crise existant**. Au-delà des capacités de prévention destinées à réduire ses vulnérabilités et sa surface d'exposition aux risques, des capacités de détection qui permettront d'identifier le plus en amont possible un incident susceptible de déboucher sur une crise, Il s'agira donc de travailler à la fois sur **l'organisation, les moyens et les processus de gestion de crise** pour réduire son impact lorsque qu'elle n'aura pu être empêchée.



© concept of data pool an ocean of information Par the_lightwriter

La gestion d'une fuite de données doit être intégrée dans un contexte juridique. Elle devra comporter une réponse tant technique qu'informationnelle pilotée par une équipe mêlant une dimension stratégique et opérationnelle.

Quelle organisation ?

L'organisation de la gestion de crise doit bien sûr être adaptée à chaque entité mais certains principes devront être respectés :

– **Un pilotage stratégique, assuré par la tête de l'entité.** La fuite de données n'étant pas seulement une crise « informatique », le pilotage sera assuré par la direction générale, un membre du COMEX ou l'un de ses représentants (secrétaire général, « *risk manager* », directeur sécurité/sûreté…), qui devra faire la synthèse entre la vision « *business* » et les réalités techniques. L'implication du top management est ainsi l'une des conditions essentielles de l'efficacité du dispositif. Ce pilotage devra par ailleurs permettre à l'entité de se positionner à la fois dans une posture de « temps court » et de « temps long » pour anticiper le « coup d'après ». L'objectif est de ne plus « subir » la crise et de reprendre la main.

– **L'implication de toutes les fonctions transverses.** Le pilotage stratégique devra associer toutes les fonctions transverses susceptibles d'être impliquées dans la crise, qu'il s'agisse de la DSI, du RSSI, de la direction juridique, du DPO, du *risk manager*, de la direction de la communication interne et externe, voire des directions de la conformité et des affaires publiques pour les organisations en disposant.

– **Une conduite opérationnelle assurée par le ou les métiers impliqués.** « Le terrain commande », dit-on dans les Armées. De fait, si le pilotage global de la crise ne doit pas leur incomber, ce seront le ou les métiers impliqués qui auront la main sur la conduite opérationnelle, tout en étant appuyés par les directions transverses.

– **La mobilisation d'experts internes ou externes** qui apporteront un éclairage complémentaire et un certain recul sur la situation. Les experts externes pourront aussi constituer des alliés précieux en matière de communication.

POINT CLÉ : l'articulation entre les niveaux stratégiques et opérationnels

Dans les grandes organisations, l'échelon opérationnel pourra faire l'objet d'une cellule spécifique, dont le fonctionnement devra être soigneusement articulé avec une cellule « tête de groupe », très resserrée, assurant le pilotage stratégique de la crise et réunissant les grandes fonctions transverses. Une autonomie excessive de la cellule opérationnelle, fréquente lorsque les deux cellules sont éloignées géographiquement, tout comme une mainmise de la cellule stratégique sur les opérations et un « micro-management de la crise » devront être évitées. Inutile par exemple d'épuiser la cellule opérationnelle par des demandes permanentes de comptes-rendus. Il est essentiel de ménager les hommes, les crises s'installant parfois dans la durée…

L'utilisation d'une matrice RACI[1] permettra d'attribuer des rôles et de déterminer les périmètres de responsabilité entre les différents acteurs. De façon globale, le dispositif devra ainsi couvrir les différentes fonctions indispensables à la gestion de crise : la « décision », l'anticipation et la planification, le suivi de situation, la conduite opérationnelle et la communication interne et externe. Au plan RH, il pourra enfin être utile de prévoir un fonctionnement 24/7, avec toutes les incidences contractuelles que cela peut avoir en interne et sur les sous-traitants.

(1) RACI est l'acronyme de « Responsible, Accountable, Consulted, Informated » - Il s'agit des rôles rattachés à un projet. Cette matrice qui permet de visualiser facilement la répartition des rôles entre les parties prenantes, et constitue un outil de coordination et de communication très efficace de gestion de projets complexes.

Quels processus ?

– **Étape 1 : *l'alerte.*** Elle peut avoir trois origines : 1. un lanceur d'alerte signale une fuite de données directement à l'organisation (exemple : le protocole utilisé par le site Zataz[2] destiné à avertir les organisations d'une vulnérabilité, d'une fuite ou d'un piratage), ce qui implique une réponse rapide de façon à éviter que l'information ne se propage dans la presse ; 2. un « *hacker* » signale lui-même la fuite à l'entreprise. Là aussi, l'information devra être rapidement prise en compte avec toutes les précautions nécessaires, a fortiori si le « *hacker* » n'est pas « éthique » et tente de monnayer sa découverte, voire de faire chanter l'organisation ; 3. le SOC/CERT de l'entreprise, internalisé ou externalisé, détecte un incident et transmet l'alerte à sa hiérarchie après une première évaluation.

(2) https://www.zataz.com/protocole-alerte-zataz/

– **Étape 2 : *l'escalade et la mobilisation.*** Une évaluation plus approfondie est menée pour savoir s'il y a lieu de mobiliser le dispositif de crise. Tout incident ne constitue pas forcément une crise potentielle. Dans le cas d'une fuite de données, il s'agira d'évaluer l'impact en termes de confidentialité et d'intégrité des données, en s'appuyant sur les analyses d'impact (*Privacy Impact Assessment* ou PIA) qui ont normalement été faites pour chaque traitement de données personnelles (cf. article 35 du RGPD). Si l'incident est considéré comme suffisamment grave sur la base de différents critères (périmètre de la fuite, nature des données « fuitées », risque juridique, risque financier, impact en termes d'image…), le dispositif de crise est alors immédiatement activé.

– **Étape 3** : ***le confinement.*** L'objectif est de prendre les mesures d'urgence permettant de faire cesser la fuite de données, par exemple en stoppant le traitement de données incriminées. Une étape particulièrement délicate puisqu'il s'agira souvent de faire des arbitrages entre la volonté d'isoler, voire de couper, telle ou telle partie du système d'information et le besoin de maintenir en l'état le système pour permettre les investigations

futures. L'arrêt d'un serveur peut en effet avoir pour conséquence de détruire les données stockées en mémoire vive, tandis qu'une déconnexion du réseau diminuera les chances de remonter jusqu'à un éventuel attaquant.

– **Étape 4 :** ***les investigations techniques.*** Cette étape est primordiale, tant d'un point de vue opérationnel afin de comprendre les causes de la fuite de donnée et y remédier, qu'au plan juridique et assurantiel. Elle donne lieu à l'exploitation, par une équipe interne ou externe, de l'ensemble des logs de connexion et à un travail de « hunting » interne pour détecter d'éventuels APT sur le réseau. À noter de ce point de vue l'importance des systèmes de « bastion » qui permettent d'enregistrer et de surveiller l'ensemble des accès aux serveurs et données critiques de l'entreprise.

– **Étape 5 :** ***les notifications aux autorités et aux clients.*** En vertu de l'article 33 du RGPD, la notification à la CNIL, qui peut se faire en ligne[3], doit avoir lieu au plus tard dans les 72 heures après que l'organisation ait eu connaissance de la fuite. À noter que la CNIL peut aussi avoir été prévenue simultanément par le lanceur d'alerte, ce qui renforce la nécessité de réagir vite. Une notification doit aussi être faite auprès de toutes les personnes physiques concernées par la fuite dès lors que celle-ci entraîne « un risque élevé pour les droits et libertés d'une personne physique » (article 34 du RGPD). À noter que pour les Opérateurs d'Infrastructures Vitales (OIV) ou Opérateurs de Services Essentiels (OSE) au sens de la directive NIS, la notification devra être assurée en parallèle auprès de l'ANSSI.

(3) https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

– **Étape 6 :** ***la remédiation et la restauration.*** Il est bien sûr préférable que cette étape ait lieu une fois les causes techniques de l'incident identifiées et analysées.

– **Étape 7 :** ***le retour d'expérience.*** Toute crise doit donner lieu à une boucle retour permettant d'améliorer le dispositif. Ce RETEX concerne à la fois le renforcement des capacités de détection, par exemple par l'intégration de nouvelles règles techniques, la création d'un « set » de réponses à incident plus ou moins automatisées, et la recherche d'une meilleure application de la politique de sécurité des systèmes d'information, notamment en matière de mise à jour des serveurs critiques. Ce processus visera aussi à améliorer le fonctionnement d'ensemble du dispositif par l'optimisation des procédures et moyens mis à disposition.

Le dispositif de gestion de crise devra en effet s'appuyer également sur différents processus « support », parmi lesquels :

– **La prévention et préparation.** Une fois créé, le dispositif de gestion de crise doit être maintenu en condition opérationnelle grâce à des sensibilisations régulières, des exercices stratégiques (ou table-top) et des entraînements opérationnels pour

les équipes techniques. Objectif : favoriser des actes-réflexe et éviter toute improvisation en situation réelle. Des média training pourront aussi être organisés pour les porte-parole qui seront désignés.

– **La gestion de la main courante.** Tout événement, information externe, prise de décision etc. devra être enregistré, tant pour des raisons juridiques et assurantielles (prouver que l'organisation a bien mis en œuvre telle ou telle mesure) que pour faciliter le retour d'expérience post-crise.
– **La veille et le suivi de situation.** Le « *situational awareness* » permet une bonne appréciation de la situation, et facilite donc la prise de décision. Ce processus fonctionnera à la manière d'une gare de triage de l'information et se traduira par l'organisation de points de situation réguliers tout au long de la mobilisation du dispositif.

Quels moyens logistiques ?

La compression du temps en situation de crise exige la mise à disposition rapide de différents moyens logistiques déjà testés et éprouvés :

– **Moyens de communication.** Ceux-ci se traduiront d'abord par la mise en place de moyens spécifiques de communication et de partage de fichier, si possible distinct de l'infrastructure habituelle de l'organisation potentiellement atteinte par la crise. Exemples : mise en place d'un système de messagerie instantanée et de téléphonie sécurisée ainsi que d'un espace documentaire partagé de type « *data room* ».

QUELLE COMMUNICATION INTERNE ET EXTERNE ?

La communication est une fonction-clé de la cellule de crise.
Sur le plan externe, elle doit s'appuyer sur une parfaite identification des parties prenantes (clients, fournisseurs, autorités, associations, médias, élus…) afin de déterminer des messages ciblés et les canaux les plus appropriés. Elle passera par la désignation d'un porte-parole qui s'appuiera sur les éléments de langage fournis par la direction de la communication. Faute d'éléments précis sur les causes techniques de la fuite de données, son périmètre ou les victimes potentielles, il s'agira souvent d'exploiter des données factuelles sur le dispositif RGPD de l'organisation, son engagement en matière de cybersécurité etc., au risque de paraître répétitif devant les journalistes. Rien n'est pire que le « rétropédalage » qui consiste à revenir sur ses propres déclarations pour « rectifier le tir », par exemple sur le nombre de victimes potentiels. Inutile, aussi, d'attribuer la fuite publiquement. Cette attribution est non seulement techniquement délicate, voire impossible, mais stratégiquement maladroite, car elle peut donner l'impression que l'organisation cherche à se défausser et à rejeter toute responsabilité. La mise en cause publique d'un sous-traitant devra ainsi être évitée, d'autant qu'au titre du RGPD, l'organisation est responsable de ses sous-traitants.
La communication interne est également essentielle. Elle permettra d'éviter la frustration, assez fréquente, des salariés qui apprennent par l'extérieur une information concernant leur propre organisation et surtout de mobiliser l'ensemble des salariés dans un moment critique.

– **Moyens physiques.** Une ou plusieurs salles devront être mises à disposition du dispositif de crise avec l'ensemble des capacités nécessaires (connectivité, projection…).
– **Moyens de veille informationnelle.** Indépendamment des capacités de surveillance et de détection utilisées en amont, une veille spécifique, temps réel, devra être menée, en particulier sur les réseaux sociaux, pour suivre les retombées de la crise.
– **Moyens méthodologiques.** Outre le manuel de gestion de crise et l'ensemble des plans d'urgence (PCA/PRA etc.), il s'agira aussi de disposer de fiches « réflexes » pour chaque processus de gestion de crise afin d'automatiser au maximum les actions et de gagner quelques précieuses heures. Plusieurs exemples : modèle de « main courante », cartographie des parties prenantes, annuaire de crise interne et externe, éléments de langage commun en matière de communication, listes de diffusion internes et externes « prêtes à l'emploi ». Il sera aussi essentiel de disposer d'une documentation à jour sur le système d'information et la politique de sécurité, sur le dispositif RGPD, sur les éventuelles assurances « cyber » etc.

LE RÔLE CLÉ DE L'ASSURANCE « CYBER »

Si les assurances traditionnelles couvrent les dommages matériels sur les réseaux et systèmes d'information, les polices « cyber » permettent d'assurer les conséquences liées aux atteintes aux données. Dans le cas d'une fuite de données, elles permettront par exemple de couvrir les frais de gestion de crise et de notification aux clients qui peuvent rapidement grimper. En revanche, leur activation supposera une évaluation précise de l'impact de la fuite en termes financiers. La souscription à de telles garanties impliquera aussi en amont la mise en place d'une démarche de management des risques.

L'AUTEUR

Guillaume Tissier est le directeur général de CEIS, société de conseil spécialisée sur les questions de défense et de sécurité. Elle intervient à la fois en matière de sécurité économique et numérique. Elle réalise notamment des prestations de conseil et d'accompagnement en cybersécurité et organise régulièrement des exercices de crise ainsi que des entraînements opérationnels dans le cadre du centre d'entraînement BlueCyForce, qu'elle anime avec Diateam.

Fuites de données, quelle réglementation ?

Par Sabine Marcellin

Dans notre monde numérique, la fuite de données est aujourd'hui l'une des vulnérabilités majeures pour les organisations. Les facteurs de risque sont multiples : erreur humaine, menace interne ou externe. Selon certaines analyses, la fuite de données est également devenue une véritable arme[1] commerciale et politique. Face à ce risque, comment la réglementation contribue-t-elle à renforcer les obligations de sécurisation ? Au sein de l'entreprise, quelles sont les mesures, notamment juridiques, qui contribuent à la sécurité de l'information ? Enfin, en cas de fuite d'information, quels sont les modes de réaction à connaître ?

(1) Pierre Gastineau et Philippe Vasset, Arme de déstabilisation massive. Enquête sur le business de fuites de données, LGDJ, 2017.

SABINE MARCELLIN

Avocate of counsel
Staub et associés

Les exemples de fuites d'informations ne manquent pas. Rien que pour la seule année 2018, la presse a cité de nombreuses sociétés victimes : Twitter, Exactis, Trello, Google+, Adidas, Française des jeux, Infogreffe, etc.

L'usage accru des technologies de l'information, la mondialisation des échanges et le recours croissant à l'externalisation exposent les organisations à des actes de prédation. La fuite de données peut avoir des conséquences dommageables pour les organisations publiques et privées, notamment la diffusion d'informations confidentielles, la violation de données personnelles et l'atteinte à l'image de marque.

Pour anticiper, quelle réglementation européenne de protection de l'information ?

Les législateurs européens contribuent au renforcement de la sécurité de l'information et à leur harmonisation entre leurs États. Les nouvelles exigences en termes de protection, l'extension du pouvoir de l'État en

© Antivirus and firewall concept By alphaspirit

Les données personnelles, sensibles par leur essence dans un espace démocratique, sont sujettes à un régime d'obligation de sécurisation et de publicité en cas de violation.

matière de contrôle et de sanctions, et les obligations de notification d'incidents sont destinées à favoriser la sécurité.

Quels sont les piliers majeurs, pour doter l'Union européenne d'une cybersécurité solide ? Les textes réglementaires renforcent la protection des données personnelles, le secret des affaires et plus largement la sécurité des systèmes d'information essentiels.

(2) Règlement (UE) 2016/679, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

L'obligation d'assurer la sécurité des données personnelles existe en France, depuis 1978, dans la première version de la loi Informatique et Libertés. Elle a été depuis largement renforcée par le Règlement Général sur la protection des données[2] (RGPD) applicable, depuis le 25 mai 2018, dans tous les États membres.

(3) Loi n° 2018-493 relative à la protection des données personnelles du 20 juin 2018.

La loi française relative à la protection des données personnelles du 20 juin 2018[3] a réformé la loi Informatique et Libertés en y introduisant les principes du RGPD et en la complétant par les dispositions laissées dans la sphère de compétences des législateurs des États membres.

(4) Directive 2016/1148, du 6 juillet 2016, concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Pour assurer la continuité d'activité des États membres et renforcer la sécurité de l'information, la directive du 6 juillet 2016[4], dite NIS (*Network and Information Security*)

ou SRI (Sécurité des Réseaux et de l'Information), concerne les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information. Cette directive NIS prévoit le renforcement des capacités nationales de cybersécurité et instaure un cadre formel de coopération entre États membres, selon plusieurs principes :

– le renforcement des capacités nationales de cybersécurité. Les État membres doivent se doter d'autorités nationales compétentes en matière de cybersécurité (en France, l'ANSSI), d'équipes nationales de réponse aux incidents informatiques (CSIRT, et pour la France le CERT-FR) et de stratégies nationales de cybersécurité ;
– le renforcement par chaque État de la cybersécurité « d'opérateurs de services essentiels » ou OSE. Ces OSE, stratégiques pour le fonctionnement de l'économie, doivent respecter des règles nationales de cybersécurité et notifier les incidents ayant un impact sur la continuité de leurs services essentiels auprès de l'autorité désignée, soit l'ANSSI en France ;
– l'établissement d'un cadre de coopération volontaire entre États-membres sur les aspects politiques et techniques de la cybersécurité ;
– l'instauration de règles européennes communes en matière de cybersécurité des prestataires de services numériques, notamment pour le cloud computing et les moteurs de recherche.

(5) Loi n° 2018-133, du 26 février 2018, portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

(6) Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

(7) Arrêtés du 13 juin, 1er août et 14 septembre 2018.

En France, la transposition de la directive NIS, assurée par l'ANSSI en lien avec les acteurs concernés, a pu bénéficier des travaux réalisés dans le cadre du renforcement de la cybersécurité des opérateurs d'importance vitale (OIV). Cette directive a été transposée en droit français par la loi du 26 février 2018[5] portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. Son décret d'application, du 25 mai 2018[6], et ses trois arrêtés[7] étendent les obligations de sécurisation de systèmes d'information des OIV aux OSE et aux fournisseurs de services numériques.

(8) Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

Afin de protéger les informations commerciales des entreprises européennes, un autre instrument a été adopté en juin 2016 : la directive applicable au secret des affaires[8].

(9) Sabine Marcellin et Thibault du Manoir de Juaye, Le secret des Affaires, éditions Lexis-Nexis, 2017-2019.

À un ensemble de textes, vaste et hétérogène, protégeant déjà les informations confidentielles des entreprises dans tous les États membres, s'ajoute dorénavant la protection spécifique au secret des affaires[9].

La France a transposé cette directive par la loi du 30 juillet 2018 relative à la protection du secret des affaires[10]. Cette loi permet aux entreprises de protéger les informations dès lors que celles-ci ont une valeur commerciale et qu'elles font l'objet de mesures de protection raisonnables pour en conserver le caractère secret.

(10) Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.

Au-delà de ces réglementations déjà applicables, demain d'autres projets européens contraindront les entreprises à sécuriser leur système d'information. Quelles sont les principales propositions de règlement ?

– Le règlement *e-privacy*[11], dont l'objectif est de renforcer la confiance des consommateurs dans l'offre de services numériques, de simplifier les règles relatives aux cookies et de rendre le marketing des entreprises plus transparent ;
– Le règlement relatif à la libre circulation des données à caractère non personnel (*free flow of data*). Dans cette proposition, la Commission avance un nouveau principe consistant à supprimer les exigences en matière de localisation des données tout en garantissant aux autorités compétentes des droits d'accès aux données à des fins de contrôle réglementaire ;
– Le « paquet cybersécurité » qui comprend une proposition de règlement et une recommandation proposant un cadre européen de réponse aux crises *cyber*.

(11) Proposition de règlement sur la vie privée et les communications électroniques.

Au travers de nouvelles propositions d'instruments européens, la volonté de l'Europe est de renforcer les structures de cybersécurité des États membres, de s'équiper d'outils adéquats pour réagir aux cyberattaques et de maintenir une autonomie stratégique dans ce domaine.

Pour prévenir, quelle politique de sécurité de l'information dans l'entreprise ?

Comment l'entreprise, qui connaît les risques de fuite de données et ses obligations de sécurisation, peut-elle se protéger ? La prévention des fuites d'information ou *data leak prevention* s'inscrit dans la politique de sécurité de l'information, qui vise à assurer non seulement la confidentialité des données mais aussi leur disponibilité et leur intégrité. Elle est conduite par le RSSI[12] ou CISO[13] qui veille à son application et assure un rôle de conseil, de formation et d'alerte. Le DPO[14] est également un acteur incontournable pour s'assurer de la conformité de l'entreprise à la réglementation relative à la protection des données personnelles.

(12) Responsable de la sécurité des systèmes d'information.

(13) Chief Information Security Officer.

(14) Data Protection Officer ou délégué à la protection des données.

La sécurité de l'information est assurée par un ensemble de moyens techniques qui restent incontournables : pare-feux, chiffrement,

(15) Security Operation Center ou centre de sécurité informatique.

analyse des flux et des applications, gestion de l'identification, de l'authentification, etc. À ces dispositifs s'ajoutent également des mesures opérationnelles, et notamment :

– La classification, permettant d'adapter la protection à la sensibilité des données,
– La cartographie des risques informatiques,
– la mise en place d'un SOC[15], c'est-à-dire une plateforme de surveillance des systèmes d'information de l'entreprise (sites Web, applications, bases de données, centres de données, serveurs, réseaux, postes de travail et autres terminaux).

(16) Kit de sensibilisation, disponible sur son site.

Pour sensibiliser non seulement les entreprises mais également les utilisateurs aux cyber-risques et à l'hygiène informatique, les pouvoirs publics se mobilisent. L'ANSSI prône l'anticipation des risques numériques et publie de nombreux guides sur son site. Par ailleurs, le programme gouvernemental *cybermalveillance.gouv.fr*[16] assume un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique et met à la disposition des usagers des outils et des publications dispensant de nombreux conseils pratiques.

Sur la palette des solutions de cybersécurité, comment le droit peut-il contribuer à la sécurisation ? L'un des outils juridiques majeurs est l'élaboration d'un cadre contractuel adapté aux activités de l'entreprise. Le contrat permet d'encadrer et de sécuriser les échanges de données, notamment pour les accords de prestations informatiques ou les contrats de travail. Dans certains cas, la réglementation contraint les responsables de traitement et leurs sous-traitants à passer un contrat (marchés publics, protection des données personnelles, etc.). Pour protéger les données, il sera utile de formaliser notamment les usages prévus, les modes de sécurisation, de confidentialité et d'audit, le contour des responsabilités, les conditions de restitution ou de destruction des données. Dans les accords internationaux, il sera nécessaire également de déterminer la localisation des données et la nationalité des entreprises, qui pourra générer parfois l'application de règles extraterritoriales[17].

(17) Assemblée Nationale, rapport d'information sur l'extraterritorialité de la législation américaine, février 2016.

Au sein de l'entreprise, d'autres instruments juridiques permettent de sensibiliser et responsabiliser les collaborateurs, comme le règlement intérieur, la charte informatique, etc. Par ailleurs, la formation et la sensibilisation régulière des collaborateurs leur permettent de mieux connaître les risques, les sanctions éventuelles et les moyens de prévention.

Enfin, un autre mécanisme pluridisciplinaire est essentiel pour anticiper les risques : la gestion de crise et son corollaire, le plan de continuité d'activité. La gestion de crise consiste à construire, sur la base de la

cartographie des risques, une organisation permettant de réagir à la réalisation de ces risques. Il s'agit de préconstituer l'équipe de décideurs et conseillers, de structurer l'information essentielle et de déterminer le mode de fonctionnement d'une cellule de crise. La fuite de données figure parmi les risques à intégrer dans la gestion de crise.

Pour réagir, quels réflexes en cas de fuite de données ?

(18) Fuite de données personnelles : comment procéder aux notifications et gérer la crise ? Sabine Marcellin et Jérôme Boisseau, Le Village de la Justice, avril 2018.

L'entreprise qui détecte qu'elle est victime d'une atteinte à son système d'information et d'une fuite de données devra réagir avec rapidité et efficacité[18]. En application de son plan de gestion de crise, la direction de l'entreprise confiera à ses experts internes de sécurité de l'information notamment le RSSI, voire externes, la gestion de l'incident et la mise en œuvre des premières mesures.

Des décisions sont à prendre par la direction de l'entreprise : à quelles autorités notifier l'incident ? Quand porter plainte ? Quand signaler la fuite à l'assureur ? Comment communiquer et gérer les conséquences du sinistre ?

(19) En application de l'article R. 1332-41 du Code de la défense. Le formulaire de déclaration est disponible sur le site de l'ANSSI.

L'entreprise victime de violation de sécurité doit la notifier auprès d'autorités administratives. Les OIV et les OSE doivent déclarer l'incident auprès de l'ANSSI[19]. Une violation de données à caractère personnel doit être notifiée à la CNIL dans les 72 heures à compter de sa constatation[20]. En cas de risque élevé, l'entreprise victime d'une violation de la confidentialité des données devra également la notifier aux personnes concernées. En cas de doute, la CNIL indiquera s'il est nécessaire de le faire.

(20) En application de l'article 34 bis de la loi n° 78-17 modifiée. Le formulaire de notification est disponible sur le site de la CNIL.

(21) Infographie - Bilan : 4 mois de RGPD en chiffres - Notification de violation, 16 octobre 2018.

La CNIL a publié un premier bilan des notifications de violations de sécurité, après 4 mois d'application du RGPD[21] : 742 d'entre elles ont été signalées à la Commission, dont 695 concernent la confidentialité des données. L'origine des fuites serait, dans 65 % des cas, un acte malveillant externe et 33 millions de personnes sont concernées.

(22) Centre de lutte contre les criminalités numériques

(23) Brigade d'Enquête sur les Fraudes aux Technologies de l'Information, dépend de la Direction régionale de la police judiciaire de Paris.

Pour l'entreprise victime d'une fuite de données, la question du dépôt de plainte se pose immédiatement. La plainte est l'acte juridique par lequel la victime d'une infraction en informe les autorités judiciaires. Les entreprises semblent réticentes à porter plainte mais les notifications obligatoires devraient les encourager en ce sens. Pour les entreprises sur les territoires, la plainte est déposée auprès de la gendarmerie (enquêteurs spécialisés NTECH et C3N[22]).

Pour les sociétés dont le siège est à Paris ou dans la petite couronne, la démarche s'effectue auprès de la BEFTI[23]. La plainte peut également être transmise au procureur de la République, en écrivant au tribunal de grande instance du lieu où l'infraction a été commise. La plainte avec constitution de partie civile est déposée devant le juge d'instruction, lorsque l'entreprise considère être victime d'un dommage.

Dans tous les cas, l'entreprise victime devra documenter sa plainte en collectant les éléments de preuve (données de connexion et d'analyse, journaux, etc.). Les délais pour déposer cette plainte dépendent de la catégorie d'infraction (exemple : 3 ans pour un délit) mais plus la plainte sera déposée rapidement, plus l'enquête sera facilitée.

Que se passe-t-il suite au dépôt de plainte ? Selon les résultats, l'enquête pourra donner lieu à l'ouverture d'une information judiciaire. Une collaboration étroite doit être mise en œuvre entre les enquêteurs et les services concernés de l'entreprise afin de recueillir le maximum d'éléments d'information permettant de caractériser l'attaque, sa motivation et son origine.

(24) Précité.

(25) Convention sur la cybercriminalité, STE n° 185, 23 novembre 2001.

L'enquête devra déterminer l'origine d'une fuite, sachant que les recherches extra-territoriales sont toujours plus complexes. Dans son ouvrage consacré aux fuites de données[24], Pierre Gastineau explique que *« reconstituer une chaîne de responsabilité après une fuite de données est une tâche aussi hasardeuse qu'herculéenne »*. La

VIOLATIONS DE DONNÉES MAJEURES – Source Breach Level Index- 2018

Organisation	Nombre de personnes concernées	date	Type de fuite	Origine de l'incident	Localisation	Domaine d'activité
Facebook	2,1 milliards	4 avril 2018	Vol d'identité	externe	États-Unis	Réseau social
Equifax	147,9 millions	15 juillet 2018	Vol d'identité	externe	États-Unis	Finance
Reliance Jo	120 millions	10 juillet 2017	Accès au compte	externe	Inde	Technologie
Friend Finder Networks	412 millions	16 octobre 2016	Données sensibles	externe	États-Unis	Site de rencontre
Anthem Insurance Companies	78,8 millions	27 janvier 2015	Vol d'identité	Action étatique	États-Unis	Santé
Yahoo	500 millions	1er décembre 2014	Accès au compte	externe	États-Unis	Technologie
Home Depot	109 millions	2 septembre 2014	Informations financières	externe	États-Unis	Service
JPMorgan Chase	83 millions	27 août 2014	Vol d'identité	externe	États-Unis	Finance
CyberVor	1,2 milliard	5 août 2014	Accès au compte	externe	Mondial	Technologie
eBay	145 millions	21 mai 2014	Vol d'identité	externe	États-Unis	Commerce en ligne

Convention de Budapest sur la cybercriminalité[25] est le seul traité international contraignant, ratifié aujourd'hui par 59 pays mais non par la Russie, la Chine, la Corée du Nord ni l'Iran, qui dispose de standards différents en la matière.

(26) Article 313-1 du Code pénal.

(27) Article 226-4-1 du Code pénal.

(28) Article 323-1 du Code pénal.

Selon les éléments de l'enquête, différentes infractions peuvent être retenues, telles que l'escroquerie[26], l'usurpation d'identité[27] ou l'accès frauduleux à un système automatisé de données[28].

(29) Rapport interministériel sur la cybercriminalité, rapporteur Marc Robert, juin 2014.

(30) Cass. Crim. 22 octobre 2014, n° 13-82.630 ; Cass. Crim. 16 janvier 2018 n° 16-87.168, Cass. Crim. 20 août 2018, n° 18-84.728.

Il est difficile d'appréhender la fréquence des procédures judiciaires dans le domaine de la cybercriminalité[29], car elles correspondent à des catégories pénales variées. Cependant il semblerait que les actions judiciaires[30] se développent. La judiciarisation des fuites de données semble incontournable, à la suite du renforcement des règles et des sanctions encadrant le traitement des données personnelles.

(31) Traduction anglaise du terme fuite.

L'entreprise victime d'un *leak*[31] sera susceptible de répondre à des réclamations judiciaires, émanant de tiers, qui auraient également subi un préjudice du fait de cette fuite. Celle-ci pourrait être mise en cause notamment pour négligence ou non-respect de ses obligations légales.

Si l'entreprise dispose d'une police d'assurance couvrant le risque cyber, une autre déclaration doit être effectuée auprès de l'assureur, dans le respect des délais applicables. Il faut rappeler qu'un contrat d'assurance « cyber » peut couvrir l'entreprise sur trois volets principaux : les frais de réponse à incident, de gestion de crise et les frais supplémentaires induits par la poursuite de l'activité durant le sinistre, tels que la location d'équipements informatiques, le recours à des sous-traitants, etc.

Au-delà des aspects sécuritaires et juridiques, l'organisation victime d'une fuite d'information doit gérer sa communication. Là encore, la gestion d'une crise nécessite d'anticiper cet exercice et de préparer en amont les moyens de communiquer avec discernement auprès des autorités publiques, des partenaires, des clients et des médias.

En conclusion, la sécurité et la solidité de l'entreprise reposent en grande partie sur son système d'information. Le régulateur développe un système réglementaire pour renforcer cette sécurité. L'entreprise, au-delà de la conformité à des obligations légales, a intérêt à s'investir dans la sécurité de l'information. La prévention des fuites de données et l'anticipation des incidents s'inscrivent dans le principe vertueux de *security by design*.

Une meilleure
cyberprévention pour les enfants scolarisés

Par Loïc Baras

Février 2018, les parents de Léa[1], 15 ans, remarquent un changement dans le comportement de leur fille : elle ne mange plus, dort mal et se renferme sur elle-même. Léa finit par leur confier que des élèves l'injurient dans un groupe Snapchat depuis plusieurs semaines… Ce cas, répertorié parmi tant d'autres dans les brigades de gendarmerie, illustre le cyberharcèlement dont sont victimes les adolescents via les réseaux sociaux.

(1) Le prénom et la date ont été modifiés.

LOÏC BARAS

Colonel de Gendarmerie Commandant le groupement de gendarmerie départementale des Yvelines.

Le cyberharcèlement, premier risque pour l'enfant connecté

Le cyberharcèlement comprend l'usage de courriels, d'Internet, de SMS, des réseaux sociaux, chats, de téléphones portables pour harceler, humilier, répandre des rumeurs et ostraciser[2]. On considère qu'il y a cyberharcèlement -et non seulement cyberviolence- quand la victime fait l'objet d'attaques perpétrées au moins une fois par semaine et pendant un mois.

(2) Patchin, J., & W., Hinduja, S. (2006). Bullies Move beyond the Schoolyard: A preliminary look at cyberbullying. Youth Violence and Juvenile Justice, 4 (2), 148-169

D'après l'UNESCO[3], « entre 2010 et 2014, la proportion d'enfants et d'adolescents âgés de 9 à 16 ans ayant été exposés au cyberharcèlement [est] passé de 8 à 12 %, en particulier chez les filles et les enfants les plus jeunes. »

(3) Rapport sur le harcèlement scolaire dans le monde, UNESCO, 22/01/2017

Entre 2016 et 2017, le Centre de lutte contre les criminalités numériques (C3N) de la gendarmerie nationale a noté une hausse de 30 % des infractions en ligne sur le territoire français[4].

(4) État de la menace liée au numérique en 2018, ministère de l'Intérieur, mai 2018.

D'après les études menées par la chercheuse Catherine Blaya[5], 41 % des victimes ont déjà fait l'objet de cyberviolences et 7 % de cyberharcèlement.

(5) Catherine Blaya, « Étude du lien entre cyberviolence et climat scolaire : enquête auprès des collégiens d'Île de France », Les dossiers des sciences de l'éducation, 33|2015, 69-90

Selon l'association française de protection de l'enfance sur Internet e-Enfance -dont Catherine Blaya est administratrice- seulement 10 % des enfants victimes de cyberharcèlement en parlent à leurs parents[6]. L'ampleur du phénomène est donc bien supérieure aux plaintes reçues par les forces de l'ordre.

(6) https://www.e-enfance.org

En France, l'âge du premier accès à Internet se situe aux alentours de 9 ans et ne cesse de diminuer. Rapidement, l'enfant est équipé d'un outil numérique personnel : ordinateur, téléphone portable ou/et tablette. Le cyberharcèlement est identifié comme le risque le plus important auquel un enfant est exposé lorsqu'il est sur Internet. Les premiers adultes qui prodiguent aide et conseils en matière de sécurité sur Internet sont les parents (60 %) puis les enseignants (43 %) et enfin les pairs (26 %).

La prévention du cyberharcèlement, un enjeu pédagogique

Devant ce constat, les pouvoirs publics ne restent pas inactifs : depuis cinq ans, le Permis Internet sensibilise chaque année la plupart des enfants de CM2 et leurs parents à un usage d'Internet vigilant, sûr et responsable.

Si le Permis Internet s'adresse aux enfants du primaire, aucun outil pédagogique comparable n'existe encore pour les collégiens, qui découvrent en général les réseaux sociaux à ce moment de leur scolarité.

(7) Étude comScore Cross-platform-Future in Focus

Par ailleurs, le foisonnement des divers réseaux sociaux peut être perçu comme un obstacle pour les adultes qui sont en charge des actions de sensibilisation. Ainsi, des décalages d'usage des réseaux sociaux entre les adultes (les parents, les gendarmes spécialisés dans la prévention de la délinquance, les personnels de l'Éducation nationale) et les adolescents sont observés, dans un contexte d'évolution rapide des applications utilisées. À titre d'illustration, la moitié des utilisateurs de Snapchat sont âgés de moins de 24 ans, quand plus des deux tiers des utilisateurs de Facebook ont plus de 35 ans[7].

Le sujet de la cyberprévention s'articule ainsi entre des adolescents, ignorant ou sous-estimant les risques et les droits associés aux réseaux numériques, et des adultes appréciant mal les possibilités d'usages offertes aux utilisateurs de réseaux sociaux qu'ils ne connaissent pas.

La gendarmerie nationale dispose de la connaissance des risques, des dangers et des pratiques déviantes auxquels le public peut être confronté sur les réseaux sociaux. Pour promouvoir une « tranquillité numérique », nombre d'initiatives locales ont pu voir le jour dans les unités de gendarmerie, selon les besoins identifiés, les expériences, les compétences et centres d'intérêt des intervenants.

Notre projet est de proposer aux formateurs un outil pédagogique fiable, efficace et moderne, que les adolescents s'approprieront.

L'innovation pédagogique retenue

Smart Hands-on (SHO) est une start-up de la French Tech qui propose une plateforme d'apprentissage par le jeu. Ce procédé favorise la mémorisation et l'engagement des apprenants. Un processus de consolidation des acquis est développé grâce à une pédagogie innovante basée sur l'intelligence collective, le challenge, dans une mécanique ludique[8]. Les techniques proposées pour favoriser la mémorisation se basent sur des publications récentes en matière de neurosciences, comme l'ancrage mémoriel. Celles-ci démontrent que les leviers d'efficacité de l'apprentissage reposent sur des facteurs indispensables que l'on retrouve dans chaque expérience de jeu[9] :

- L'attention : Motiver pour garder le participant à bord,
- Les sens : Ancrer l'apprentissage en l'associant avec un ou plusieurs sens,
- Les émotions : Associer une émotion pour rendre l'expérience mémorable,
- La disponibilité : Limiter les informations pour éviter les surcharges,
- La consolidation : Répéter les exercices pour les entériner.

Sur les 12 derniers mois et un panel de 3 200 apprenants (thématiques variées), la plateforme Smart Hands-on affiche un taux d'engagement de 80 %, un taux de complétion de 93 % et un taux de satisfaction de 97 % des utilisateurs.

Un partenariat gagnant-gagnant

L'équipe projet s'est constituée en mai 2018 et fédère l'association e-Enfance, la brigade de prévention de la délinquance juvénile de la gendarmerie des Yvelines et la start-up SHO.

Ces trois structures sont très complémentaires.

L'association e-Enfance possède une expertise reconnue en matière d'usages numériques des mineurs, plus particulièrement de cyberharcèlement, notamment via sa plateforme : Net Écoute 0800 200 000. Elle est agréée par le Ministre de l'Éducation nationale pour ses actions de prévention. Son statut d'association reconnue d'utilité publique lui permet de bénéficier de

(8) Pour en savoir plus sur les mécaniques ludiques : http://www.cirta.org/index.php/50-banque-de-textes-actes-colloque-2016

(9) https://www.smart-handson.com

subventions publiques et de mener à bien la réalisation du projet.

La gendarmerie des Yvelines dispose quant à elle de gendarmes habitués au contact avec les jeunes et les établissements scolaires par le biais d'un réseau de proximité œuvrant quotidiennement dans le domaine de la prévention de la délinquance juvénile. La structure nationale de la gendarmerie permet d'envisager un déploiement rapide et fiable avec des intervenants formés.

La start-up SHO maîtrise l'animation de projets en mode agile et apporte son expérience pour consolider les acquis à travers une application ludique et engageante.

© Gendarmerie nationale

Une tablette numérique connectée est un vecteur naturel pour placer l'enfant et l'adolescent dans une attitude réceptive.

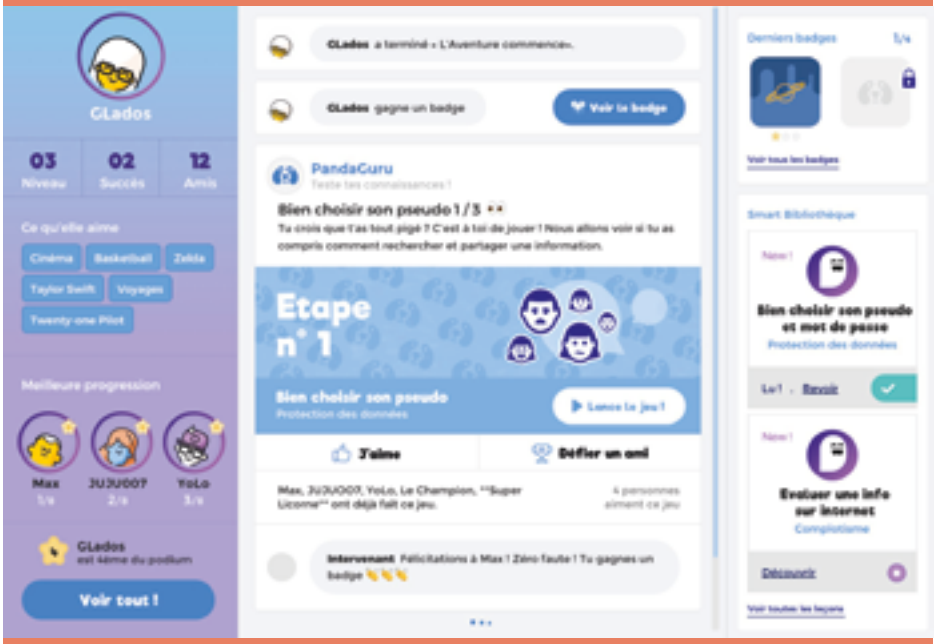
Plusieurs bénéfices sont attendus de ce partenariat : la mise à disposition d'une application avec des contenus élaborés par une équipe pluridisciplinaire, une approche pédagogique mettant l'adolescent au centre de l'apprentissage par le biais d'une tablette numérique connectée (permettant une meilleure appropriation) et une valorisation de l'intervenant, qui se consacre à l'animation de la séance autour des points d'attention qui seront apparus au cours des jeux.

Un contenu pédagogique ciblé

Concrètement, la plateforme reprend l'univers des réseaux sociaux avec des références d'identité graphique à Snapchat, Facebook et Instagram. L'interface est évolutive avec un concept de « libération de la parole » entre les équipes et l'attribution d'avatars. Une expérience utilisateur simple est recherchée, avec un accès direct à l'ensemble des éléments (badges, classement, bibliothèque intelligente), directement sur l'écran principal de la tablette.

Trois thèmes sont retenus pour la première version de l'application, avec les contenus pédagogiques suivants :

– **Cyberharcèlement :** Sur la base de cas issus de Net Écoute pour ancrer les jeux dans le réel, une approche selon les trois points de vue (le harceleur/le harcelé/le témoin) est utilisée. L'objectif est de savoir reconnaître les signes témoignant d'une situation de harcèlement et comment réagir.
– **Complotisme :** Les élèves sont invités à comprendre le complotisme par une expérience ludique en étant confrontés aux biais cognitifs auxquels les théories du complot font appel pour convaincre



© SHO

Une interface évolutive et ancrée dans l'univers des réseaux sociaux facilite l'ancrage de l'utilisateur dans un processus pédagogique.

les plus crédules. Les thématiques abordées sont « savoir partager ou non une information », « évaluer sa fiabilité » et « savoir rechercher l'information ».

– **Protection des données :** mise en situation de captation de données pour prendre conscience de leur valeur et de la nécessité de les protéger. Les bonnes pratiques de protection seront abordées.

Déploiement de l'expérimentation

Prenant son origine dans les Yvelines, le projet sera expérimenté dans ce département pour l'année scolaire 2018-2019, dans un panel de collèges, en zones urbaine, périurbaine et rurale. Les séances seront animées par des formateurs de la gendarmerie nationale, de la police nationale et de l'association e-Enfance. Cette dernière assurera la formation initiale des formateurs gendarmerie et police à la prise en mains de l'application et à l'animation pédagogique d'une séance de prévention. L'objectif visé est d'étendre cette application à l'ensemble du territoire national pour la rentrée 2019.

L'ASSOCIATION E-ENFANCE

Les professionnels d'e-Enfance interviennent toute l'année, dans toute la France, auprès d'élèves dans les établissements scolaires (100 000 par an), auprès des parents et des professionnels. Les équipes sont formées, encadrées et qualifiées pour intervenir et s'adaptent à chaque public.
Les missions :
- sensibiliser les jeunes, les parents et/ou les professionnels aux pratiques responsables d'utilisation du numérique, qu'il s'agisse d'internet, des réseaux sociaux ;
- leur expliquer comment réagir face aux risques potentiels d'Internet dans une démarche d'acquisition de compétence pour une meilleure maîtrise des usages.
L'Association e-Enfance est reconnue d'utilité publique, agréée par le Ministère de l'Éducation Nationale et elle reçoit le soutien du CIPDR et de la DILCRAH. Elle opère le numéro national pour la protection des mineurs sur Internet NET ÉCOUTE 0800 200 000 dans le cadre du programme Safer Internet de la Commission européenne.

LE GROUPEMENT DE GENDARMERIE DES YVELINES

La gendarmerie nationale intègre, dans sa stratégie de sécurité, la prévention de la délinquance comme un des leviers d'action majeurs pour lutter contre la commission des crimes et des délits, en amont du passage à l'acte.
La chaîne de prévention de la délinquance au niveau du département s'articule autour de deux acteurs essentiels :
- l'officier adjoint prévention de la délinquance (OAP), placé au niveau départemental, qui anime la chaîne de prévention, notamment la brigade de prévention de la délinquance juvénile, et assure le lien avec les partenaires identifiés,
- les correspondants territoriaux prévention de la délinquance (CTP), désignés dans chaque brigade ou communauté de brigades, qui participent à la conception, à l'animation et au suivi du service dans ce domaine au niveau local, en veillant à développer les contacts de proximité.Internet de la Commission européenne.

LA START-UP SHO

Smart Hands-on est une plateforme d'apprentissage par la pratique qui permet développer ses talents en s'appuyant sur les mécanismes du jeu. Elle met en œuvre une pédagogie innovante qui est basée sur l'intelligence collective, la pratique et l'immersion. Un processus de consolidation des acquis est développé à travers 3 leviers : la pratique en groupe, les apprentissages courts et ludiques et la recommandation pertinente et ciblée de documentation théorique.

L'AUTEUR

Le colonel Loïc Baras commande le groupement de gendarmerie départementale des Yvelines depuis 2016. Diplômé de l'ESM St-Cyr en 1997, il a alterné des postes de commandement en unités opérationnelles, en métropole et outre-mer, et des fonctions de conception et de direction de haut niveau en administration centrale.

La France face au défi

de la protection des mineurs sur Internet
Mieux protéger les professionnels de terrain pour mieux protéger les victimes

Par Pauline Sêtre et Quentin Aoustin

Réalité déplorable et alarmante, la France est le 4e plus gros hébergeur mondial[1] de contenus d'abus et d'exploitation sexuels sur mineurs. En 2017, ce sont 13 263 publications hébergées sur son sol qui ont été qualifiées comme manifestement illicites par l'association Point de Contact. Services de police et de gendarmerie, associations et professionnels du secteur éducatif, doivent plus que jamais s'investir pour la protection des mineurs sur Internet, le rendre plus sûr, et apprendre aux plus jeunes à y naviguer en toute sécurité.

(1) Classement issu des statistiques du réseau INHOPE http://inhope.org/Libraries/2017_stats/CSAM_hosting.sflb.ashx http://inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2017.aspx

QUENTIN AOUSTIN

Directeur des Opérations à Point de Contact

PAULINE SÊTRE

Responsable Hotline au sein de Point de Contact

(2) https://www.pointdecontact.net/cliquez-signalez/

L'équipe de *Point de Contact* apporte son concours à cet effort en mettant à disposition des internautes un formulaire de signalement en ligne[2] et, très prochainement, des modules complémentaires de signalement directement intégrés aux différents navigateurs existants dont Tor. Son action se matérialise par un traitement quotidien des signalements qu'elle reçoit, en coopération avec les autorités et les hébergeurs.

Point de Contact : un engagement collectif pour protéger l'enfance

(3) https://www.pointdecontact.net/

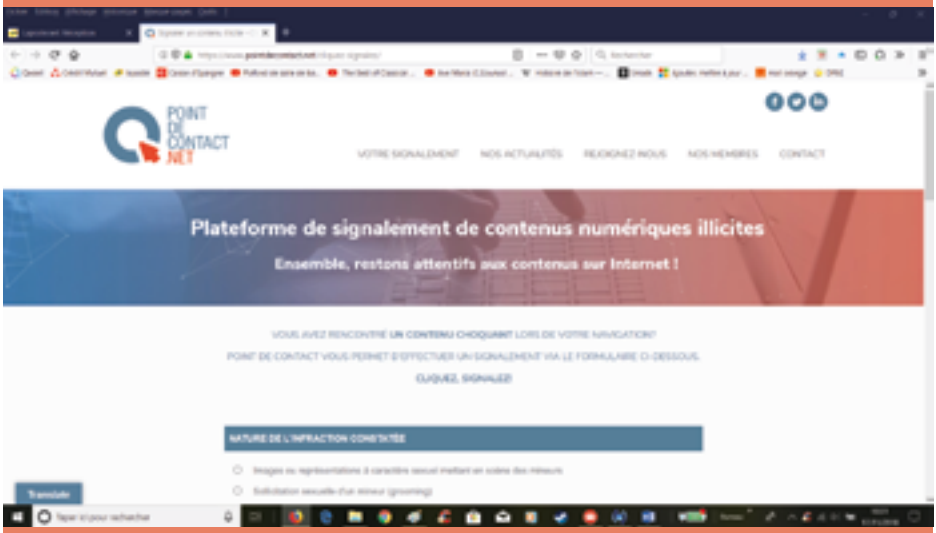
Point de Contact[3], association loi 1901, a été créée en 1998 avec pour ambition de lutter contre la prolifération des contenus illicites accessibles à tous sur la toile. Pour ce faire, elle offre aux internautes la possibilité de lui soumettre les liens vers les contenus choquants rencontrés lors de leurs navigations. Ainsi, faisant d'eux de véritables acteurs de la lutte contre la diffusion de ces contenus, elle place les signalants au cœur de son dispositif dédié à rendre l'Internet plus sécurisé.

(4) https://www.pointdecontact.net/#!/nos_membres

L'association bénéficie du soutien de nombreux acteurs privés (fournisseurs d'accès à Internet, hébergeurs, plateformes Web et réseaux sociaux, fournisseurs de solutions technologiques) et publics, notamment la Commission européenne à travers le programme *Safer Internet*.[4]

La protection de l'enfance en ligne au cœur de son champ de compétence

Son champ d'action permet de mettre les compétences de ses analystes à l'épreuve de divers types de contenus. Abus et exploitation sexuels d'enfants, contenus choquants accessibles aux mineurs, incita-



Extrait de l'écran d'accueil de la plateforme de signalement.

© Association point contact

tion à la violence, à la discrimination ou à la haine, harcèlement sexuel, provocation au terrorisme ou à la fabrication de bombes, provocation au suicide et proxénétisme forment l'éventail de publications qui regardent son domaine d'activité.

(5) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418095

Mais, parce que les images, vidéos et représentations d'abus et d'exploitation sexuels de mineurs en ligne sont ceux qui lui sont signalés en plus grand nombre par le public et par les autres organismes de signalement de contenus dans le monde, sa principale compétence réside dans la lutte contre leur prolifération. En 2014, 1 897 contenus sont qualifiés comme manifestement illicites au regard de l'article 227-23 du Code pénal[5]. Depuis, ce chiffre augmente de façon constante : 4 875 contenus en 2015, 7 341 en 2016, et 13 263 en 2017.

(6) Classement issu des statistiques du réseau INHOPE http://inhope.org/Libraries/2017_stats/CSAM_hosting.sflb.ashx http://inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2017.aspx

La France, et c'est ce qui explique en partie l'augmentation de ces chiffres, est l'un des pays qui héberge le plus de contenus d'abus et d'exploitation sexuels de mineurs en Europe et dans le monde[6]. À l'échelle mondiale, avec 7 % des contenus hébergés, elle se place en quatrième position après les États-Unis (43 %), les Pays-Bas (19 %) et la Fédération de Russie (7 %). Au niveau européen, elle arrive en deuxième position (18 %) après les Pays-Bas (51 %). Néanmoins, le travail de notification et de retrait de ces contenus fonctionne sans entrave auprès des hébergeurs français, ce qui permet d'endiguer leur multiplication.

Ses partenaires acteurs de la protection des mineurs en ligne

L'association travaille en coopération avec de nombreux acteurs de la protection de l'enfance en ligne : au niveau national avec le *consortium Safer Internet France et international* avec le réseau INHOPE.

Safer Internet France

(7) https://www.e-enfance.org/

(8) http://www.internetsanscrainte.fr/

(9) http://www.saferinternet.fr/

Point de Contact travaille en étroite coopération avec les associations *e-Enfance*[7] et Internet Sans Crainte[8] dans le cadre du programme européen Safer Internet[9] : *e-Enfance* met à disposition des jeunes une ligne d'écoute, *NetEcoute*[10], qui est le numéro vert national au service des enfants et adolescents mis en difficulté dans leurs usages d'Internet alors qu'*Internet Sans Crainte* œuvre à la sensibilisation des jeunes, des parents, et des professionnels de l'éducation, aux thématiques du monde numérique. Écoute, sensibilisation et signalement sont donc les trois pôles de ce consortium dédié à la protection de l'enfance en ligne.

(10) https://www.netecoute.fr/

Écran d'accueil de la plateforme Internet sans crainte.

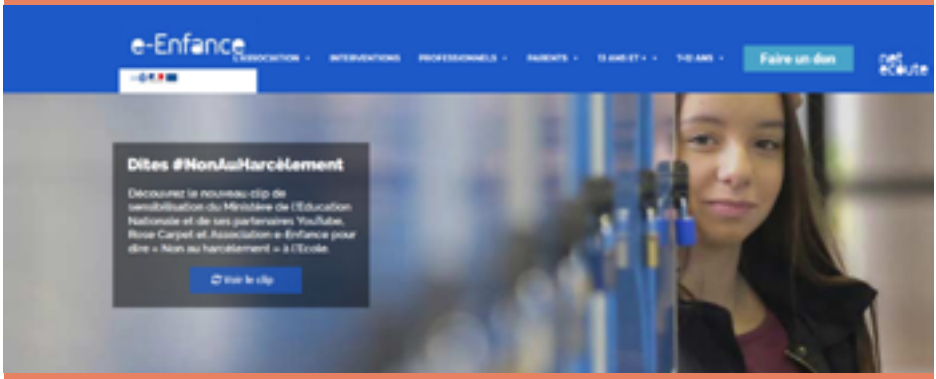
La synergie de ces trois organisations permet de faire face aux risques encourus par les mineurs sur Internet à travers, notamment, une communication conjointe permettant d'accroître la visibilité des trois services auprès des jeunes, et un partage de connaissances et de compétences.

INHOPE

(11) http://inhope.org/gns/home.aspx

Le réseau international INHOPE[11], dont *Point de Contact* est membre fondateur, a pour engagement d'éradiquer les contenus d'abus et d'exploitation sexuels de mineurs diffusés sur la toile. Pour ce faire, il réunit 45 membres dans 40 pays en Europe, Amérique, Asie et Afrique, à qui il offre une plate-forme collaborative pour mieux lutter contre ces publications. Grâce à ce dispositif, chaque membre, désigné sous le nom générique de « hotline », peut envoyer les URL qu'il reçoit au pays dans lequel elles sont hébergées. Les infractions en ligne étant un phénomène international par nature, il est essentiel d'impliquer le plus possible de nations dans leur traitement. C'est pourquoi INHOPE s'attache aussi à soutenir et accompagner la création de nouvelles hotlines dans les pays où une telle initiative n'existe pas encore.

Lorsque les analystes constatent qu'une URL présente un ou des contenus d'abus ou d'exploitation sexuelle de mineurs



Écran d'accueil du site Internet e-enfance.org.

manifestement illicites au regard de la loi française (images, vidéos ou représentations), celle-ci est transmise aux autorités françaises via la plateforme PHAROS[12] avec toutes les informations pertinentes pouvant faciliter son traitement et sa qualification juridique : IP, hébergeur, localisation du serveur, mot de passe pour les archives chiffrées, procédure particulière pour accéder aux contenus, etc.

(12) Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Signaler-un-contenu-suspect-ou-illicite-avec-PHAROS

Les contenus hébergés en France sont directement notifiés aux hébergeurs afin de leur permettre de procéder au retrait. Ils sont indirectement signalés aux hébergeurs étrangers grâce à la base de données du réseau international INHOPE qui alimente elle-même la base de données ICSE[13] d'Interpol. Les services de l'organisation policière internationale prennent en charge l'identification des victimes et de leurs agresseurs, en renfort du travail des forces nationales de police.

(13) https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification

Si le retrait n'est pas obtenu dans le pays hébergeur, PHAROS peut, grâce une compétence exclusive, procéder au blocage administratif du contenu qui sera, par conséquent, inaccessible via les fournisseurs d'accès à Internet français. La procédure de blocage administratif se fait sous le contrôle de la personnalité qualifiée de la CNIL[14].

(14) Commission nationale de l'informatique et des libertés https://www.cnil.fr/fr/controle-du-blocage-administratif-des-sites-la-personnalite-qualifiee-presente-son-3eme-rapport

Carte des pays participant à la Hotline INHOPE

© INHOPE

Point de Contact : un engagement pour la protection des professionnels exposés aux contenus choquants

Le retrait des contenus d'abus sexuels sur mineur est essentiel pour la protection des victimes, pour l'identification de celles qui ne sont pas encore connues ainsi que de leurs agresseurs. Il intervient également dans la prévention de la délinquance des internautes qui en font la consommation. Cependant, même si le professionnel, qui contribue à cette mission d'intérêt public, peut se sentir par là même utile, cela ne peut en soi suffire à donner un sens à son action et à éviter les risques psychosociaux. Il faut protéger les personnels, ainsi que ceux qui les côtoient au sein de l'entreprise, à travers la mise en place de bonnes pratiques.

L'environnement et les conditions de travail

C'est d'abord un environnement de travail adapté qui permet aux professionnels exposés à ces contenus de travailler dans des conditions propices à réduire le stress qui pourrait les affecter. Nous veillons à ce que ces personnels ne soient pas seuls lorsqu'ils procèdent à la constatation et au traitement de ces contenus. Un espace de détente est aménagé en dehors du lieu où les contenus sont analysés afin de permettre aux salariés de changer d'environnement. Ils sont également encouragés à faire des pauses régulières lorsque le besoin s'en fait ressentir.

L'espace de travail est par ailleurs pensé pour que ceux qui peuvent se trouver dans les locaux, non habilités à travailler

avec ces contenus, n'y soient pas exposés. Nous nous attachons néanmoins à ce que la protection renforcée de cet espace n'entraîne pas pour autant un isolement total au sein de la structure et que les salariés ne s'y sentent pas reclus.

Point de Contact travaille également au développement d'outils technologiques tels que la reconnaissance d'image. Sans espérer pouvoir se passer complètement de l'œil humain, l'association mise sur ces développements pour soutenir le travail d'analyse et alléger le processus de prise de décision. Il s'agit notamment de simplifier les procédures en limitant le caractère répétitif de certaines tâches grâce à leur automatisation. L'utilisation de ce type de technologies vise également à limiter la surexposition des analystes à des contenus déjà connus et qualifiés comme manifestement illicites.

Le suivi psychologique des professionnels exposés

Les métiers nécessitant une exposition régulière à des contenus d'abus et d'exploitation sexuelle d'enfants sont récents et continuent de se professionnaliser. Les conséquences psychologiques potentielles sont encore mal connues. C'est pourquoi Point de Contact porte une attention toute particulière à l'équilibre psychologique et au bien-être de son équipe.

C'est au moment du recrutement qu'une première évaluation se fait pour apprécier les capacités d'une personne candidate à assumer un tel travail. L'avis du psychologue est un indicateur important pour orienter la décision finale. Ensuite, pendant toute la période de travail, un suivi psychologique régulier est assuré tout au long de l'année pour tous les analystes, quelle que soit leur ancienneté. Nous encourageons les analystes à consulter, en dehors du suivi obligatoire, dès que le besoin s'en fait ressentir.

Nous insistons auprès des salariés sur le fait que demander un entretien psychologique ne doit jamais être considéré comme un aveu de faiblesse ou un indicateur d'incapacité. Bien au contraire, l'expérience montre que savoir identifier les moments où son équilibre peut être menacé, et prendre l'initiative d'en prévenir le risque, permettent de pouvoir poursuivre sa mission dans de bonnes conditions.

La prise en considération du bien-être des personnels demande un effort et une remise en question constante. C'est pourquoi, après avoir participé à sa création en 2014, *Point de Contact* est directement associé à la réactualisation d'un livre blanc, fruit d'une réflexion commune des secteurs public et privé, sur les bonnes pratiques en matière de traitement des signalements de contenus d'abus sexuels sur mineurs et de propagande terroriste. Un développement approfondi sera consacré à la protection des profes-

sionnels exposés à ces publications. Le ***Forum International de Cybersécurité 2019*** a été choisi pour en annoncer la publication.

L'AUTEUR

Quentin Aoustin, directeur des Opérations à Point de Contact, œuvre depuis plus de 10 ans dans le domaine de la cybercriminalité. Diplômé en droit des nouvelles technologies – Université de Paris X – il est titulaire d'un diplôme de second cycle en informatique – Université de Montpellier.

L'AUTEURE

Pauline Sêtre est responsable Hotline au sein de Point de Contact. Elle est diplômée du Master 2 Professionnel MSI « Droit du Multimédia et des Systèmes d'Information » - Université de Strasbourg.

Les fichiers de sécurité : une exigence d'efficacité et une obligation de conformité

Par Mark Evans

Les nouveaux enjeux de sécurité ont sensiblement modifié le débat sur les fichiers de sécurité. Il est désormais admis que pour protéger un territoire sur lequel pèse une menace terroriste et criminelle élevée, tout en préservant les libertés fondamentales, les forces de l'ordre doivent nécessairement mettre en œuvre des traitements de données à caractère personnel. Si la vigilance est toujours de mise à l'égard des fichiers, c'est aussi leur efficacité qui intéresse aujourd'hui l'opinion publique.

MARK EVANS

Lieutenant-colonel de gendarmerie
Chef du département de la protection et de la gouvernance des données
Direction générale de la gendarmerie nationale

Dans le même temps, le « droit des fichiers » a considérablement évolué en faveur de la protection des données. Les fichiers de sécurité seront toujours un sujet sensible politiquement, le moindre soupçon d'irrégularité pouvant engendrer la défiance des citoyens et de leurs représentants. C'est bien dans l'objectif de concilier le devoir d'efficacité avec l'obligation de conserver la confiance des usagers que la gendarmerie nationale a entrepris d'obtenir le Label « gouvernance informatique et libertés » proposé par la CNIL.

Le défi ne porte plus tant sur la déclaration des fichiers que sur la conformité de leur mise en œuvre.

Les fichiers de la « sphère pénale », mis en œuvre par les forces de sécurité intérieures, n'entrent pas dans le champ du règlement européen relatif à la protection des données (RGPD) mais dans celui de la directive européenne 2016/680 associée. Elle a été transposée dans le droit national par la loi relative à la protection des données personnelles du 20 juin 2018, modifiant la loi dite « informatique et libertés » du 6 janvier 1978. Les fichiers, dits « de souveraineté » et ayant pour finalité la sûreté de l'État, sont hors du

(1) En France, ces fichiers peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise ; seul le sens de l'avis de la CNIL est publié en même temps que le décret autorisant la dispense de publication de l'acte.

champ de la réglementation européenne[1]. Le paquet européen de protection des données substitue à une logique de formalité préalable une logique de conformité continue, par la responsabilisation renforcée des acteurs, responsables de traitement comme sous-traitants. Il ne prévoit pas de formalité déclarative préalable en dehors de l'obligation de tenir un registre des activités de traitement et de mener une analyse d'impact pour les traitements « à risque ». Pour les traitements entrant dans le champ de la directive, en revanche, la loi prévoit d'appliquer ces nouvelles obligations tout en maintenant le régime d'autorisation de mise en œuvre par acte réglementaire après avis publié de la CNIL.

Les enjeux de la conformité pour les forces de sécurité intérieure ne se situent donc pas tant sur les formalités de déclaration des traitements qui évoluent peu, que sur le respect des principes de gouvernance imposés par le RGPD et repris par la directive.

Responsabilité – accountability

La conformité s'acquiert désormais sur un spectre large de compétences : administration fonctionnelle et technique des traitements, sécurité des données et gestion des incidents, gestion des droits des personnes concernées, formation des utilisateurs, doctrine d'emploi, sensibilisation des acteurs, contrôle interne, communication…

Le principe de responsabilité suppose de formaliser les procédures et d'historiser l'ensemble des actions afin que le responsable de traitement puisse rendre compte tout au long de la vie du traitement des mesures prises pour protéger les libertés individuelles. La DGGN s'est fortement inspirée du référentiel prévu par le label de la CNIL pour mettre en place une gouvernance des traitements rénovée. Une structure dédiée a été créée, le département de la protection et de la gouvernance des données (DPGD), avec pour mission d'animer et de coordonner la conformité dans toutes ses composantes, en liaison avec le responsable central de la sécurité des systèmes d'information (RCSSI), le service des technologies et des systèmes d'information de la sécurité intérieure (ST (SI)[2]) et le service de traitement de l'information gendarmerie (STIG) qui héberge la grande majorité des traitements, les responsables fonctionnels de traitements et enfin l'inspection générale de la gendarmerie nationale. Point de contact du délégué ministériel à la protection des données, le DPGD pilote en outre l'ensemble des accès aux fichiers par les gendarmes.

Respect de la vie privée dès la conception – privacy by design

L'analyse de conformité doit désormais être menée dès la phase initiale d'un projet de

traitement, jusqu'à son déploiement. La gouvernance des traitements de données à caractère personnel doit donc intégrer une procédure standardisée de conduite de projet jalonnée d'échelons de consultation et de validation et prévoyant une parfaite coordination des acteurs.

La gendarmerie a adopté une procédure bâtie sur une articulation précise entre les acteurs précités. Cette chaîne de compétences doit permettre d'évaluer la conformité du projet par une étude croisée de la légalité du traitement et de la sécurité des données.

L'étude de légalité passe nécessairement par une évaluation juridique initiale. En fonction des finalités identifiées et du type de données collectées, cette analyse préalable renseigne le responsable du traitement sur le cadre légal à envisager, celui-ci pouvant aller de la dispense de déclaration jusqu'au décret en Conseil d'État après avis publié de la CNIL, certains traitements pouvant également nécessiter de légiférer. Cette évaluation complète l'analyse de faisabilité et l'estimation des délais de mise en œuvre. En identifiant au plus tôt les points d'achoppement au regard du « droit des fichiers », le DPGD oriente et accompagne l'équipe projet pour trouver les équilibres entre différents paramètres : finalités, nature des données, durées de conservation, périmètre des accédants, mesures de sécurité, traçabilité des actions, droits des personnes concernées…

(2) S'inspirant initialement du guide d'intégration de la sécurité des systèmes d'information dans les projets de l'ANSSI et intégrant les exigences de la politique de sécurité des systèmes d'information de l'État.

Sur la base des résultats de l'évaluation initiale et de la démarche d'intégration de la sécurité dans les projets du ministère de l'Intérieur[2], une analyse d'impact est menée, pouvant revêtir un caractère formel lorsque le traitement est susceptible d'engendrer un risque élevé.

L'étude de sécurité est intégrée à la chaîne de conformité. Elle répond aux mêmes principes d'évaluation préalable et continue pour aboutir, suivant une démarche adaptée au degré de sensibilité du traitement, à une homologation de sécurité.

Le *privacy by design* fait des garants de la conformité des partenaires des équipes « projet ». Cet accompagnement suppose une parfaite compréhension du besoin et donc des connaissances « métier » solides.

La conformité doit accompagner la modernisation des systèmes et l'innovation.

L'enjeu pour les forces de sécurité intérieure est de s'adapter au nouveau paradigme de la conformité tout en conservant sa capacité à faire évoluer les fichiers rapidement au gré des innovations technologiques et des évolutions de la menace.

Les fichiers entrant dans le champ de la directive sont soumis à des formalités déclaratives qui s'étendent sur plusieurs

mois. Toute modification substantielle de ces traitements engendre un nouveau cycle de déclaration. Or, le nombre des projets de traitements, comme le rythme de leurs évolutions, va croissant. Pour préserver la réactivité des services, il importe de délimiter plus précisément le champ d'application de la directive en retenant la définition la plus ajustée.

Il est défini par la finalité des traitements et non par la nature des données qui y sont contenues. Aussi se limite-t-il aux traitements dont le périmètre fonctionnel comprend les enquêtes judiciaires et la prévention des atteintes à la sécurité publique.

Il faut noter que les forces de sécurité intérieure utilisent également des traitements visant à améliorer la sécurité des citoyens sans pour autant relever de la directive. Une grande part de leur activité est tournée vers la sécurité dite « du quotidien » qui s'apparente à des prestations de service public « ordinaires » nonobstant la qualité des agents et des militaires qui l'exercent (prévention, accueil du public, services numériques divers à destination des usagers…). De surcroît, la dispense d'acte réglementaire ne se fait pas au détriment de la sécurité des données puisque l'analyse d'impact reste de rigueur, en particulier pour les traitements susceptibles de contenir des données sensibles.

En second lieu, le besoin est avéré de disposer d'un régime dérogatoire, dispensé d'acte réglementaire préalable mais soumis à des standards de sécurité particulièrement exigeants, pour mettre en œuvre temporairement et en transparence avec les autorités de contrôle des traitements expérimentaux, aux fins de valoriser les données collectées pour une meilleure analyse des phénomènes.

Le RGPD accorde aux États la possibilité d'adopter un régime particulier pour les traitements à finalité de recherche scientifique.

La loi du 20 juin 2018 autorise sous certaines conditions un traitement ultérieur de données à des fins de recherche scientifique s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées. Toutefois, les modalités d'application de cette disposition aux fichiers de sécurité mériteraient d'être éclaircies et assouplies.

Engagée dans une profonde transformation numérique, la gendarmerie a fait le choix de la transparence sur sa gouvernance des traitements de données à caractère personnel. Conserver la confiance des citoyens, des autorités de contrôle et du législateur sera en effet indispensable pour relever les défis à venir en matière de biométrie, de modernisation des fichiers et d'exploration des sciences de la donnée, en particulier dans le champ de l'intelligence artificielle. Isabelle Falque-Pierrotin, présidente de la CNIL, déclarait récemment que la conformité au RGPD pouvait

devenir un argument concurrentiel en faveur des entreprises. La conformité à la directive pourrait bien devenir un vecteur de performance pour les forces de sécurité intérieure.

L'AUTEUR

Officier de gendarmerie, Mark Evans dirige le département de la protection et de la gouvernance des données à la DGGN. Il a alterné des postes opérationnels dans la filière aéronautique, d'abord dans l'aviation légère de l'armée de terre puis au sein des forces aériennes de gendarmerie, et des commandements en gendarmerie départementale à Versailles et à Évry. Saint-cyrien de formation, breveté de l'école de guerre en 2013, il rejoint la DGGN en 2016, d'abord comme chargé de projet « fichiers » au sein de la direction des opérations et de l'emploi, ensuite comme chef de département au sein de la mission du pilotage et de la performance.
Il est également l'auteur d'une publication dans la Revue sur le thème de l'emploi des drones pour les missions de sécurité publique.

LA BLOCKCHAIN RIME-T-ELLE AVEC LA SÉCURITÉ ET LA CONFIDENTIALITÉ ?

La blockchain consacre une nouvelle organisation de registres distribués qui offre, en principe, l'assurance que la base de données est protégée de toute manipulation.

Les registres distribués présentent toutefois un certain nombre d'inconvénients en termes de confidentialité et de sécurité. Des erreurs dans les développements, une fragilité des infrastructures physiques, une protection imparfaite des clés de chiffrement ou une sécurisation insuffisante de l'exécution automatique de contrats sont autant de vulnérabilités.

On ne peut occulter des problématiques de confidentialité du fait de la pseudonymisation des données. Des outils permettent de reconstituer des historiques de transactions illicites ou d'extraire des métadonnées voire d'identifier des récurrences. Par contre, les registres distribués ont le potentiel de suivre des objets individuellement et d'augmenter leur traçabilité en véhiculant des certifications et des propriétés de produits ou en permettant de les localiser.

Blockchain :
Sécurité et Confidentialité

Par Gilles Hilary

La technologie dite de la « blockchain » est apparue en 2008 pour permettre la création d'une crypto-monnaie, le *Bitcoin*. Il est important de souligner que cette technologie, indépendante de son utilisation initiale, permet aujourd'hui (et encore plus demain) de nombreuses autres applications. Toutefois, les spécificités du *Bitcoin* ont coloré la perception de la *blockchain*.

Blockchain et registres distribués

GILLES HILARY

Professeur d'université Georgetown University
Chercheur associé CREOGN

La *blockchain* fait partie d'une classe de technologies plus large appelée « registres distribués ». Il s'agit essentiellement d'une nouvelle organisation de base de données. Le concept initial a émergé dans les années 1960 autour d'une structure centralisée. Dans ce paradigme, il existe une version unique de la base active (qui peut cependant être copiée). Cette approche est aujourd'hui mature et appropriée pour de nombreuses applications. Toutefois, la concentration sur une machine unique fait que la base est inopérante, voire détruite, si cette machine n'est plus en état de fonctionner. Pour atténuer ce problème, les bases de données distribuées sont dispersées sur plusieurs serveurs. Elles offrent ainsi une tolérance aux pannes (***fault tolerance***).

Les registres distribués (comme la *blockchain*) vont plus loin. Dans l'approche traditionnelle, le propriétaire de la base contrôle les données qui y sont stockées. Sa prise de contrôle permet des manipulations potentiellement indétectables. Les utilisateurs doivent donc avoir confiance dans le maintien de l'intégrité de la base par son propriétaire en toutes occasions. Les registres distribués offrent, au moins

en principe, l'assurance que la base de données est protégée de toute manipulation. On parle alors de résistance byzantine aux failles (*byzantine fault tolerance*).

© Blockchain concept banner. Par AndSus

La sécurité des blocs repose sur leur appariement crypté, leur essaimage sur des sites différents avec des mises à jour simultanées.

Dans le cas de la *blockchain*, il y a deux éléments centraux. Les données sont conservées dans des « blocs » liés entre eux par des éléments cryptographiques dans une chaîne qui croît avec le temps. Par ailleurs, la base de données est répliquée sur plusieurs machines (dont le nombre peut être restreint ou élevé). Il est important de souligner qu'il ne s'agit pas de simples copies mais de multiples bases actives simultanément. Il est donc essentiel que ces différentes versions ne divergent pas sur le long terme. Pour empêcher cela, il existe un « mécanisme de consensus » qui les rapproche constamment. Dans le cas du *Bitcoin*, la machine (ou « nœud ») qui résout un problème mathématique (bien spécifique) en premier obtient le droit de graver le prochain bloc dans la version permanente de la base. Ce mécanisme, très consommateur en énergie, est toutefois spécifique au *Bitcoin*. La plupart des autres applications utilisent des mécanismes différents qui n'ont pas le même coût (mais peuvent présenter d'autres problèmes).

On distingue les *blockchains* publiques, que tous peuvent rejoindre, et les *blockchains* privées qui sont soumises à autorisation par les parties prenantes. La plupart des crypto-monnaies utilisent la première approche tandis que les chaînes logistiques utilisent plutôt la seconde. Dans ce dernier cas, seuls des fournisseurs accrédités peuvent participer à la *blockchain* avec des niveaux différents d'accès aux données en fonction de leur situation (par exemple, pour éviter que des concurrents puissent consulter des informations confidentielles).

Même si elle est plus ancienne, la technologie a réellement commencé à émerger ces deux dernières années. Elle est donc en pleine évolution et offre des capacités de traitement de l'information plus réduites que les bases centralisées. À ce jour, la finance et la logistique sont les secteurs où les applications sont les plus développées, même si beaucoup d'autres s'y intéressent.[1]

(1) Cf. "Distributed Ledgers and Operations", Babich et Hilary, Manufacturing & Service Operations Management, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3131250 pour la logistique, et "Blockchain and Finance", Hilary et Liu, Palgrave-MacMillan Handbook of Alternative Finance pour la finance.

Il faut souligner que, si la cryptographie est utilisée pour lier les blocs entre eux, l'information contenue dans ces blocs n'est pas nécessairement cryptée. De fait, les blocs peuvent simplement contenir un lien vers des données conservées à l'extérieur de la chaîne. Cette approche augmente la vitesse de traitement mais réduit la protection offerte par la *blockchain*. Ce lien externe peut être dynamique ou offrir une garantie (sous forme de « hash ») que l'information contenue en dehors de la chaîne n'a pas été modifiée ultérieurement.

Il est souvent considéré, à tort, que l'information dans une *blockchain* est immuable. Mis à part les cas de piratage et des erreurs de code, il existe au moins deux autres moyens de modifier ces données. La première possibilité est que les différentes parties prenantes décident collectivement de changer les propriétés de la chaîne. On parle alors de « fourche » (*hard fork*). Une deuxième possibilité développée plus récemment se base sur la technique dite des « *chameleon hashes* » qui permet la rédaction a posteriori de blocs si un certain nombre de conditions prédéfinies sont réunies.

Sécurité et Confidentialité

Les registres distribués présentent un certain nombre d'inconvénients en termes de confidentialité et de sécurité.

Sécurité

Il faut distinguer la chaîne proprement dite de son environnement immédiat. Le contenu de la chaîne semble relativement bien protégé à ce jour mais cette sécurité ne peut pas être absolue. Le développement d'applications pouvant nécessiter des millions de lignes de code, des erreurs ou des fautes intentionnelles est possible. Ce développement est souvent réalisé par des PME innovantes qui peuvent avoir des priorités autres que la sécurité. Par ailleurs, au moins un État non intégré à l'OTAN semble développer une politique d'infiltration systématique des comités techniques internationaux à des fins stratégiques.

Une autre vulnérabilité est la destruction de l'infrastructure physique des chaînes. Certaines sont tellement distribuées que cette situation est improbable. Toutefois, ce risque semble plus significatif pour les chaînes privées et même pour certaines chaînes publiques. Par exemple, NEO est une crypto-monnaie avec une valorisation théorique au-delà du milliard de dollars. Elle semble reposer sur une poignée de nœuds, tous sous le contrôle de l'entité fondatrice en Chine. Cette concentration peut aussi être exploitée pour prendre le contrôle du réseau au moyen de fausses identités (on parle alors d'attaque *Sybil*). Plus généralement, la *blockchain* est une technologie nouvelle et ses faiblesses n'ont peut-être pas encore été clairement identifiées. Les évolutions de la cryptographie à moyen terme, par exemple avec l'ordinateur quantique, peuvent avoir des implications mal comprises actuellement.

L'environnement de la *blockchain* est beaucoup plus fragile. Par exemple, les utilisateurs de crypto-monnaies utilisent des « portefeuilles électroniques » qui leur permettent de réaliser des transactions par l'intermédiaire de plateformes spécialisées. Les clés privées de chiffrement nécessaires pour ces opérations sont souvent mal protégées, soit par les utilisateurs finaux, soit par ces plateformes (il s'agit ici du cryptage des transactions stockées dans les blocs et non du cryptage des liens entre les blocs). Un second cas est l'exécution automatique de contrats sur la chaîne (*smart contracts*). Par exemple, une température peut déclencher le paiement d'une prime d'assurance. Toutefois, la mesure de cette température est faite hors chaîne et communiquée par un protocole (ou « oracle »). La manipulation de cette transmission est possible même si l'exécution des contrats elle-même est complètement sécurisée. Un troisième exemple est le piratage d'ordinateurs pour permettre la production sauvage de crypto-monnaies (les coûts sont supportés par la victime, les bénéfices revenant aux pirates).

Vie privée et confidentialité

Il faut distinguer « l'anonymisation » de la « pseudonymisation ». Cette dernière consiste en un traitement des données afin qu'il ne soit pas possible de les attribuer à une personne sans recourir à des informations supplémentaires (par exemple, en connaissant une identité numérique). L'anonymisation, quant à elle, est un processus qui empêche totalement et irréversiblement la possibilité d'identifier une personne. L'anonymisation est techniquement difficile, la plupart des informations stockées sur les *blockchains* sont donc au mieux pseudo-anonymes. Cela crée des problèmes de confidentialité mais offre *a contrario* des pistes d'audit pour les forces de l'ordre. Par exemple, la saisie d'ordinateurs peut permettre de reconstituer des historiques de transactions illicites. Par ailleurs, les ordinateurs qui exécutent les transactions sur les *blockchain*s ne sont normalement pas à même de lire les données. Toutefois, ils peuvent extraire des métadonnées (des données sur d'autres données) et identifier des récurrences empiriques importantes.

Les données ajoutées à la chaîne ne sont pas immuables mais sont difficiles à détruire. On peut imaginer que des copies (protégées par des techniques cryptographiques devenues obsolètes) se perdent. Cette difficulté d'effacement des données peut être aussi exploitée à des fins criminelles. Par exemple, la base *Bitcoin* contient des éléments pédopornographiques. Il est donc possible d'implanter, de façon presque définitive, des documents personnels ou illicites dans des *blockchains* publiques dans un but de chantage ou de diffusion.

Identité

Les registres distribués offrent aussi des avantages certains en termes de sécurité et de confidentialité même si on peut s'inter-

roger sur la question de la suppression des données à caractère personnel. Beaucoup de ces applications n'ont pas encore été déployées. En particulier, la *blockchain* peut faciliter la gestion des identités, aussi bien pour les individus que pour les machines. Ce point est important car, dans un monde interconnecté, la cyberdéfense est de plus en plus liée à l'identification. Par exemple, la gestion des objets connectés pourrait être facilitée par le déploiement de *blockchains*. Ces objets souffrent souvent d'une faible sécurité mais peuvent jouer un rôle important dans les écosystèmes informatiques. Les registres distribués ont le potentiel de suivre ces objets individuellement et d'augmenter la confiance, la transparence et la traçabilité dans leur déploiement. Par exemple, ces registres peuvent contenir des certificats de sécurité, connaître les propriétés des différents composants d'un système, s'assurer qu'il ne s'agit pas de copies, ou permettre la localisation d'objets pour les rappeler si besoin est.

La *blockchain* peut également favoriser l'identification de personnes physiques. Elle peut par exemple faciliter la portabilité de documents dans des procédures de « connaissance client » en milieu bancaire, mais aussi la création d'identités synthétiques pour des migrants internationaux. Par exemple, le projet « Id 2020 » se propose d'aider le milliard d'individus sans identité reconnue officiellement. La *blockchain* peut aussi aider à concilier vérification d'identité et protection de la vie privée en offrant des droits de lecture différents en fonction de la situation. Par exemple, une personne chargée de vérifier l'âge à l'entrée d'un établissement peut en principe utiliser une identité contenue dans une *blockchain* sans que la personne contrôlée n'ait besoin de révéler son nom et son adresse (ni même sa date de naissance).

Conclusion

La technologie de la *blockchain* et plus généralement celle des registres distribués peut avoir des implications importantes pour la sécurité et la vie privée. Il s'agit d'une nouvelle approche qui est encore mal comprise. Toutefois, il est probablement préférable de la réguler alors qu'elle en est encore à ses débuts. Une approche législative ou même administrative est sans doute très largement prématurée mais le développement de groupes de travail comprenant différentes parties prenantes pour comprendre et structurer son essor serait une bonne chose. Il serait souhaitable que les acteurs européens y jouent pleinement leur rôle, à l'inverse de ce qu'il s'est produit pour Internet.

L'AUTEUR

Gilles Hilary est professeur à l'Université de Georgetown. Il est Chercheur Associé au Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN) et Membre Fondateur du Cercle K2.

© Blueboy2014 pour AdobeStock

LA BLOCKCHAIN FAIT L'OBJET D'UN INVESTISSEMENT STRATÉGIQUE

La transformation numérique suscite l'apparition d'outils nouveaux dont la blockchain est un fleuron. Supportée par un réseau pair à pair décentralisé, elle propose une authentification qui garantit la discrétion. La blockchain ne se limite pas aux cryptomonnaies et se déploie au sein de chaînes publiques, semi-publiques ou privées. Ces dernières peuvent être utiles pour faciliter le partage de l'information au sein de grandes organisations à multiples acteurs, ce qui est le cas des entités militaires. La décentralisation facilite une intermédiation qui permet le transfert d'informations multiformes incluant le protocole de transport et un cryptage. De plus, l'horizontalité du système accroît sa résilience et se conjugue avec l'immuabilité de l'information qui est déposée au sein des Blockchain. C'est la raison pour laquelle les grandes puissances développent des projets stratégiques dans les domaines des opérations de renseignement et de la logistique militaire.

La blockchain est-elle un tournant stratégique ?

Par Olivier Kempf

Cet article, qui s'inscrit dans la ligne éditoriale de cette revue et les thèmes développés pour le FIC 2019, a été publié dans la revue de la défense nationale (Tribune N° 1011 du 6 juin 2018). La qualité et la pertinence de ce propos nous a conduit à le proposer à votre attention avec l'aimable autorisation de la revue de la défense nationale.
http://www.defnat.com/bibliotheque/resultats_auteur.php?cenvoi=1&cidaut=290&cauteur=%27Olivier%20Kempf%27

Les innovations informatiques se succèdent au point qu'il est difficile d'en prendre la mesure. Pourtant, chacun a pu apprécier l'importance de cette révolution informatique qui se déroule depuis maintenant 35 ans et qui avait été décelée très tôt par le jeune Zbigniew BRZEZINSKI (1971). Que se passe-t-il en effet ? Au cours des années 1980, les ordinateurs individuels se répandent : 1re vague de cette révolution informatique. Fin des années 1990, irruption d'Internet et de la communication entre ordinateurs : 2e vague. Milieu des années 2000, ce qu'on a appelé le Web 2.0, à savoir l'ère des blogs et autres réseaux sociaux permettant à tout un chacun de s'exprimer sur « la Toile » : 3e vague. Enfin, nous serions, au cours de notre décennie 2010, en train de vivre la 4e vague de cette révolution, celle que l'on dénomme « transformation numérique ».

OLIVIER KEMPF

Docteur en science politique,
Chercheur associé à l'IRIS,
Directeur de la lettre stratégique La Vigie

Elle peut se caractériser par bien des choses : une très grande mobilité, des méthodes particulières, des outils nouveaux. Parmi ceux-ci, des mots reviennent : infonuagique (*cloud)*, Internet des objets (IOT), Données massives (*Big Data*), Intelligence artificielle (IA), robotique, *blockchain* (« chaîne de blocs », en bon français, même si la traduction n'a jamais trouvé audience : nous accepterons donc *blockchain* dans cet article).

Celle-ci a attiré l'attention des grands médias à la suite de la spéculation autour

du Bitcoin, une cryptomonnaie dont les cours se sont envolés cet hiver avant de replonger à des niveaux moins spéculatifs (mais toujours assez élevés[1]). Cependant, si le Bitcoin est indissociable de la *blockchain*, on ne peut réduire celle-ci aux cryptomonnaies. L'enjeu est différent et a des potentialités qui doivent intéresser les stratégistes.

(1) Parti d'environ 5 000 $ à la fin de l'été 2017, il était monté au-dessus de 19 000 $ l'unité, puis il avait plongé fin décembre, baissant jusqu'à 6.500 $ début avril. Fin avril, il entamait une remontée autour de 9 500 $.

Les généraux byzantins

Tout débute justement par un problème d'apparence stratégique, ce qu'on a appelé le dilemme des généraux byzantins. Peut-être faut-il y voir une allusion à Bélisaire, le fameux général de l'empereur Justinien, résistant victorieusement aux Ostrogoths lors du siège de Rome en 537, ou peut-être aux assauts contre les Perses auxquels s'affrontait Byzance. Mais il s'agit surtout d'un problème mathématique de théorie des jeux décrit en 1982 par Leslie LAMPORT, Robert SHOSTAK et Marshall PEASE. Depuis les études sur la dissuasion nucléaire, les stratégistes ont appris quelques rudiments de théorie des jeux et ils liront donc ce qui suit avec plaisir.

Voici donc des généraux byzantins qui campent, chacun à la tête de son corps d'armée, autour d'une cité ennemie qu'ils assiègent. Ils ne peuvent communiquer entre eux qu'au moyen de messagers et c'est nécessaire pour établir un plan de bataille commun. Sans cette communication, la défaite sera certaine. S'il n'y avait que deux généraux, cela ne serait pas trop difficile mais imaginez que huit généraux assiègent le camp perse ? Chacun doit communiquer avec les sept autres et il n'y a pas de général en chef qui puisse assurer la coordination des huit.

Dès lors, tout repose sur les messagers. Que l'un d'eux soit un traître ou soit attrapé par l'ennemi, et les Byzantins perdent. Il a été démontré qu'en utilisant uniquement des messages oraux, ce problème des généraux byzantins peut être résolu, si et seulement si plus des deux tiers des messagers sont loyaux. Ainsi, un seul traître peut confondre deux généraux loyaux. De plus, le problème peut être résolu pour un nombre quelconque de messagers renégats si les messages sont écrits (et non falsifiables).

Bref, comment surmonter la défaillance d'un membre d'un groupe et établir un consensus suffisamment solide pour arriver à ses fins ? Comment établir la confiance dans un système décentralisé en partageant les intentions de chacun ? « La *blockchain* constitue la première et peut-être la seule solution au problème des généraux byzantins » (Laurent LELOUP, p. 46). Un système informatique décentralisé peut ainsi gérer les défaillances de certains de ses composants en utilisant un algorithme cryptographique fondé sur un système décentralisé de preuves. S'il existe d'autres systèmes de tolérance aux défaillances, la *blockchain* met

l'accent sur un réseau de pair à pair et sur l'authentification cryptographique.

Ce problème aurait pu être réservé aux seuls informaticiens jusqu'à ce qu'un auteur écrivant sous le pseudonyme de Satoshi NAKAMOTO annonce en 2008 la naissance du Bitcoin, « une monnaie électronique fondée sur un système de pair à pair ». Par cette méthode qui résout le problème des généraux byzantins, deux agents peuvent échanger des actifs sans passer par un tiers de confiance.

Les cryptomonnaies ont popularisé la Blockchain

Le succès est rapide. Le Bitcoin est en effet une chaîne de blocs ouverte, « fonctionnant par un réseau de pair à pair, sans autorité centrale (et donc sans autorité financière [comme une banque centrale]) tout en enregistrant chaque transaction (horodatage) dans un grand livre de compte (*ledger*) dans lequel toute modification est impossible » (L. LELOUP, p. 34).

Bitcoin, c'est donc de l'argent, ce qu'on appelle une cryptomonnaie : une monnaie, mais crypto, c'est-à-dire à la fois cachée (hors des banques centrales) et utilisant la cryptographie. Elle garantit ainsi la discrétion, grâce à une décentralisation absolue (celle du réseau pair à pair), mais pas l'anonymat, beaucoup moins que l'argent liquide par exemple (cf. RAY). Et c'est une monnaie car les transactions sont enregistrées « pour toujours ». Un actif reste un actif. Une chaîne de blocs constitue ainsi une technologie WORO (*Write Once, Read Only*) : on ne peut écrire qu'une fois l'écriture considérée sur le livre de compte : ensuite, il n'est possible que de la lire. D'ailleurs, chaque écriture est reliée à la précédente et ainsi de suite jusqu'au début : les écritures précédentes, authentifiées, garantissent la nouvelle écriture. Celle-ci n'est rendue possible que par la résolution d'un problème cryptographique (la preuve de travail, ou *Proof of Work*), opération que l'on désigne sous le terme de « minage » et qui nécessite de très grosses puissances de calcul.

Dans le cas du Bitcoin, chaque résolution de problème permet de gagner de nouveaux Bitcoins : cela explique pourquoi tant de consortiums se sont lancés dans le minage, pourquoi il y a des fraudes au minage (votre ordinateur peut être phagocyté pour participer en réseau à l'effort de minage), pourquoi enfin cela consomme énormément d'énergie. La folie du minage ressemble aux ruées vers l'or du XIX^{e} siècle. Toutefois, si l'or enrichit, le Bitcoin aussi ! Il se dit ainsi que Satoshi Nakamoto détiendrait un million de Bitcoins, soit près de 10 milliards de dollars… Il reste que le nombre de Bitcoins est limité : il y a un plafond à la masse monétaire en circulation.

À la suite du bitcoin, d'autres cryptomonnaies ont été lancées : on pense à Litecoin, Peercoin puis Monero, Ethereum, nouvelles cryptomonnaies utilisant des techniques supplémentaires (adresses de furtivité,

contrats intelligents, etc.). Les systèmes de preuves évoluent également avec des calculs moins gourmands en énergie, mais aussi des possibilités nouvelles. Ethereum permet ainsi d'associer des contrats intelligents (*smart contracts*), technique qui est utilisée par certains assureurs dans des contrats expérimentaux : votre avion est annulé et automatiquement, par simple constat de l'annulation, la prime d'assurance vous est versée…

La folie des cryptomonnaies s'est étendue. Ainsi, Kodak a vu son cours de bourse multiplié par trois lorsqu'en janvier 2018, il a annoncé vouloir créer une cryptomonnaie Kodakcoin, liée aux échanges photographiques (voir l'article sur EGEA). La cryptomonnaie de la messagerie Telegram est attendue par beaucoup. De même, de multiples start-up proposent des ICO (*Initial Coin Offering*) : ce sont des systèmes permettant de financer les premiers capitaux propres grâce à la souscription des cryptomonnaies associées au projet de la start-up. Là aussi, il y a énormément de spéculations.

L'intérêt de la blockchain ne se limite pas aux cryptomonnaies

Est-ce pourtant à dire que la *blockchain* n'est qu'une affaire financière ? Non, car la cryptomonnaie n'est pas systématique et une chaîne de blocs est d'abord autre chose, selon Wikipédia : « Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en bloc, l'ensemble étant sécurisé par cryptographie, et formant ainsi une chaîne ». C'est un registre distribué (décentralisé) et sécurisé de toutes les transactions inscrites. Ces deux caractéristiques nous intéressent fortement.

Certains expliquent en effet que la *blockchain* revêt les caractéristiques du protocole *TCP/IP*, lorsqu'il apparut au milieu des années 1990 : qui eût parié sur la généralisation aussi massive de ce protocole qui a permis le développement d'Internet (et notamment la deuxième vague que nous mentionnions en introduction). Par beaucoup d'aspects, la *blockchain* permet de tels développements. Ses deux caractéristiques majeures sont en effet la sécurité et la décentralisation.

La sécurité intéresse par définition tous les stratégistes. Voici en effet un système garantissant des transactions de toute sorte, c'est-à-dire des échanges d'information. Or, une *blockchain* peut être utilisée de plusieurs façons : on parle ainsi de chaînes publiques, semi-publiques ou privées. Dans une chaîne publique, tout le monde peut écrire et lire. Dans une *blockchain* semi-publique, seuls les membres du consortium peuvent écrire mais tout le monde peut la lire. Dans une *blockchain* privée, seuls les membres du consortium peuvent écrire mais aussi la lire. Cette dernière configuration peut à l'évidence être utile pour de grandes orga-

nisations à multiples acteurs où le partage de l'information est difficile mais qui doit rester le fait des seuls membres : de ce point de vue, les organisations militaires sont particulièrement représentatives de ce cas de figure.

La décentralisation est cependant la caractéristique la plus importante. D'abord dans le monde civil. On dit en effet de la *blockchain* qu'elle peut ubériser Uber. Si l'industrie financière a été la première à prendre en compte l'impact potentiel de la *blockchain*, pour les raisons que l'on a vues, c'est toute l'économie qui risque elle aussi de se voir transformer en profondeur. On sait que la société Uber a fondé sa réussite sur l'intermédiation entre des offreurs de microservices (un voyage en stop, une chambre chez l'habitant) et des demandeurs. Ce modèle a été repris par de nombreuses plateformes : Uber donc pour les taxis, Blablacar pour le covoiturage, AirBnB pour les chambres chez l'habitant… Mais Uber et Blablacar se présentent comme des intermédiaires centraux qui gèrent l'intermédiation (et en tirent leurs profits). Or, une fois qu'on a compris que chacun pouvait acheter et offrir des microservices, a-t-on toujours besoin d'une plateforme dédiée ? Ne peut-on pas économiser les coûts associés à son usage ? Une *blockchain* totalement décentralisée permettrait de résoudre cette difficulté et donc de se passer d'Uber. La *blockchain* peut donc ubériser Uber.

L'intérêt stratégique pour la blockchain de par le monde

Constatons que dès 2015, les États-Unis se sont intéressés à la technologie de la chaîne de blocs dans une perspective de défense. La DARPA (*Defense Advanced Research Projects Agency*) a ainsi lancé en 2016 un appel d'offres pour une « plateforme de messagerie sécurisée » (cf. Giulio PRISCO) : celle-ci doit être capable de transférer des messages via un protocole décentralisé sécurisé sur plusieurs canaux, incluant le protocole de transport, le cryptage des messages et la mise en œuvre de la *blockchain* personnalisée.

La *DARPA* note que cette plateforme de messagerie sécurisée planifiée permettra de cartographier l'écosystème du ministère américain de la Défense (*DoD*), organisé actuellement selon une logique de métier qui entrave la bonne communication entre services. Outre une simplification des échanges, le système offre une meilleure sécurité et améliore la productivité. Selon le cabinet SIA PARTNERS, « la clé de chiffrement utilisée ne les rend lisibles que par le destinataire final, mais la diffusion du message crypté à l'ensemble du réseau garantit la stabilité du système de messagerie et la confidentialité des métadonnées, l'émetteur et le récepteur devenant impossibles à identifier par un tiers. Cela constitue un progrès par rapport au système actuel, dans lequel les données sont inégalement distribuées, les rendant vulnérables à une défaillance

des serveurs, liée ou non à une démarche hostile ».

À la suite de la *DARPA*, l'agence Otan des communications informatiques (la *NCIA*) a lancé un défi d'innovation sur ce même thème de la *blockchain*. Notons enfin que dans le programme de 700 milliards de dollars d'investissement de défense signé par le président Trump en décembre 2017, la *blockchain* est explicitement mentionnée dans la Section 1646[2].

Les Russes aussi sont intéressés, comme en témoigne la déclaration à l'agence *Tass* du PDG de Voentelecom (une société russe de télécommunications travaillant pour le ministère russe de la Défense) le 22 août 2017. En Israël, le principal fabricant d'aéronautique IAI a annoncé, en janvier 2018, développer un produit *blockchain* pour une solution de cybersécurité (cf. Shoshanna SOLOMON). La Chine ne semble pas en reste : on apprenait ainsi (cf. Wilson VORNDICK) que le colonel Zhu QICHAO, directeur du Centre des études stratégiques et de sécurité nationale de l'Université de défense et de technologie de Pékin, par ailleurs, un des experts chinois reconnus en Intelligence artificielle, avait coécrit un article en avril 2016 où il soulignait les intérêts de la *blockchain* dans la panoplie chinoise de sécurité. Il discernait ainsi trois domaines favorables : les opérations de renseignement, le cycle de vie des armes et la logistique militaire. Toutefois, l'aspect structurellement décentralisé de la chaîne de blocs pose un évident problème au système centralisé chinois…

Quel intérêt militaire ?

On peut, d'ores et déjà, identifier plusieurs applications de la chaîne de blocs dans le monde de la défense. D'abord, des améliorations du fonctionnement organique.

La chaîne de blocs introduit en effet un changement de paradigme. Jusqu'à présent, les organisations et notamment l'institution militaire ont adopté une logique de château fort pour garantir l'information. Cette approche paraît de plus en plus vaine, tant l'information se multiplie et se disperse dans les usages les plus courants. Dès lors, utiliser une nouvelle technologie décentralisée est peut-être la bonne approche. Autrement dit, on passe d'un système vertical à un système horizontal, qui assure une meilleure résilience et surtout l'immuabilité de l'information qui y est déposée.

(2) Le projet de loi décrit explicitement le cas d'utilisation de la technologie blockchain dans la défense nationale et l'applicabilité d'un registre immuable pour la protection des informations sensibles. L'étude devrait inclure une description des applications cyberoffensives et défensives potentielles de la technologie blockchain et d'autres technologies de bases de données distribuées ; une évaluation des efforts déployés par les puissances étrangères, les organisations extrémistes et les réseaux criminels pour utiliser ces technologies ; une évaluation de l'utilisation ou de l'utilisation prévue de ces technologies par le gouvernement fédéral et les réseaux d'infrastructures essentielles ; et une évaluation des vulnérabilités des réseaux d'infrastructures critiques aux cyberattaques (www.defense.gov/News/Special-Reports/0518_budget/). Le cycle de vie des armes et la logistique militaire. Toutefois, l'aspect structurellement décentralisé de la chaîne de blocs pose un évident problème au système centralisé chinois…

La chaîne de blocs permettrait alors une meilleure protection de nos informations, renforçant la cybersécurité actuelle. En effet, les menaces d'ordre cyber croissent exponentiellement (en nombre, en qualité et en diversité d'agression) et un nouveau modèle semble nécessaire. Premièrement, les réseaux *blockchain* sont conçus sans tiers de confiance (puisqu'il s'agit de répondre au dilemme des généraux byzantins), ils assument structurellement le compromis du réseau par les initiés et les étrangers. Deuxièmement, les *blockchain*s sont sécurisées de manière transparente et reposent sur une structure de données cryptographiques qui rend la falsification à la fois exceptionnellement difficile (attaque dite à 51 %, impossible à atteindre dans les faits) et immédiatement évidente. Enfin, les réseaux *blockchains* sont tolérants aux pannes puisqu'ils mobilisent les efforts des nœuds valides pour rejeter ceux qui sont suspects. En conséquence, les réseaux de chaînes de blocs réduisent non seulement la probabilité de compromis, mais imposent également des coûts beaucoup plus élevés à un adversaire pour l'atteindre. Un des objectifs recherchés par la *DARPA* serait donc de garantir l'intégrité des données associées à des systèmes d'armes cruciaux, comme ceux soutenant les armes nucléaires ou les satellites (cf. Joon Ian WONG).

Notons enfin que la *blockchain* sera probablement le meilleur moyen de contrôler la sécurité de l'Internet des objets (IOT) dont les déficiences sont aujourd'hui patentes. Le logiciel malveillant Mirai a ainsi utilisé un réseau de caméras de surveillance pour susciter une des plus grandes agressions DDOS (attaque par déni de service) de l'histoire, en septembre 2016. Or, la sécurité informatique de la plupart de ces objets est défaillante. Placer un réseau d'objets connectés sur une *blockchain* permettrait sans nul doute de contrôler les échanges entre eux, d'autant plus que la chaîne gagne en sécurité à mesure que des organisations s'y connectent. Une expérience britannique aurait ainsi été menée en ce sens avec le *Defence Science and Technology Laboratory (DSTL)*, la DGA d'outre-Manche : *« using a blockchain to improve the trustworthiness of a network of sensors on, for example, security cameras »*.

Mais la *blockchain* pourra également améliorer les opérations. Cela paraît évident en termes de logistique, un des grands domaines civils où elle se répand à grande vitesse. La chaîne de blocs permet ainsi d'accélérer les livraisons, d'améliorer la qualité des produits en flux tendu ou encore de faciliter la maintenance des véhicules. De même, elle permet de garantir la traçabilité des denrées et produits transportés. On imagine la fiabilité obtenue dans les acheminements opérationnels de logistique diverses vers des zones les plus difficiles et dans des environnements inconfortables (Tchad, Mali, Afghanistan). L'auteur de ces lignes se souvient ainsi d'un conteneur de pièces de rechange qui avait disparu et qui empêchait le Maintien en condition opéra-

tionnelle (MCO) des bataillons déployés à Abéché lors de l'opération EUFOR Tchad. On l'avait retrouvé, dix mois après, égaré dans une zone de stockage annexe.

Comme le constate le cabinet Sia Partners, « la possibilité de mieux gérer les acheminements de matériels *via* la *blockchain* devrait permettre selon IBM une réduction de 20 % des coûts grâce à la réduction des démarches administratives et des erreurs, la réduction des temps de transit sur toute la chaîne d'approvisionnement et la simplification des processus. [Elle] devrait aussi permettre une diminution des coûts d'assurance en offrant un meilleur contrôle aux clients sur les transports de leurs marchandises. La *blockchain* permet aussi de résoudre de nombreuses difficultés actuelles : les contrôles et les vérifications sont réalisés par consensus et chaque étape est scrupuleusement enregistrée. Cette technologie permet ainsi de diminuer les coûts des opérations de vérification, et plus généralement du tracking ».

D'autres apports opérationnels peuvent être imaginés, plus proches des missions des troupes de contact : le contrôle des armes à feu dans la circonstance de processus DDR (Désarmement, démobilisation et réintégration) ou encore la certification du statut et du niveau de sécurité des individus accédant à une base opérationnelle.

En quelques mots, la *blockchain* présente plusieurs qualités qui intéresseraient la défense : une source unique et immuable d'authenticité des informations qui y sont enregistrées ; l'organisation plus facile et plus visible de chaînes logistiques complexes ; un système automatisé ; une qualité de service renforcée ; un meilleur système de compte rendu, donc de pilotage ; une sécurité renforcée ; et surtout, un chemin privilégié vers la transformation digitale qui est synonyme de décentralisation, mobilité et explosion du nombre de données, autant de contraintes auxquelles la chaîne de blocs répond avec aisance.

À l'heure où l'intelligence artificielle est dans toutes les bouches et fait l'objet de toutes les attentions, la chaîne de blocs constitue une innovation technologique probablement plus accessible et aux potentialités certaines. La négliger serait une erreur.

Revue Défense N@tionale
Le revue du débat stratégique

L'AUTEUR

Docteur en science politique, chercheur associé à l'IRIS, directeur de la lettre stratégique La Vigie, Olivier Kempf est consultant en stratégie digitale. Il a publié avec François-Bernard HYUGHE et Nicolas MAZZUCCHI : Gagner le cyberconflit, au-delà du technique (Économica, 2015, 175 pages). Olivier Kempf est l'auteur de : Introduction à la cyberstratégie (Economica, 2012) et Alliances et mésalliances dans le cyberespace (Economica, 2014)

ÉLÉMENTS DE BIBLIOGRAPHIE

BRZEZINSKI Zbigniew, La révolution technétronique, 1971, Calmann-Lévy (1970 pour l'édition anglaise).
KEMPF Olivier, « Kodak et le numérique : naufrage puis renaissance », EGEA Blog, 28 avril 2018 (www.egeablog.net/index.php?post/2018/04/28/Kodak-et-le-num%C3%A9rique%3B-naufrage-puis-renaissance).
LAMPORT Leslie, SHOSTAK Robert et PEASE Marshall, « The Byzantine Generals Problem », ACM Transactions on Programming Languages and Systems, vol. 4, n° 3, juillet 1982.
LELOUP Laurent, La blockchain, la révolution de confiance, Eyrolles, 2017, 224 pages.
LIAN Lin, ZHU Qichao et ZHAO Zhao, « Blockchain Technology and Its Potential Military Value [区块链技术及其潜在的军事价值] », National Defense Science & Technology [国防科技], vol. 37 N° 2, avril 2016, p. 30-34.
NAKAMOTO Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 (https://bitcoin.org/bitcoin.pdf).
PRISCO Giulio, « DARPA, NATO Looking at Military Applications of Blockchain Technology », Bitcoin Magazine, 23 mai 2016 (https://bitcoinmagazine.com/).
RAY, « Bitcoin : le point sur l'anonymat », Contrepoints.org, 20 juin 2014 (www.contrepoints.org/2014/06/20/169540-bitcoin-le-point-sur-lanonymat).
SIA PARTNERS, « La blockchain, nouvelle botte secrète des armées », 1er mars 2018 (http://secteur-public.sia-partners.com/20180301/la-blockchain-nouvelle-botte-secrete-des-armees).
SOLOMON Shoshanna, « Bank Hapoalim IAI to join forces on using blockchain for cybersecurity applications », The Times of Israel, 3 janvier 2018 (www.timesofisrael.com/bank-hapoalim-iai-to-join-forces-on-using-blockchain-for-cybersecurity/).
TASS, « Blockchain Technology may be introduced in Russia's Armed Forces », 22 août 2017 (http://tass.com/defense/961423).
VORNDICK Wilson, « Beyond Bitcoin : Could China Embrace Blockchain for Defense and Security Applications ? »,
China Brief, vol. 18, n° 2, The Jamestown Foundation, 13 février 2018 (https://jamestown.org/program/beyond-bitcoin-china-embrace-blockchain-defense-security-applications/).
WONG Joon Ian, « Even the US military is looking at blockchain technology—to secure nuclear weapons », Quartz, 10 octobre 2016 (https://qz.com/).

© Fotolia

LE CRYPTO-CRACKING EST UN OUTIL DE L'INFORMATIQUE LÉGALE

Si on constate une diversification des activités criminelles lucratives, par le biais de l'anonymat par clés cryptées, l'informatique légale dispose d'outils qui permettent un traçage et une analyse des flux illicites. Les technologies de crypto-tracking reposent sur une exploration des transactions des crypto-monnaies inscrites de manière indélébile dans les blockchains. Elles sont soutenues par l'arsenal juridique français qui oblige les prestataires de service de portefeuille à identifier de manière probante leurs clients et les bénéficiaires des transactions. On doit également mentionner le caractère impératif du signalement à TRACFIN des transactions suspectes.

Les procédures d'investigation doivent toutefois être menées par des agents habilités, sous contrôle de magistrats, et prendre soin de respecter les règles concernant les traitements de données à caractère personnel. Cela concerne la proportionnalité de la collecte, la qualité et les modalités de conservation des données mais également le fait que les opérateurs de crypto-cracking devront renforcer les mesures de sécurité entourant leurs opérations, journaliser les actions et prévoir une analyse d'impact sur les données traitées.

Crypto-tracking :
Les nouveaux outils d'enquête pour les forces de l'ordre

Par Adel Jomni

Offrant des perspectives de créativité et de croissance à l'échelle de la planète, le développement exponentiel du cyberespace génère une criminalité sans frontières. Les utilisations malveillantes des réseaux pouvant être facilement maquillées, il est en pratique très difficile d'identifier les cyberdélinquants agissant sur le Darknet et utilisant les monnaies virtuelles dans le cadre de leurs transactions. Afin d'apporter à cette criminalité émergente une réponse étendue et spécifique, les forces de l'ordre doivent se doter de nouveaux outils d'investigation.

ADEL JOMNI

UFR Droit & science politique
Université de Montpellier

À l'heure où les données informatiques sont en passe de devenir les nouvelles reines des preuves, détrônant parfois l'aveu ou l'ADN, il devient essentiel de doter les autorités compétentes d'outils performants et adaptés de manière à traquer les cyberdélinquants. Ces derniers dissimulent en effet leurs activités en publiant du contenu illicite accessible uniquement depuis les « *Darknet*s ». En plus de cet Internet caché, les cybercriminels disposent d'une armada technologique redoutable aux fins de masquer leurs activités criminelles. En tête de celles-ci, l'utilisation de monnaies virtuelles, aussi appelées crypto-monnaies, permet de réaliser des transactions de façon quasi-intraçable (I).

Face à ce constat, les forces de l'ordre se doivent de réagir et de lutter à armes égales contre cette nouvelle délinquance. Le « *Digital forensic* », ou « l'Informatique légale », s'est beaucoup développé ces dernières années. On y retrouve les outils de « *crypto-tracking* » qui rendent possible l'analyse des flux de transactions sus-

pectes réalisées en monnaie virtuelle de manière à identifier leurs auteurs (II).

Le développement de ces outils nécessite néanmoins le strict respect du principe de loyauté que l'on retrouve au stade de l'enquête (III). À défaut, les preuves obtenues grâce aux outils de *crypto-tracking* pourraient être déclarées irrecevables devant le juge.

I / Darknets, espaces de délinquance

Sur ce cyberespace obscur, des sites cachés de la vue du grand public proposent un panel de produits et de services illicites (A) moyennant quelques crypto-monnaies (B).

A) Organisation de l'activité criminelle sur le Darkweb

L'activité criminelle présente sur le *Darkweb* est devenue extrêmement professionnelle et organisée au cours de ces dernières années. Véritable marché guidé par la demande, le crime s'y est organisé en adaptant la qualité et la diversité de ses offres de service. On parle même parfois de Plateformes « *Crime-as-a-Service* » (CaaS).

Face à une demande croissante, les sites les plus lucratifs du *Darkweb* ont adopté le modèle de « place de marché » et plébiscitent l'utilisation de moyens de paiement cryptographiques. Parmi ces marchés noirs numériques, aussi appelés « crypto-marchés ».

Sur ces crypto-marchés, l'identité des acteurs est obscure, vendeurs et acheteurs se cachant derrière des pseudonymes pour perpétrer leurs activités. La confiance est donc le facteur clé de cette économie cyber-souterraine, nécessitant le recours à une architecture organisationnelle bien rodée.

B) Crypto-monnaies : pilier de la cybercriminalité sur le Darkweb

L'anonymat offert par les crypto-monnaies est une véritable aubaine pour les cyber-délinquants qui peuvent aisément dissimuler leurs identités derrière une clé « publique » générée aléatoirement par des procédés cryptographiques. La plus célèbre d'entre elles, le *Bitcoin* (BTC), est également la crypto-monnaie la plus utilisée sur le *Darkweb*. Elle permet d'effectuer des transactions de façon quasi-anonyme en n'ayant pour seule et unique information que l'adresse *Bitcoin* du bénéficiaire de l'échange.

Bien qu'« uniques », les adresses *Bitcoin* peuvent être « multiples ». Il est dès lors possible de créer en quelques clics une adresse différente pour chaque nouvelle transaction. Cette méthode est énormément mise à profit par les cyber-délinquants afin de camoufler leurs échanges.

Dans la même veine, d'autres outils, comme les *Bitcoin Mixer* ou *Bitcoin Tumblers*, sont utilisés. Ces services permettent de mélanger des fonds de crypto-mon-

naies avec d'autres afin de flouter le chemin vers la source originale des fonds.

(1) P. RODRIGUEZ, La révolution Blockchain, DUNOD 2017

Certaines crypto-monnaies ont acquis une réputation sulfureuse sur le *Darkweb* et sont particulièrement privilégiées par les cyber-délinquants. Fin octobre 2016, la technologie Blockchain a donné naissance au *Zcash* (ZEC). Cette monnaie offre davantage de sécurité et d'anonymat que le *Bitcoin*. Elle s'appuie sur le protocole ZKIP (preuve à divulgation nulle de connaissance), principe cryptographique permettant d'authentifier ou d'identifier un utilisateur sans fournir d'autre information que la réponse à une question posée. Dans le cadre d'une utilisation pour des monnaies virtuelles, ce protocole a été amélioré et rebaptisé « *Zk-Snark* » et permet d'accroître l'intraçabilité des échanges en ligne[1]. On peut également citer la monnaie virtuelle *Monero* qui s'inscrit dans le même sillage que le *Zcash* en faisant la promotion de la protection de la vie privée de leurs utilisateurs.

Des développements qui précèdent, il est possible de dresser le constat suivant : la majorité des sites présents sur le *Darkweb* proposent des contenus illicites et plusieurs d'entre eux utilisent des moyens de paiement cryptographiques quasi-intraçables. Cette nouvelle forme de criminalité appelle à la mise en place d'outils d'analyse et d'enquête dédiés à l'identification des cyber-délinquants.

II/ Les technologies de Crypto-tracking au service de l'enquête

Les technologies de *crypto-tracking* reposent sur l'étude approfondie des transactions en crypto-monnaies, lesquelles sont inscrites de manière indélébile sur la Blockchain. Par croisements d'informations via l'utilisation de puissants algorithmes, il est dès lors possible de retracer l'ensemble des flux de transactions jugées suspectes. Le but recherché par le *crypto-tracking* est de remonter jusqu'à l'adresse d'un service de portefeuille en ligne, ou d'une Plateforme d'échange de monnaies virtuelles.

(2) Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE (Texte présentant de l'intérêt pour l'EEE)

(3) C. mon. fin., art L 561-2 et s.

En effet, avec la nouvelle Directive anti-blanchiment[2] qui vient compléter l'arsenal législatif français[3], les prestataires de services d'échange entre monnaies virtuelles et monnaies légales (PSEMV) et désormais les prestataires de services de portefeuille de conservation (PSPC) ont l'obligation d'identifier leurs clients (KYC) mais aussi les bénéficiaires effectifs de la transaction. Les éléments d'identification fournis doivent présenter un caractère probant, que les clients soient occasionnels ou non.

Ces nouveaux acteurs ont également l'obligation d'effectuer un examen renforcé

de toutes les opérations particulièrement complexes ou d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite. Ils doivent signaler le cas échéant les transactions suspectes au TRACFIN. Ces mesures permettent notamment de lutter contre le blanchiment d'argent et le financement du terrorisme.

Par un recoupement entre l'historique des transactions et l'identité des personnes, les enquêteurs ont dès lors la possibilité d'identifier les vendeurs et acheteurs agissant sur les crypto-marchés du *Darkweb*.

III/Crypto-tracking, quel cadre légal ?

Malgré leur efficacité pratique, les outils de *crypto-tracking* devront, sous couvert de respecter le principe de loyauté de la preuve pénale en respectant les procédures d'investigation (A) et le principe de loyauté des traitements de données à caractère personnel consacré par la Directive Police-Justice récemment transposée (B), s'adapter à la réglementation applicable. À défaut, les éléments de preuves collectées pourraient être invalidés par le juge.

© Gold bitcoin coin Par Andrey Burmakin

La nouvelle directive anti-blanchiment obligera les prestataires de services à fournir les tables de correspondance entre les informations personnelles des individus et les adresses portefeuille et brisera ainsi l'anonymat des transactions.

A) Crypto-tracking & loyauté de la preuve pénale

(4) Veille policière, Captation de données informatiques, Interception de données…

(5) CPP, art. 706-47-3, 706-35-1, 706-2-2, 706-72, 706-87-1, 706-2-3

Des différentes procédures d'investigation envisageables[4], l'enquête sous pseudonyme[5] est à plébisciter en matière de crypto-tracking.

L'objectif de cette procédure est de faciliter la constatation d'infractions par des agents ayant suivi une formation spécifique et spécialement habilités, sans qu'il soit nécessaire pour ces derniers d'obtenir une autorisation préalable délivrée par un magistrat.

Cette technique d'enquête numérique s'applique en particulier aux infractions de criminalité organisée, de pédopornographie et de lutte contre le terrorisme, qui sont légion sur le *Darkweb*.

Les agents habilités peuvent notamment :
– Participer, sous pseudonyme, aux échanges électroniques ;
– Extraire, acquérir ou conserver par ce moyen des éléments de preuve et des données sur les personnes susceptibles d'être les auteurs de ces infractions ;
– Extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites dans des conditions fixées par décret.

Bien que séduisante, l'enquête sous pseudonyme connaît malheureusement plusieurs travers qui appellent à des évolutions législatives afin d'optimiser l'efficacité des outils de *crypto-tracking*.

(6) CPP. art. 706-87-1

Tout d'abord, le critère de « criminalité organisée » justifiant le déclenchement de l'enquête sous pseudonyme[6] ne peut se présumer. Idéalement, il conviendrait d'insérer une présomption de criminalité organisée dès lors qu'un individu opère sur un réseau caché tel que le *Darkweb* afin de faciliter le travail des enquêteurs. En effet, la simple mise en ligne d'un crypto-marché nécessite des moyens tels qu'en pratique elle s'inscrit nécessairement dans des situations de criminalité organisée.

Une autre limite découle d'une carence législative liée à l'absence de décret précisant les conditions de transmission, d'acquisition et de conservation (stockage) des contenus illicites pourtant prévues à l'alinéa 4° de l'article 706-87-1 du Code de procédure pénale. Cette situation constitue un véritable flou juridique pour l'exploitation des outils de *crypto-tracking*.

B) Crypto-tracking & loyauté des traitements de données

Les opérations de *crypto-tracking* engendrent nécessairement des traitements de données à caractère personnel. L'objectif de ces nouveaux outils d'investigation est en effet d'identifier physiquement les personnes se cachant derrière les

transactions frauduleuses effectuées en crypto-monnaies.

À l'instar des adresses IP[7], des tables de correspondance existent en matière de crypto-monnaies. Comme nous l'avons vu précédemment avec la nouvelle Directive anti-blanchiment, les PSEMV et les PSPC européens seront très prochainement soumis à des obligations de lutte contre le blanchiment d'argent et le financement du terrorisme[8]. Ils bénéficieront donc de tables de correspondance entre les informations personnelles des individus et les adresses portefeuille utilisées pour les transactions en crypto-monnaies.

(7)CJUE, 19 oct. 2016, affaire C-582/14, Patrick Breyer c. Bundesrepublik Deutschland,

(8) Cette obligation existe déjà en droit français pour les Plateformes d'échange depuis l'ordonnance n° 2016-1635 du 1er décembre 2016 modifiant l'article L 561-2 du Code monétaire et financier.

Les traitements de données personnelles générés par le *crypto-tracking* doivent embrasser la réglementation applicable issue de la Directive Police-Justice n° 2016/680 récemment transposée en droit interne le 20 juin 2018 avec la modification de la loi Informatique et Libertés n° 78-17.

La Directive concerne les traitements de données à caractère personnel mis en œuvre par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Les collectes de données doivent respecter les principes de proportionnalité de la collecte, s'assurer de la qualité des données collectées, définir des durées de conservation pertinentes, être mises en œuvre dans le respect des concepts de *Privacy by Design* et *Default*… Les concepteurs des solutions de *crypto-tracking* auront quant à eux l'obligation de renforcer des mesures de sécurité techniques et organisationnelles, comprenant notamment une journalisation de l'ensemble des actions, de tenir un registre des activités de traitement, d'effectuer des analyses d'impacts sur la protection des données ou encore de désigner un délégué à la protection des données.

Le non-respect de cette réglementation serait à même de caractériser une atteinte disproportionnée à la vie privée des personnes concernées et d'entraîner une invalidité de l'ensemble des éléments produits dans le cadre de l'enquête.

Bien que prometteur, le *crypto-tracking* devrait aujourd'hui bénéficier d'un cadre juridique consolidé afin de pouvoir démontrer toute son efficacité. Cette technologie étant encore émergente, il appartient en effet au législateur de s'approprier les enjeux de la cybercriminalité et de préparer un terreau législatif fertile à même de doter les forces de l'ordre d'outils d'enquêtes adaptés.

L'AUTEUR

Monsieur Adel Jomni est enseignant-chercheur à l'UFR : Droit & science politique de l'université de Montpellier. Il est directeur du diplôme d'université : Cybercriminalité - droit, sécurité de l'information et informatique élargie et co-directeur de la session cybercriminalité et preuve numérique (École nationale de la magistrature-Paris). Expert international auprès du Conseil de l'Europe, il est membre de l'European Cybercrime Training and Eduction Group (ECTEG-Europol). Il est également membre-fondateur du Cecyf.

© Fresque monastère grec

LE CONSENSUS DES GÉNÉRAUX BYZANTINS

La sécurité de l'information repose finalement sur des principes simples de communicants : il faut des interlocuteurs authentifiés, qu'un tiers n'interfère pas dans la conversation, que le message arrive complet, dans une chronologie cohérente et sans insertions qui en faussent le sens. Enfin, le dernier souhait est que la conversation ne touche que ceux qui ont à en connaître. C'est un des fondements de la sécurité des transactions effectuées sur Internet. La Blockchain apporte par sa nature une réponse à des opérations requérant un consensus entre les parties à un contrat et ne suscite pas une authentification par un tiers de confiance. Le chaînage crypté des blocs vise à garantir l'absence d'une pollution des données et de leur distribution aux acteurs d'une opération. La fameuse problématique du système d'ordre des généraux byzantins sert dans cet article de démonstration des mécanismes de la Blockchain.

L'État ne sait pas
assiéger Byzance ?

Par Édouard Klein

La BlockChain nourrit les fantasmes. Seule une compréhension des concepts cryptographiques sous-jacents permettra un débat politique sain. Nous proposons dans cet article une définition formelle, quoiqu'accessible, de ce qu'est la BlockChain et de ce qu'elle n'est pas, aidée d'une comparaison avec les actes notariés. Nous proposons ensuite de porter le débat sur les questions que la technologie des *BlockChain* ne permet pas encore de régler.

ÉDOUARD KLEIN

Capitaine de Gendarmerie
Division de la lutte contre la cybercriminalité (DLC)
Service de renseignement criminel (SRC)
DGGN

La sécurité

Il est courant de définir la sécurité de l'information en la décomposant ainsi :

– **Intégrité :** la donnée ne doit pas être modifiée,
– **Authenticité :** L'auteur de la donnée doit être identifié,
– **Disponibilité :** La donnée doit être accessible,
– **Confidentialité :** Seul le destinataire de la donnée doit pouvoir la consulter.

Cette formalisation de la sécurité de l'information est élégante car ces quatre notions sont orthogonales et couvrent l'ensemble de ce qui est désirable dans un cryptosystème. Nous l'utiliserons dans la suite de cet article.

Nous sommes confrontés à ces notions dans notre vie de tous les jours. Prenons par exemple une visite chez un notaire à des fins testamentaires.

Le notaire

Outre son travail de percepteur, le notaire doit veiller à la sécurité de l'information portée sur l'acte qu'on lui confie :

– **Intégrité :** le contenu du testament d'une

personne ne doit pas être modifié
- **Authenticité :** au moment où la personne vient déposer son testament, le notaire doit vérifier son identité.
- **Disponibilité :** après le décès de la personne, le notaire doit mettre son testament à disposition de l'exécuteur et des héritiers.
- **Confidentialité :** avant son décès, la personne est la seule à pouvoir accéder à son testament.

Le notaire est ce que l'on appelle *un tiers de confiance* : il est un point unique de fiabilité et une défaillance de sa part entraîne l'écroulement de tout le système. Or, la protection des actes confiés au notaire ne repose pas sur les moyens techniques mis en œuvre. Les tampons physiques sont aisément falsifiables et la transition numérique opérée par les offices met en jeu des technologies avec des vulnérabilités connues. La protection des données contre des incidents et des attaques externes et la collaboration fidèle du notaire sont assurées par la force publique et des peines dissuasives sanctionnent une carence qui est une atteinte aux fonctions régaliennes. En effet, le crime de faux en écriture publique est puni de 10 ans de prison et 150 000€ d'amendes, portés à 15 ans et 225 000 € lorsqu'il est "commis par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions ou de sa mission". La confiance que l'on apporte à un acte notarié repose donc en réalité sur la violence légitime dont l'État a le monopole, ou tout du moins dans nos sociétés occidentales modernes, sur la menace crédible de violence. L'État est le tiers de confiance « ultime », le plus fort, le plus solide, le plus durable. Il est celui qui assure la valeur de la monnaie et le caractère inviolable de la propriété.

Pourtant, historiquement, l'État n'est pas infaillible. De révolutions en défaites militaires ou au détour d'une élection, les évolutions étatiques poussent quiconque a un peu de bon sens à chercher non pas un hypothétique tiers de confiance qui serait infaillible mais un système permettant par sa constitution, sans tiers de confiance, d'arriver à un consensus entre parties potentiellement antagonistes.

Les généraux byzantins

Du dîner des philosophes, en passant par l'algorithme de la boulangerie, le problème du voyageur de commerce ou du sac à dos, les informaticiens aiment à donner des noms mémorables à leurs problèmes et aux solutions qu'ils leur trouvent.

Depuis **[lamport1982byzantine]**, la question que nous venons de décrire, celle du consensus distribué, est connue sous le nom du problème des généraux byzantins. La métaphore veut que des généraux assiégeant Byzance doivent arriver à une décision consensuelle (attaquer ou battre en retraite), chacun ayant la possibilité de communiquer avec tous les autres. Une

décision non unanime, certains attaquent pendant que d'autres battent en retraite, est désastreuse pour tous.

Le problème est rendu intéressant par la présence de généraux félons, qui vont communiquer de manière différente avec chacun de manière à casser le consensus. Les messagers eux-mêmes peuvent également consulter, copier et modifier les messages (simulant ainsi un réseau hostile).

Les informaticiens ont l'habitude de mener leurs études dans un contexte adversarial, la justification mathématique étant qu'un algorithme résistant aux attaques volontaires et réfléchies est également résistants aux fautes aléatoires. Quiconque a déjà essayé de programmer un système distribué sait que la vraie raison est que la Nature mène une guerre active contre le bonheur des Hommes [mickens2013night].

Le succès fulgurant du *Bitcoin* d'abord, puis des *BlockChain* en général, vient de la résolution pratique du problème des généraux byzantins. Voyons cela au travers l'exemple de généraux : Alice, Bob et Charlie (généraux légitimes), Ève (l'espionne au service de Byzance qui se contente de rapporter la teneur des échanges) et Mallory (le général félon).

La Blockchain

Une stratégie classique pour Mallory consiste à dire à Alice, Bob ou Charlie que les deux autres ont dit quelque chose qu'ils n'ont en réalité pas dit. Elle va donc attaquer l'intégrité des données de la conversation.

Intégrité

L'aspect principal, celui qui donne son nom aux *BlockChain*s, est justement celui qui permet de maintenir **l'intégrité**.

Le mécanisme repose sur la notion cryptographique de fonction de hashage. Une fonction de hashage est une fonction déterministe « à sens unique » qui, à un argument, va associer un hash sous les conditions suivantes :

– une modification mineure de l'argument (un seul bit changé, en plus ou en moins) change complètement le hash,
– il n'est pas possible de remonter vers l'argument si l'on ne connaît que le hash,
– il n'est pas possible de deviner comment manipuler l'argument pour influencer le hash.

Le hash est typiquement une chaîne de caractères qui ressemble à ça : **`e3b0c44`**`298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`. Dans notre exemple on le réduira aux quelques premiers caractères: **`e3b0c44`**.

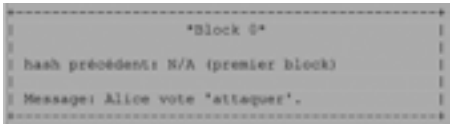
Maintenant, examinons la **notion de *bloc***. Il faut décider d'une unité atomique d'information qu'on nommera le *bloc*. On pourra ensuite aller chercher des choses à l'intérieur d'un bloc pour les analyser séparément. En ce qui concerne l'intégrité, soit

tout un bloc est valide, soit il est invalide, mais il ne peut être à moitié valide ou avoir une partie valide et l'autre invalide.

Dans le cas des généraux, imaginons qu'un block soit un message du style : `Alice vote 'attaquer'.`

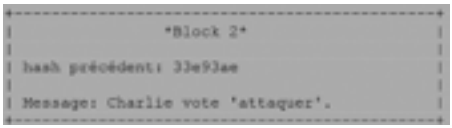
Il ne manque que la **notion de *chaîne***: une *BlockChain* est un système dit *append-only*: on ne peut jamais qu'ajouter des données, sans supprimer ni modifier ce qui a été publié avant. Depuis 1995, une telle chaîne est publiée dans le New York Times [oberhaus2018world]. Ce genre de systèmes est connu depuis des décennies pour par exemple la sauvegarde de fichiers [quinlan2002venti].

Pour faire d'un système de *bloc* une *BlockChain* qui soit réellement *append-only*, il suffit de ne déclarer valide que les blocs qui font référence à un bloc précédent connu et valide, via son hash. Ainsi, Alice doit publier par exemple le bloc :



Bob peut alors répondre :

Et Charlie peut surenchérir :



Dans ce contexte, Mallory ne peut pas faire croire à Bob ou Charlie qu'Alice a voté 'retraite':

– en effet, cela aurait changé le contenu du bloc 0 et Bob aurait alors calculé un hash différent, non pas `2a42ced` (qui est effectivement le hash du bloc 0), mais `1bb0dfb` (le hash d'un block 0 hypothétique dans lequel Alice vote 'retraite').
– du coup, Charlie n'aurait pas calculé le hash du bloc 1 de Bob comme `33e93ae` (effectivement le hash du bloc 1) mais `118372f`, le hash d'un bloc 1 hypothétique de Bob où le hash du block 0 est `1bb0dfb`.

En intégrant le hash du block précédent dans le block courant, on s'assure qu'aucun des blocs passés ne peut changer. En changeant le moindre bit d'un block, on modifie son hash dans le bloc suivant, ce qui a pour effet de modifier son hash dans le bloc d'après et ainsi de suite…

Comme on ne peut manipuler le hash en changeant astucieusement l'argument (en théorie), il est impossible de faire une modification qui ne changerait pas le hash du bloc le plus récent.

Ici, non seulement Charlie sait ce qu'Alice et Bob ont voté, mais tout le monde sait qu'il

sait. De manière générale, tout le monde sait la même chose et tout le monde est convaincu que tout le monde sait cette même chose. C'est un *consensus*.

Du moins ça le serait sans deux soucis majeurs :

Rien n'empêche Mallory (la félonne) d'émettre le block suivant à la place de Bob :

```
+-----------------------------------------+
|                *Block 1*                |
|                                         |
| hash précédent: 2a42ced                 |
|                                         |
| Message: Bob vote 'retraite'.           |
+-----------------------------------------+
```

Et Charlie peut de bonne foi tout à fait émettre le bloc :

```
+-----------------------------------------+
|                *Block 1*                |
|                                         |
| hash précédent: 2a42ced                 |
|                                         |
| Message: Charlie vote 'attaquer'.       |
+-----------------------------------------+
```

Car personne ne l'a prévenu qu'il était censé attendre que Bob s'exprime pour parler à son tour.

Nous avons maintenant 3 candidats pour le bloc 1. Comment choisir ?

Authenticité

L'attaque de Mallory est triviale à régler depuis les années 70 et la publication de cryptosystèmes à clef publique **[rivest-1978method]** qui permettent à quiconque de s'assurer de **l'authenticité** d'un message.

Dans un cryptosystème à clef privée, les deux interlocuteurs partagent un secret et l'utilisent pour chiffrer et déchiffrer leurs messages. On parle de cryptographie symétrique. Dans un système à clef publique, chacun à son secret (sa clef privée) qu'il ne partage pas et publie une clef publique, que l'on peut voir comme un cadenas ouvert que tout le monde peut avoir.

Pour chiffrer un message, on prend ce cadenas ouvert et on enferme le message dans une boîte fermée par ce cadenas. Seul le propriétaire du secret pourra ouvrir le cadenas. Ce n'est pas parce qu'on a le cadenas que l'on peut trouver la forme de la clef, sauf à y passer beaucoup de temps.

La magie des chiffres fait que les clefs secrètes et publiques peuvent changer de rôle : la clef privée devient le cadenas et la clef publique devient la clef que l'on distribue à tous. Ainsi, si l'on parvient à ouvrir un cadenas avec la clef publique de quelqu'un, cela signifie que la boîte avait été fermée par le propriétaire de la clef privée. C'est le principe de la signature cryptographique : en chiffrant un message avec sa clef privée, on le signe (puisque tout le monde peut le déchiffrer avec la clef publique).

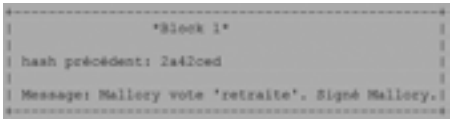
Il suffira d'exiger que les blocs soient signés par leur auteur et Mallory ne pourra plus s'exprimer au nom d'Alice, Bob ou Charlie car elle ne possède aucune de leurs clefs privées.

Seuls restent pour l'instant deux candidats pour le bloc 1, celui de Bob et celui de Charlie.

Disponibilité

Les généraux étant au cœur d'un réseau pair à pair, ils savent que le consensus va mettre du temps à s'établir et qu'il y aura de nombreux moments où toute l'information ne sera pas propagée partout. Ils ont donc décidé de toujours faire confiance à la chaîne de blocks la plus longue. Sachant que cette politique est en place, on a intérêt à abandonner une chaîne plus courte qu'une autre car elle va être ignorée par les autres généraux.

Mallory peut exploiter cela en publiant de nombreux blocs valides à la suite :



Les deux blocs 1 légitimes de Bob et de Charlie n'ont aucune chance d'être pris en compte, car la chaîne émise par Mallory est la plus longue. Mallory peut émettre autant de blocks qu'elle le souhaite pour empêcher que les messages 'attaquer' soient publiés et choisit d'intégrer les messages 'retraite' légitimes des autres utilisateurs. Par exemple, si face à ces revirements Alice change d'avis et émet un bloc 4 valide en votant retraite, Mallory émettra immédiatement des blocs 5, 6, et 7 par dessus pour l'entériner.

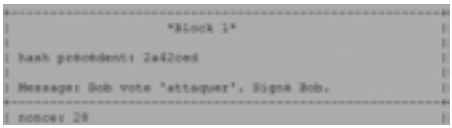
À l'inverse, si Bob propose quand même un bloc 8 proposant une attaque, Mallory va proposer son propre bloc 8 'retraite', et immédiatement après va proposer les blocs 9, 10 et 11 pour que la chaîne intégrant son blok 8 'retraite' soit la plus longue.

La disponibilité est brisée : les généraux ne peuvent pas lire certains messages émis par d'autres.

L'astuce utilisée par la *BlockChain Bitcoin* pour éviter ces attaques consiste à exiger qu'un block contienne une preuve de travail (concept publié vraisemblablement pour la première fois par **[dwork1992pricing]**) pour être valide : il faut maintenant fournir, en plus du blok, un nombre (le nonce) qui lorsqu'on en prend le hash avec le bloc (à quelques détails près) donne un hash qui finit, disons par 0.

Ainsi:

Ne sont pas des blocs valides (les hashes du bloc et du nonce sont respectivement `e091a2d` et `10d8c9e`), mais



et

Sont des blocs valides (les hashes du bloc et du nonce sont respectivement `e4693`**0** et `410699`**0**).

Comme une fonction de hash ne fonctionne que dans un seul sens, les généraux, avant d'émettre un block, n'ont d'autre choix que de tester tous les nonces, ce qui demande du travail. Dans ce cas, il a fallu à Bob 28 essais et 10 à Charlie. Il y a donc toutes les chances que le bloc 1 de Charlie parvienne à Bob avant que celui-ci n'ait fini son calcul, et Bob devra abandonner le travail effectué sur la création du blok 1 et commencer à intégrer son message dans un blok 2 dont il cherchera le nonce.

Comme le bloc 2 de Bob contient le hash du bloc 1 de Charlie, rien de ce qu'a calculé Bob lors de la recherche du nonce du bloc 1 n'est réutilisable pour la recherche du nonce du block 2, même si le message est le même. Un seul bit de différence suffit à changer complètement le hash.

Bob n'a pas intérêt à s'entêter à trouver le nonce de son bloc 1 car les trois autres ont déjà commencé la recherche du nonce du bloc 2 à partir du block 1 de Charlie. S'ils le trouvent avant lui, Bob aura maintenant 2 blocs de retard. La probabilité que Bob prenne du retard en s'obstinant est d'autant plus forte que le nombre de participants est grand. Il n'arrivera alors jamais à s'exprimer puisque seule la plus longue chaîne compte.

Mallory ne peut plus émettre des blocs itératifs pour noyer les messages des généraux légitimes.

Confidentialité

Le système décrit ici ne permet pas la confidentialité, les acteurs sont identifiés et les messages clairs. Ève sait au même titre que les autres généraux quand l'attaque aura lieu.

Bitcoin permet la pseudonymité, chacun n'y est connu que par sa clef publique, mais si l'on connaît la ou les clefs publiques de quelqu'un, on a accès à la liste complète des transactions. Des crypto monnaies comme *Monéro* ou *Zcash* par-

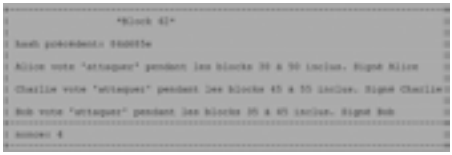
viennent à l'aide de différentes méthodes à la confidentialité des échanges, mais ces systèmes sont beaucoup trop complexes pour être décrit ici.

Au-delà de l'attaque de Byzance

Si une solution simple du style « chacun parle à son tour » vous vient à l'esprit devant ce système, sachez qu'elle a probablement été testée et qu'elle est exploitable par Mallory. Par exemple « chacun parle à son tour » permet à un général félon de ne jamais parler et donc de bloquer toute décision.

Les messages échangés par les généraux peuvent devenir plus complexes. Certains messages peuvent même être échangés entre les généraux sans appartenir à un bloc, pour que le prochain qui a le droit de soumettre un bloc les y intègre. Ainsi, on verrait apparaître un bloc du style :

Mais il faudrait alors dater les messages, pour empêcher Mallory de stocker le message `Alice vote 'attaquer'`. Signé Alice et de le ressortir plus tard quand Alice a changé d'avis, dater les messages, par exemple :



Il faut produire une interdiction d'inclure un message incohérent par rapport à un message inclus dans un block précédent. Ainsi un message `Alice vote 'retraite' pendant les blocs 40 à 45` inclus ne pourrait plus être inséré dans un bloc faisant référence au bloc 42 ci-dessus.

Ce bloc 42 permet à tout le monde d'attaquer au bloc 45, car c'est le bloc le plus petit à partir duquel une majorité a voté 'attaquer'. Mallory ne peut plus rien faire pour empêcher une attaque coordonnée. Avec ce système, les généraux félons ne pourraient gagner que s'ils sont en majorité. Si la majorité est félonne, les autres deviennent les félons…

Cette question du formatage et du contenu acceptable des messages contenu dans un block, ce qu'on appelle la charge utile ou payload, est une question qui peut être abordée dès la compréhension du protocole de création et de maintien de consensus distribué.

La payload

Déclarations

On peut estimer qu'il est possible d'intégrer un message arbitraire dans un bloc. Cela

est mis à profit à diverses fins, comme par exemple lorsque le Cercle du Coin a émis des *Bitcoins* souvenirs en y intégrant le hash d'une photo et d'un morceau de musique : https://lecercleducoin.fr/bitcoin-pluribus-impar/souvenir/.

Certaines pratiques testent les limites de nos systèmes judiciaires : il est possible d'insérer des données illégales dans une *BlockChain*, qui en protégera l'intégrité (il sera impossible de les effacer) et leur disponibilité (il sera impossible de les censurer).

La notion de donnée illégale fait sourire beaucoup d'informaticiens, qui se moquent souvent du concept, soit en cachant un nombre tel que `09 F9 11 02 9D 74 E3 5B D8 41 56 C5 63 56 88 C0` (une clef privée protégeant du contenu multimédia protégée par le DMCA aux USA) partout où ils le peuvent, soit en créant des logiciels tels que πfs [pifs], un système de fichier contenant le nombre π, et donc tous les nombres de longueur finie (il faut juste être patient), y compris tous les « nombres illégaux ».

Si en pratique la plupart des *BlockChains* existantes sont mal adaptées au stockage d'information de masse, la possibilité d'introduction de données portant atteinte à la vie privée, par exemple, peut faire de réelles victimes et ne doit pas être négligée. Il n'existe malheureusement aucun moyen technique de prévenir ce phénomène, sauf peut-être à glisser vers un contrôle total de l'information par l'État.

Une utilisation plus constructive consiste à insérer dans la *BlockChain* des informations du type : dépôt de brevet, actes d'état-civil, etc. Il est possible de prouver grâce à la *BlockChain* l'existence d'une information à une certaine date mais avec une précision variable, de l'ordre de quelques minutes en général. En effet, tout le monde ne reçoit pas les blocs en même temps.

En revanche, si cette information concerne quelque chose qui existe en dehors de la *BlockChain*, alors son exactitude n'est pas garantie. Par exemple, les généraux peuvent utiliser la *BlockChain* pour se partager le butin à venir, mais comme le protocole ne prévoit pas de règles sur la gestion de ces messages, rien ne les empêche de faire des promesses mensongères comme proposer dans un échange des actifs qu'ils ne possèdent pas.

Il faut donc pour être utile que la charge reste dans le domaine défini par le protocole de la chaîne. Dans le cas de *Bitcoins*, par exemple, il s'agit de transactions.

Transactions

Ces transactions sont écrites dans un langage simple, assez similaire dans l'esprit aux protocoles des généraux : pour être valide, un message doit respecter certaines conditions dépendantes du contenu des blocks passés et être signé correctement.

De la même manière que les généraux disent: «`Alice vote 'attaque' pendant les blocks 40 à 45 inclus. Signé Alice`, une transaction *Bitcoin* dit typiquement en substance: `J'utilise les 2.2 Bitcoins qu'on m'avait donné lors de la transaction XYZ pour en donner 1.0 à la clef publique ABC et 1.2 à clef publique DEF. Signé DEF`.

Cette transaction est valide si la transaction `XYZ` est valide, présente dans ce block ou un précédent et donne des *bitcoin*s à la clef publique `DEF`, qui n'ont pas déjà été dépensés par `DEF`.

C'est simple à vérifier. Mais cela ne permet de parler que de *Bitcoins*. Pour échanger une maison, il faudra encore passer chez le notaire, afin que celui-ci s'assure que la maison existe et que les participants sont bien qui ils disent qu'ils sont. Seule la partie intégrité et disponibilité (les points faibles techniques des notaires) est gérée par la *BlockChain*, la partie authentification est partagée entre la *BlockChain* et la vraie vie: la *BlockChain* vérifie la signature, mais l'association entre les signataires et un office notarial, l'acheteur et le vendeur se fait hors chaîne.

La vérification d'une transaction est assez rapide. On peut même borner, en fonction de la taille de la *BlockChain*, le temps que prendra la vérification d'une transaction. On dit en Informatique que le langage permettant d'écrire les transactions a la propriété de ne pas être *Turing-Complet*.

Smart contracts et le théorème de Rice

Ceux qui étudient la complexité algorithmique ont créé des modèles de la calculabilité, pour découvrir ce qu'il est possible de connaître avec une définition mécanique du calcul.

Il s'avère que personne n'a jamais trouvé un seul exemple concret de calcul qui ne pourrait être, en très gros, réalisé par un ordinateur. Le modèle mathématique sous-jacent est celui de la machine de Turing. Elle dispose d'un temps et d'un espace illimité pour donner sa réponse et c'est sur ce détail important que reposent plusieurs mécanismes de sécurité de la *BlockChain*.

Tous ceux qui ont trouvé d'autres modèles de calcul mécanique que celui de la machine de Turing ont fini par démontrer que tous ces modèles étaient équivalents entre eux.

Pour simplifier, la *Turing-Completude* représente un saut dans la complexité d'un langage:

– soit il est tellement simple qu'une machine de Turing n'est pas nécessaire pour résoudre les problèmes (par exemple la vérification des transactions *Bitcoins*) exprimés dans ce langage,
– soit il est suffisamment complexe pour exprimer tous les problèmes expri-

mables dans tous les autres langages *Turing-Complets* connus.

Ce saut de complexité rapidement et la liste des systèmes qui sont Turing Complets sans le vouloir est longue [turing].

Nos généraux ne peuvent ouvrir la voie à des messages même modérément complexes, jouant sur des calculs et des conditions sur le nombre de votes et leur durée, sans ouvrir la boîte de Pandore de la complexité et permettre à Mallory d'exprimer des messages indécidables ou très longs à vérifier.

Pour exprimer les "contrats intelligents", ou *smart contracts*, qui permettent par exemple d'avoir la sécurité de la *BlockChain* pour des applications comme le prêt, les loteries, les assurances, etc. il faut un langage *Turing-Complet*. Les *BlockChain* qui ont fait le choix d'un tel langage (comme par exemple *Ethereum*) subissent le Théorème de Rice qui explique que pour toute propriété non triviale d'un contrat (par exemple, qu'il remplit bien ce qu'on attend d'un contrat de prêt) il est impossible de créer un système automatique qui vérifie si cette propriété est validée ou non pour tous les contrats qui lui sont soumis. Il faut par une laborieuse démonstration mathématique contrôler si le contrat remplit la condition.

On peut avoir confiance dans la *BlockChain*, qui exécutera le contrat sans failles, mais le contrat lui-même peut contenir une porte dérobée (ou une erreur) permettant à son auteur (ou à des pirates) de siphonner les fonds. De nombreux exemples existent déjà.

Vérification formelle

Le spectre du Théorème de Rice hante depuis longtemps les chercheurs et programmeurs informatiques. Les équipements embarqués notamment ne peuvent pas se contenter de programme peu sûr.

Des travaux, certains très aboutis comme la suite logicielle *Coq* [coq] existent. Ils permettent de démontrer des propriétés non triviales d'un programme donné. Cette démonstration est vérifiée par ordinateur et on peut donc accorder le même niveau de confiance à un contrat démontré qu'à une transaction *Bitcoin* par exemple.

Si le langage utilisé dans la *BlockChain* à contrats intelligents la plus populaire (Ethereum) ne se prête pas du tout à ce genre d'exercice, le langage choisi par les experts qui ont créé la *BlockChain* Tezos a été prévu depuis le début pour faire l'objet de ce type de démonstrations.

Il est donc possible d'éditer des contrats sûrs pour peu que l'on rédige, en même temps que le contrat, la démonstration vérifiable de ses propriétés.

La souveraineté

L'État ne doit pas voir une menace dans l'apparition de bases de données non modifiables, non censurables. Au contraire, celles-ci représentent une chance pour la démocratie. L'État et son monopole sur la violence ont encore un rôle à jouer.

Le non-sens de la blockchain privée

Ce rôle n'est pas de garantir l'intégrité, l'authenticité ou la disponibilité des informations de la chaîne car les protocoles cryptographiques s'en chargent mieux que lui. À ce stade, on comprendra qu'une *BlockChain* privée est un non-sens :

– la chaîne n'a d'intégrité que si tout le monde connaît le dernier hash,
– elle n'est authentifiée que si tout le monde peut vérifier les signatures,
– elle n'est disponible que si l'émission des blocs est démontrablement limitée de la même manière pour tous.

Qu'un seul de ces aspects soit laissé à un seul acteur soi-disant de confiance et les propriétés s'écroulent.

La validation des informations off-chain

Le rôle de l'État est autour de la *BlockChain* :

– garantir l'intégrité des informations hors chaîne (mentir quant au résultat d'un match sur un smart contract de pari sportif est une escroquerie),
– garantir l'accès à tous à la *BlockChain* (la neutralité du net existe encore en Europe),
– décourager les comportements immoraux (publier des informations portant atteinte à la vie privée où que ce soit, y compris sur la *BlockChain*, reste punissable),
– etc.

Il est illusoire de légiférer contre la réalité (« interdire le *Bitcoin* », « censurer la *BlockChain* », etc.). Les interactions entre le monde réel et la *BlockChain* (échanges crypto-monnaies contre Euros, saisie de crypto-monnaies, etc.) sont assez nombreuses pour que les forces de l'ordre puissent y travailler utilement.

La maîtrise de la technique

Le vrai défi pour la protection du citoyen est dans la compréhension par le grand public des concepts et techniques ici évoqués et dans l'accompagnement de l'innovation par nos chercheurs et ingénieurs dont le niveau en France ne fait pas rougir.

La souveraineté technologique

Cet accompagnement se fera par le choix de l'État d'une *BlockChain* souveraine. Une *BlockChain* souveraine n'est pas une *BlockChain* que l'État contrôle mais ses choix techniques correspondent à un savoir-faire et une expertise française qui facilitent les comportements utiles à la communauté (comme la vérification formelle des contrats).

À ce titre, il vaut mieux privilégier des équipes françaises de développement et des applications usant d'un langage enseigné et développé en France afin de positionner des entreprises avec lesquelles l'état pourrait mener ses expériences et dont il accompagnerait les développements. Faute de quoi, nous nous retrouverons dans le foisonnement incertain de dizaines de *BlockChain* concurrentes ou pire, avec la *BlockChain* souveraine d'un autre pays et encore pire avec une « *BlockChain* » privée.

Conclusion

Nous avons vu que la *BlockChain* peut stocker et garantir l'intégrité, l'authenticité et la disponibilité d'informations de complexité variable :

– de simples informations déclaratives, comme le vote de généraux, des déclarations d'existence ou du stockage simple,
– des informations modérément complexes comme le vote daté des généraux, les transactions *Bitcoin*,
– des informations les plus complexes comme des contrats intelligents, mathématiquement équivalents à des programmes informatiques.

Nous avons illustré le fait que tant que les protocoles cryptographiques sous-jacents sont sains, la *BlockChain* est sûre mais nous avons aussi illustré ses limites :

– cette sécurité ne s'étend pas aux informations hors chaîne (les notaires ont encore de beaux jours devant eux),
– le Théorème de Rice montre la dangerosité inhérente des contrats intelligents non accompagnés d'une démonstration mathématique.

BIBLIOGRAPHIE

[Lamport et al., 1982]
Lamport, L., Shostak, R., and Pease, M. (1982). The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4 (3):382--401.

[Mickens, 2013]
Mickens, J. (2013). The night watch. ;login: logout.

[Rivest et al., 1978]
Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21 (2):120--126.

[Dwork and Naor, 1992]
Dwork, C. and Naor, M. (1992). Pricing via processing or combatting junk mail. In Annual International Cryptology Conference, pages 139--147. Springer.

[Langdale, 2012]
Langdale, P. (2012). πfs - the data-free filesystem! https://github.com/philipl/pifs.

[Gwern, 2018]
Gwern (2012-2018). Surprisingly turing-complete. https://www.gwern.net/Turing-complete.

[Coq and contributors, 2018]
Coq, A. and contributors (1984-2018). The coq proof assistant. https://coq.inria.fr/.

© Padlock over EU map, GDPR metaphor Par tanaonte

LE DROIT APPUIE LE CONCEPT « PRIVACY BY DESIGN »

Les dispositions législatives et réglementaires évoluent logiquement pour accompagner et sécuriser les relations d'un monde digitalisé.

Le droit national français a pris en compte un nouveau cadre juridique européen en modifiant les divers dispositifs existants. La mise en application du Règlement Général sur la Protection des Données (RGPD), de la directive NIS (Network and Information Security) et de la Loi de Programmation Miliaire (LPM) (Loi de Programmation Militaire) impose de comprendre les risques financiers, techniques et juridiques liés à l'absence de mesures préventives et responsabilise les acteurs des traitements de données. À ce titre, le concept de "Privacy by Design", qui a pour objectif de garantir que la protection de la vie privée dans les nouvelles applications technologiques et commerciales soit prise en compte dès leur conception, est consubstantiel à cet édifice juridique.

Le droit face au Privacy et security by design

Par Myriam Quéméner

Le droit est désormais confronté aux concepts de *privacy et security by design* qui nécessitent des évolutions législatives et réglementaires constantes pour s'adapter au monde désormais digitalisé.

À l'heure d'une société dont l'ADN est devenu numérique, le législateur se devait d'apporter des réponses nouvelles pour protéger les données personnelles des citoyens et des entreprises et assurer la sécurité des systèmes d'information.

MYRIAM QUÉMÉNER

Avocat général près la Cour d'appel de Paris
Docteur en droit

En effet, la protection des données numériques et des systèmes d'information concerne désormais tous les secteurs d'activité humaine et nécessite de faire émerger une véritable culture de la cybersécurité.

Les grandes attaques et défaillances informatiques, dont les médias se font régulièrement l'écho, imposent une prise de conscience grandissante sur les insuffisances de sécurité des outils numériques. Les réponses face aux éventuelles dérives du numérique empruntent largement des réponses inspirées de la *common law* d'où le recours aux termes anglo-saxons de *privacy* et de *security by design*.

Il est intéressant de faire un point afin de cerner la façon dont le droit appréhende ces notions de protection des données personnelles et de sécurité des systèmes d'information dès la conception.

Droit et concept de privacy by design

Définition

Le concept de *"Privacy by design"* a pour objectif de garantir que la protection de la vie privée est intégrée dans les nouvelles applications technologiques

et commerciales dès leur conception et donc dès le départ d'un projet. Il intéresse le traitement des données à caractère personnel et son impact sur la vie privée afin d'apprécier et de minimiser les risques sécuritaires et de non-respect de la réglementation.

Il est étroitement lié à celui *"Privacy by default"*, selon lequel chaque entreprise traitant des données applique par défaut la protection maximale pour chaque nouvelle application, produit ou service traitant des données à caractère personnel. Les entreprises et autres responsables du traitement devraient offrir à leurs utilisateurs ou clients le plus haut niveau possible de protection des données. Le concept de *Privacy by design* permet une protection optimale des données personnelles lors de chaque usage d'une nouvelle technologie.

Grâce au principe de « *Privacy by design* », la protection des données personnelles n'est plus une option pour les entreprises mais une obligation inhérente à chacune de ses activités.

Négliger les questions de *"Privacy"* peut avoir des conséquences graves pour les entreprises : des poursuites judiciaires, des vols de données business, une perte de parts de marchés ou des dégâts pour l'image de marque. Au contraire, une prise en compte optimale de ces questions peut améliorer la réputation de la marque, la confiance des clients et finalement leur loyauté.

L'approche *Privacy by design* permet d'assurer la conformité des traitements de données à caractère personnel. Elle consiste à adapter dès leur conception et par défaut, des mesures organisationnelles et techniques appropriées, afin de limiter la collecte des données au strict besoin du traitement, permettant ainsi de garantir la protection de la vie privée et des libertés fondamentales.

Par exemple, pour assurer le développement du marché des objets connectés, il est nécessaire voire indispensable d'assurer aux individus le respect de leurs droits et de rassurer le consommateur. Selon une étude de la société Havas, alors que la plupart des consommateurs interrogés reconnaissent les avantages des objets connectés, 78 % craignent néanmoins un risque accru pour leur vie privée.

La protection de l'information devient une préoccupation de certaines grandes entreprises. L'essor du commerce et, à partir du XIX^{e} siècle, de l'industrie moderne (générant des données qu'il était indispensable de maintenir confidentielles et inaccessibles aux concurrents) ont étendu cette préoccupation aux grandes entreprises qui devaient se protéger notamment contre les risques d'espionnage industriel.

Traduction juridique par le RGPD

L'article 25 du Règlement Général de la Protection des Données[1] (RGPD) intitulé « Protection des données dès la conception et protection des données par défaut » prévoit le principe de « *Privacy by design*[2] ». Le règlement européen sur la protection des données vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations pesant sur les responsables de traitements et les sous-traitants. L'application de ce principe permet donc de mettre en œuvre des mesures préventives limitant les risques de violation des données personnelles. Les mesures doivent empêcher la collecte de données personnelles sans raison légitime d'une part et la suppression d'information d'une base de données s'il n'y a pas ou plus de raisons de la stocker d'autre part.

Le principe du « *Privacy by design* » est la réponse aux problèmes du Big Data et de la fuite massive de données liées à

(1) Le Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

(2) J.-L. Sauron, Le règlement général sur la protection des données, règlement (UE) n° 2016/679 du 27 avril 2016 : de quoi est-il le signe ? : Comm. com. électr. 2016, étude 16).

Les dispositions du RGPD concourent à une réponse globale liant stratégie d'entreprise, mesures structurelles et d'organisation, et une inscription dans un corpus juridique visant à une homogénéité des dispositifs de protection.

© GDPR General Data Protection Regulation Business Internet Technology Concept Par Sikov

l'automatisation de la collecte de données personnelles. Le non-respect de ces exigences expose les entreprises à une sanction pouvant aller jusqu'à 4 % de leur chiffre d'affaires global. À ce risque financier s'ajoute un risque d'image. Les sanctions sont en effet accompagnées d'une publication sur le site de l'autorité du pays (la CNIL en France), ce qui pourrait refroidir les investisseurs, connus pour préférer les entreprises qui se protègent sérieusement.

Au niveau national, la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles a procédé aux adaptations nécessaires, en vue de prendre en compte ce nouveau cadre juridique européen, en modifiant plusieurs volets de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(3) https://www.cnil.fr

La CNIL[3] vient de dresser un premier bilan de l'application du RGPD. Elle a reçu 742 notifications de violations concernant les données de 33 727 384 personnes, situées en France ou ailleurs. Le secteur de l'hôtellerie est concerné par 185 d'entre elles. Les causes de ces violations résident, pour plus de la moitié, dans des actes de piratage, des logiciels malveillants ou de l'hameçonnage. En vue de prévenir les violations de données, la CNIL rappelle la nécessité de mettre en œuvre des méthodes de gestion des risques. Elle encourage notamment à effectuer régulièrement des mises à jour de sécurité sur les systèmes d'exploitation, les serveurs applicatifs ou les bases de données.

Le droit face au security by design

Security by design et cybersécurité

Il existe une cohérence entre privacy et *security by design* car cette approche *Security by design* offre aux industriels une plus grande sécurité juridique et a pour objectif de réduire les coûts. Rappelons que le défaut de sécurité d'un traitement de données à caractère personnel est sanctionné par l'article 226-17 du Code pénal.

(4) Sécurité des données - Cyber-sécurité : l'âge de raison - Étude par Matthieu Bourgeois et Denis Pélanchon et Franck Régnier-Pécastaing : Revue Internationale de la Compliance et de l'Éthique des Affaires n° 1, Mars 2018, étude 34.

Les grandes quantités de données produites et reçues, qui sont désormais traitées par des machines (logiciels, serveurs, etc.), sont de plus en plus souvent accessibles à distance (via Internet ou des réseaux locaux). Ceci facilite la tâche des attaquants qui, en exploitant les failles de sécurité de ces machines, peuvent accéder à distance à la quasi-totalité des données de l'organisation ciblée. De ce fait, celle-ci encourt des risques démultipliés, aussi bien dans leur nature que dans leurs impacts[4].

Les réponses juridiques

La sécurité des systèmes d'information est au cœur de la gouvernance des entreprises. La législation tant française qu'européenne a évolué en ce sens. La nécessaire

démarche « *security by design* » n'est pas un sujet réservé uniquement à certains experts mais doit être l'affaire de tous. À défaut de l'être, l'organisation ne parviendra pas à élever le niveau de protection de ses données de manière satisfaisante. Pour y parvenir, il faut inscrire la protection des données dans une démarche globale impliquant la définition préalable d'une politique et d'une gouvernance de la sécurité. Celle-ci permettra d'identifier au préalable la menace pour pouvoir mieux y répondre.

La directive sur la sécurité des réseaux et de l'information[5] (SRI) ou directive NIS (« Network and Information Security »)

(5) Directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

La directive prévoit des obligations en matière de sécurité interne incombant aux « opérateurs de services essentiels » et aux « fournisseurs de services numériques ». Dans un certain nombre de secteurs critiques tels que l'énergie, les transports, les services financiers et la santé, les États membres devront identifier, sur la base de critères énoncés dans la directive, les opérateurs de services essentiels qui seront soumis à des exigences et à une surveillance renforcées. Des obligations moins lourdes pèseront sur les fournisseurs de services numériques, à savoir les moteurs de recherche, les services en nuage et les plates-formes de commerce électronique. Les micro-entreprises de ces secteurs sont toutefois exemptées, au même titre que les réseaux sociaux, comme Facebook et Twitter.

(6) Sécurité des données - Cyber-sécurité : l'âge de raison - Étude par Matthieu Bourgeois et Denis Pélanchon et Franck Régnier-Pécastaing : Revue Internationale de la Compliance et de l'Éthique des Affaires n° 1, Mars 2018, étude 34.

La directive oblige aussi les opérateurs concernés à signaler aux autorités nationales compétentes les incidents de sécurité majeurs dont ils sont victimes. Elle devrait surtout contribuer à rendre les partenaires européens plus coopératifs et on notera que le dispositif français met déjà en œuvre l'essentiel des mesures préconisées[6].

(7) https://www.ssi.gouv.fr

Les principaux apports de cette directive sont la désignation d'« autorités nationales compétentes » et d'un « point de contact unique » à savoir en France l'ANSSI[7].Les États membres devront désigner une ou plusieurs autorités nationales spécialisées en matière de sécurité des réseaux et des systèmes d'information.

La loi n° 2018-133, du 26 février 2018, présente les mesures de transposition de la directive NIS dans la législation nationale. Le décret n° 2018-384 du 23 mai 2018 détaille les modalités d'application des obligations législatives et liste les secteurs, les types d'opérateur et les services essentiels concernés. Enfin, l'arrêté du 13 juin 2018 fixe les modalités de déclarations des incidents de sécurité.

La digitalisation des entreprises et la mise en application de nouvelles réglementations (RGPD (Règlement Général sur la Protection des Données), NIS (Network and Information Security), LPM (Loi de Programmation Militaire), etc.) imposent, d'une part aux professionnels de la cybersécurité de comprendre les enjeux réglementaires et juridiques, et d'autre part aux responsables juridiques d'avoir une vision plus avancée des enjeux de sécurité informatique. Les risques financiers, techniques et juridiques doivent aussi être clairement identifiés par les directions générales. Les entreprises et les entités publiques prennent conscience qu'il faut avoir une vraie compréhension des aspects techniques, organisationnels et juridiques de la protection des données.

Conclusion et perspectives

(8) M. Quéméner , le droit face à la disruption numérique, Gualino Lextenso 2018

(9) Petit C., « Cybersécurité, le risque le nouveau concept clef du RGPD et de NIS », Revue Expertises, février 2018, p. 76 et s.

En apparence différents, le RGPD et la directive NIS ont un point commun important explicité dans le tableau ci-dessous[8], à savoir la prise en compte du risque lié au numérique, évoqué d'ailleurs à 78 reprises dans le RGPD et à 39 reprises dans la directive NIS[9].

Au-delà des textes, les concepts de *privacy* et de *security by design* constituent aussi un changement de mentalité. Pour respecter les obligations réglementaires, les acteurs doivent anticiper les risques numériques dans le cadre d'une stratégie globale de cybersécurité.

Directive NIS	RGPD
Protection des réseaux et des systèmes d'information	Protection des données à caractère personnel
Mesures préventives techniques et organisationnelles (identification des risques, mesures préventives, continuité du service)	Mesures techniques et organisationnelles (sécurisation du traitement de données, analyse d'impact, obligation de rendre des comptes)
Notification à l'ANSSI en cas d'incident affectant la sécurité des réseaux et des Systèmes	Notification des failles de sécurité dans un délai maximum de 72 heures
Pas de sanction prévue, mais sanctions prévues par le Code pénal	Sanction administrative jusqu'à 200 000 euros ou 4 % du chiffre annuel

L'AUTEUR

Myriam Quéméner, magistrat judiciaire , docteur en droit, après un détachement au ministère de l'intérieur comme conseiller juridique en matière de cybercriminalité est actuellement avocat général près la cour d'appel de Paris. Elle est chargée du contentieux économique et financier et assure la veille juridique en matière de droit du numérique pour le parquet général de la Cour d'appel.
Membre de la chaire Cyber de Saint-Cyr, elle a publié récemment « le droit face à la disruption numérique « aux éditions Gualino Lextenso (2018).

© Fotolia

UN ENVIRONNEMENT NUMÉRIQUE PROBATOIRE

La complexité des architectures de communication, un Internet multidimensionnel et l'émergence d'objets connectés conditionnent l'interaction d'un individu avec son environnement numérique. On peut dès lors réaliser l'identification et la collecte des traces laissées par une personne sur une scène de crime ou lors d'un périple délictuel. Une signature fréquentielle et la localisation d'un dispositif entrent dans un champ probatoire. La difficulté pour un enquêteur sera de valoriser les informations captées en distinguant leur pertinence, au besoin par assistance logicielle, et en les associant à un portrait socio-psychopathologique d'un suspect ou aux éléments d'une scène d'investigation et en les protégeant de toute pollution numérique. L'apport de l'enquêteur à la manifestation de la vérité combine cette dextérité à extraire les données numériques probantes et à les inclure dans un formalisme procédural.

Bâtir
une enquête 4.0

Par François Bouchaud

L'investigation judiciaire a une valeur, un sens et une portée qui est celle de l'action. Avec le développement exponentiel de l'Internet des objets (IoT), celle-ci se remodèle, se restructure et se définit en fonction d'une autre échelle : un écosystème numérique global. Au travers de la domotique, de la sphère de la santé, de l'usage d'appareils ménagers, d'automobiles ou d'équipements urbains, nos existences se digitalisent et s'interconnectent. Les ensembles de données qui apparaissent, de la collecte initiale par l'objet connecté jusqu'à la constitution de données à plus forte valeur ajoutée, constituent une nouvelle source d'investigation.

FRANÇOIS BOUCHAUD

Lieutenant de gendarmerie
Officier criminalistique
Département Informatique-Electronique
Institut de Recherche Criminelle de la Gendarmerie Nationale

Au centre de l'investigation, les éléments matériels de l'infraction se distinguent ; ce sont sur ces données matérielles et l'environnement numérique de l'infraction que s'énoncent des preuves. Toutes les données sont ainsi considérées comme précieuses par définition.

La compréhension de l'élément moral de l'infraction a également sa place dans l'architecture de l'ensemble des données. Elles sont des indicateurs des comportements d'un individu et l'intimité numérique de ce dernier peut être un intéressant reflet de son portrait socio-psychopathologique, surtout lorsque les données sont collectées dans la durée et croisées avec d'autres informations. L'exploitation et le croisement de sources disparates vont améliorer la connaissance de la scène d'investigation. Replacé dans une vision

différente, un relief se dessine, dont l'architecture était à peine perçue ; de nouvelles preuves s'imposent dont on ne soupçonnait pas « l'amplitude ».

Les objets connectés permettent au numérique de conquérir le dernier territoire sur lequel il n'avait pas encore d'emprise : le réel. La contrainte des formats perdant en influence, les objets connectés peuvent être invisibles à l'œil nu et les obstacles même à la connectivité s'effacent. Action continue, de recoupement, de valorisation d'informations en temps réel, c'est tout un déplacement de perspective. Ce mouvement plus flexible, d'analyse, de compréhension de preuves digitales par l'investigation numérique s'affirme, non seulement pour édifier une réponse judiciaire, mais pour prévenir la commission de l'infraction.

Avec l'Internet des objets, plusieurs natures de matériels doivent être considérées : les objets connectés à Internet, les terminaux communicants comme les tablettes ou les smartphones, le M2M qui définit la communication entre machines sans intervention humaine. L'hétérogénéité des dispositifs connectés, la complexité des architectures de communication, le foisonnement des approches techniques bouleversent les habitudes et les manières de raisonner. C'est un Internet multidimensionnel, un environnement en interaction avec et entre les objets physiques et leur représentation virtuelle. Il redéfinit les méthodes traditionnelles d'investigation connues en téléphonie ou en informatique. L'analyse sur ces objets contribue avec d'autres procédés d'investigation, et selon ses méthodes propres, à obtenir des informations exploitables et à les rendre intelligibles.

De nouvelles preuves

L'environnement infractionnel, né avec l'infraction, en est inséparable. L'Internet des objets est marqué par le développement des réseaux, des partenariats et d'interrelations complexes. La multiplication de capteurs dans l'espace public et privé rend possible l'obtention de données qui permettent d'analyser les activités, les comportements sans qu'un individu soit informé de cette collecte, de son ampleur et de ce qui peut en résulter. Différents types de capteurs, actionneurs ou points d'interconnexion, interagissent avec l'environnement et sur les conditions d'utilisation et d'opération des objets. Les informations reçues sont centralisées, collectées, stockées et produites en nombre croissant dans un Cloud dédié grâce à des traitements automatisés et au recours aux technologies de l'intelligence artificielle. Elles acquièrent une représentation d'un contenu et contribuent à le modifier en tissant, avec cet environnement, des liens constants ou occasionnels d'une diversité remarquable. L'utilisateur accède à ce contenu traité et valorisé par des interfaces telles qu'un *smartphone* ou un portail web. Il en va de même de montres et bracelets connectés, d'immeubles connectés ou encore d'assistants vocaux. Les données

brutes doivent être distinguées des données lissées ou interprétées. L'analyse des données de fonctionnement d'un objet, croisées avec l'ensemble des autres données environnementales et de contrôle, est le fondement de l'investigation. L'enquêteur y revient sans cesse, car c'est là que l'essentiel est donné, que se noue et se dénoue l'enquête.

De nouveaux procédés d'investigation

Une investigation ordonnée est essentielle à la manifestation de la vérité. Sur une scène d'investigation contenant des dispositifs IoT, l'enquêteur réalise des opérations techniques. Il préserve, fige la zone d'étude et consigne méthodiquement tout indice matériel disponible. Il procède à l'identification et à la collecte des traces laissées par l'auteur de l'infraction et choisit des données longitudinales distinctes selon le principe de Locard[1], puis les priorise. Les particularités de la scène d'investigation et les caractéristiques techniques des objets retenus guident le travail de l'enquêteur. Une montre connectée découverte sur une scène de crime, déconnectée de l'infrastructure IoT, garde des informations localement. L'empreinte numérique et la cartographie des lieux de commission de

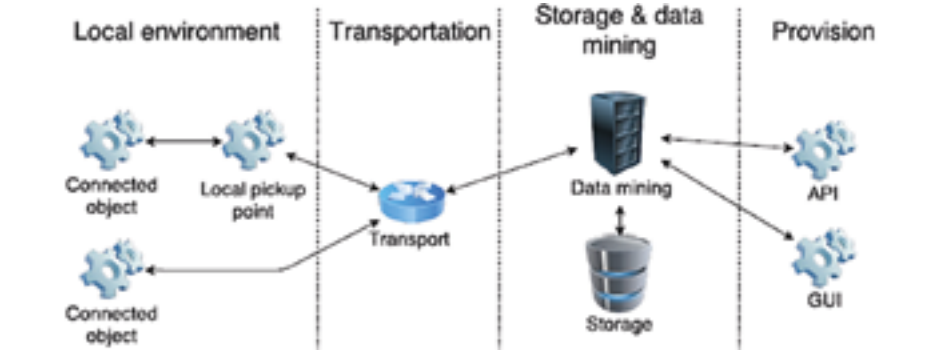
(1) Le principe d'échange de Locard, énoncé par le pionnier de la police scientifique Edmond Locard, détermine que lorsque deux corps entrent en contact l'un avec l'autre, il y a nécessairement un transfert entre ceux-ci. En d'autres termes, lorsqu'un acte criminel se produit, l'individu responsable laisse des traces de sa présence et emporte avec lui des traces du lieu où il se trouvait.

l'infraction sont des sources d'investigation. L'étude de la signature fréquentielle offre un instantané des dispositifs actifs et présents sur la zone. Pour obtenir l'empreinte des objets inactifs ou semi-connectés, des commandes externes de *« réveil »* peuvent être concomitamment mises en œuvre. La localisation des dispositifs est également réalisée à partir des signaux reçus par un processus de *netmonitoring*. Cette cartographie va être affinée et complétée par des mesures en plusieurs points et par une investigation terrain. À l'enquêteur d'étudier les données disponibles, de mieux comprendre l'intervention des objets dans la commission de l'infraction et son environnement immédiat. Les dispositifs sont reconnus et étudiés en particulier par les éléments d'identification physique des objets, notamment le FCCID[2] ou l'adresse MAC et par leur signature électromagnétique unique. Enfin, une phase de recoupement d'informations s'appuyant sur une approche par graphe des dépendances est opérée.

(2) L'Identifiant de Commission de Communications Fédéral est un ensemble de caractères alphanumériques qui identifie chaque modèle de dispositif sans fil produit par une entreprise et mis en vente aux USA.

De nouveaux enjeux

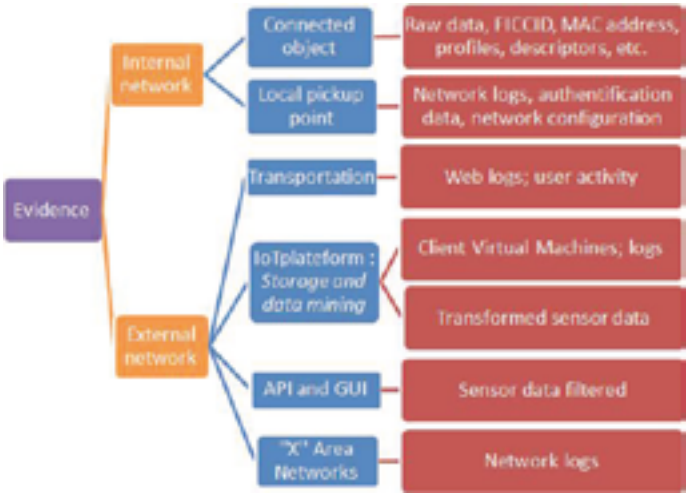
Les dispositifs communicants sont un tout. Ils se nourrissent des données et en augmentent en retour le volume. Les données émises deviennent si volumineuses, variées et véloces qu'il devient difficile d'en connaître la totalité. Cette massification est rendue possible par la conjonction de deux facteurs : une simplicité d'accès aux données numériques et son coût marginal. Néanmoins, l'enquêteur n'est pas abandonné dans un face-à-face avec des données brutes ; les données non structurées ne seraient d'ailleurs pas pertinentes par elles-mêmes. Elles deviennent créatrices de valeur une fois analysées et en gagnent



en fonction du contexte dans lequel elles sont utilisées. Si brève soit-elle, la captation de l'infraction par les périphériques et le positionnement stratégique d'une information, rendent indispensable une connaissance approfondie des matériels en contact avec l'auteur de l'infraction et de son fonctionnement nominal.

Bien entendu, la multiplicité des informations disponibles et de leur expression est aussi un défi pour l'enquêteur. Il n'en demeure pas moins que, dans la mesure où l'enquêteur s'efforce d'y cerner des éléments matériels, l'exploitation des données collectées tient à leur pertinence, leur accessibilité, leur localisation et leur nature.

En premier lieu, la pertinence de l'information recueillie s'entend de sa proximité temporelle et spatiale à l'infraction. L'identité d'une information captée offre la possibilité de dater un fait, de déterminer sa durée et un lieu en fonction de l'identité, de l'interactivité, du « *shadowing* », de la sensibilité et de l'autonomie d'un matériel donné. La connaissance de la distance de la donnée à l'infraction est en outre essentielle pour la fiabilité de l'investigation. Encore faut-il pouvoir l'intégrer dans un champ analytique au sein duquel la trace retenue constitue l'une des clefs possibles de compréhension de l'infraction. Ainsi, par exemple, une variation de tension électrique perçue par un capteur peut traduire une modification d'une température et



donc l'émission d'une donnée par un objet connecté. De simples données anodines comme le nombre de pas quotidiens ou un rythme cardiaque peuvent devenir des indicateurs avancés de certains comportements. Ces données brutes peuvent paraître anodines ; accumulées sur le long terme, elles peuvent cependant très facilement être utilisées pour suivre, analyser, sonder et cibler un profil criminel. L'information contextualisée peut également dater un évènement ou un fait.

En deuxième lieu, s'agissant de l'accessibilité à la donnée, son analyse immédiate peut être différée par des systèmes de chiffrement ou de sécurité.

En troisième lieu, les actes techniques à entreprendre, le placement sous scellé d'objets connectés est conditionné à la portabilité des données. Il s'agit de récupérer des données qui concernent la scène d'infraction, afin d'éviter qu'elles ne se trouvent *« enfermées »* dans un univers technologique donné. Un stockage à distance impose une identification précise des dispositifs locaux présents lors d'une infraction et l'intervention d'un opérateur Cloud. Nombre d'objets connectés décentralisent le stockage d'informations vers les points d'interconnexion selon un procédé dit de *« fog computing »*, comme par exemple les assistants vocaux. Or, l'investigation des objets connectés est souvent sous-exploitée, en particulier sur les passerelles. En effet, des données numériques sont notamment générées dans les périphériques qui administrent ces dispositifs. Les journaux d'évènements et l'observation de l'évolution des données sur une durée constituent également des données indirectes exploitables dans le cadre de l'enquête. Parmi les prix à payer pour la décentralisation de l'investigation vers des périphériques, il en est un qui doit être relevé : alors que l'enquêteur découvre l'importance de l'investigation de l'IoT, le danger est de ne pas recouper les données, d'isoler et d'escamoter l'analyse derrière une démarche atone de connaissance d'une scène d'investigation.

Partout et en toute situation, l'enquêteur doit s'attacher à confronter les données collectées. La confrontation de moyens d'investigation est un défi collectif de mise à profit de toutes les informations disponibles. Et au-delà de l'évidence première, l'analyse de données clairsemées doit procéder d'une déduction logique et fonctionnaliste. En dernier lieu, la nature de la donnée, dont dépend son objectivité, résulte de son caractère direct, de l'intervention humaine et de son interprétation. Suscitant parfois des paradoxes ou des contrecoups inattendus, l'investigation sur des objets connectés doit bénéficier à la compréhension de la vérité judiciaire, où elle trouvera à la fois son terme et son accomplissement selon le double sens du mot fin.

L'AUTEUR

Lieutenant de gendarmerie, François BOUCHAUD est officier criminalistique au sein du département Informatique-Electronique de l'Institut de Recherche Criminelle de la Gendarmerie Nationale. Doctorant en informatique à l'Institut de Recherche sur les Composants logiciels et matériels pour l'Informatique et la Communication Avancée, il est diplômé de l'École Supérieure d'Électronique de l'Ouest et de l'École Centrale Paris.

PERCEV@L : UNE PLATEFORME DE SERVICE AUX CITOYENS

L'essor du commerce en ligne repose sur la confiance du consommateur. Les nouvelles directives européennes sur les services de paiement entérinent cette acception quant au contentieux des usages frauduleux des cartes bancaires. La disparité des auteurs des infractions, du niveau de préjudice et des catégories de plaignants rendait difficile pour les juridictions de jugement la mesure de l'atteinte réelle de ces faits.

La création d'un téléservice, ayant les garanties d'un site public, organisé pour répondre à un impératif d'intuitivité, d'intelligibilité et d'authentification répond à une attente forte des citoyens. Ils peuvent en conséquence obtenir la preuve opposable aux tiers de leur signalement et sont assurés d'une suite judiciaire. En effet, la concentration initiale des procédures sur un seul parquet donne de la cohérence à ce dispositif et à la réponse pénale.

La plateforme PERCEVAL

Par Cyril Piat

Dans la légende, le roi Arthur réunit ses chevaliers afin d'être éclairé par leurs points de vue et leurs conseils. Loin de la fable épique, la plateforme PERCEVAL[1] cherche toutefois à faciliter la prise de décision face au contentieux extrêmement massif et surtout peu ou mal traité des usages frauduleux de cartes bancaires (I). Ouvert depuis le 6 juin 2018, PERCEVAL est un téléservice destiné aux citoyens. Il leur permet de signaler directement en ligne aux forces de l'ordre ce type d'infraction lorsqu'ils en sont victimes. Ces formulaires sont centralisés et exploités par le service central de renseignement criminel de la gendarmerie nationale (SCRCGN), basé à Pontoise (95).
La plateforme vise d'une part à simplifier les démarches des victimes (II), d'autre part à améliorer la réponse étatique, répressive et préventive (III). Aboutissement de travaux menés avec de nombreux partenaires et autorités, PERCEVAL constitue également une étape complémentaire dans la transformation numérique du ministère et de la gendarmerie en particulier.

(1) L'acronyme PERCEVAL renvoie à Plate-forme Électronique de Recueil des Coordonnées bancaires et de leurs conditions d'Emploi par les Victimes d'Achats frauduleux en Ligne.

CYRIL PIAT
Colonel de gendarmerie
Chef du projet PERCEVAL

I- Les usages frauduleux de cartes bancaires

Avant d'aborder le service rendu par la nouvelle plateforme, il est nécessaire de rappeler dans les grandes lignes l'évolution de ce contentieux particulier des usages frauduleux de cartes bancaires.

Depuis 2001, avec la loi sur la sécurité intérieure puis au travers de nombreuses

évolutions dont celles portées par l'emblématique loi sur la confiance dans l'économie numérique, le législateur n'a cessé de veiller aux garanties du particulier consommateur. Une telle posture était nécessaire pour autoriser sans retard l'essor du commerce en ligne. En matière de paiement à distance par carte bancaire, ces garanties ont consisté principalement en la création d'une obligation pour la banque de rembourser son client en cas de fraude. La nouvelle directive européenne sur les services de paiement, entrée en vigueur le 13 janvier 2018, rappelle qu'il s'agit d'un principe désormais standardisé au niveau de l'Union.

La situation a toutefois changé depuis une dizaine d'années, avec deux phénomènes parallèles : d'une part, la démobilisation des services d'enquête face à des préjudices individuels souvent peu élevés, avec une relativisation des atteintes du fait de l'obligation légale de remboursement des victimes-porteurs de carte ; d'autre part, la disponibilité croissante de références de cartes bancaires détournées, directement mises en vente sur internet.

Ce dernier point s'explique par les campagnes malveillantes de phishing de plus en plus sophistiquées, intégrant des stratagèmes parfois en plusieurs étapes pour mieux saper la vigilance des internautes. Au-delà, des vols de données chez des e-commerçants ou chez des opérateurs de services, soit par piratage, soit par indélicatesse d'employés ont pu expliquer certaines atteintes très diffuses. La popularité croissante du Darkweb a permis également le commerce très étendu de ces identifiants de moyens de paiement. Sur certains forums francophones, on dénombre aujourd'hui plus de 1 400 fils de discussions sur les pratiques criminelles visant les cartes bancaires détournées.

Le monde des banques et des prestataires de paiement est très vigilant et réactif sur l'analyse de ces fraudes. Sous l'égide de la banque de France, l'observatoire sur la sécurité des moyens de paiement assure une veille technique et publie des statistiques issues des banques et du e-commerce. De 2013 à 2016, le nombre d'usages frauduleux a doublé avec désormais 1,9 million de fraudes par an. Ce chiffre comporte toutefois les nombreuses tentatives bloquées par les acteurs économiques, grâce aux algorithmes de scoring[2], imperceptibles par les usagers porteurs de carte.

Le contentieux est enfin mal traité. Ce type de fraude apparaît, à la vue des enquêtes fructueuses, comme le fait d'individus extrêmement réitérants. Or, les plaintes des victimes sont reçues de manière très éparpillée avec des préjudices individuels en

(2) Le scoring est la détection, à partir de critères variés, de comportements anormaux susceptibles de caractériser une fraude. L'achat en ligne de 15 téléphones portables « dernier cri » auprès d'un même commerçant devrait générer une alerte de sécurité conduisant à suspendre la transaction, le temps de vérifier directement l'achat en cours auprès du client.

deçà des seuils de classement usuellement recensés. Seule la capacité à recouper plusieurs dossiers permet à une juridiction de jugement de mesurer l'atteinte réelle causée par un fraudeur, en préjudice cumulé et en nombre de fraudes. En 2016, les enquêteurs du centre de lutte contre les criminalités numériques (C3N) avaient identifié et interpellé un couple ayant dépensé 90 000 € en trois mois à partir d'identifiants de cartes bancaires compromises.

II- La facilitation des démarches citoyennes.

Ce tableau brossé, il faut retourner auprès de l'usager se découvrant victime d'un usage frauduleux de sa carte bancaire et considérer les démarches que celui-ci doit réaliser dans son propre intérêt.

Le plus urgent est de signaler sans tarder à sa banque la compromission de sa carte. L'abstention d'une telle information conduit à être considérée comme responsable des fraudes ultérieures qui pourraient intervenir avec cette carte.

Une fois la situation sécurisée, l'usager peut souhaiter exposer sa situation, soit en vue d'un remboursement, soit en vue de permettre l'identification judiciaire de l'auteur des faits. C'est principalement pour faciliter la poursuite simultanée de ces deux finalités que PERCEVAL peut utilement constituer l'étape suivante : une déclaration aux forces de l'ordre par le biais de la plateforme permet non seulement de trouver un formulaire complet mais également de ne pas saisir deux fois les informations essentielles, un récépissé reprenant ces dernières étant délivrées automatiquement au signalant. D'une part, l'usager évite la saisie des mêmes informations sur une seconde correspondance pour la banque, d'autre part la banque pourra s'assurer auprès de la gendarmerie de l'authenticité de ce document.

Il est ici nécessaire de rappeler qu'en aucun cas un remboursement n'est suspendu à un dépôt de plainte ou à un signalement du porteur de carte auprès des forces de l'ordre. Notons simplement qu'une telle démarche est souvent perçue comme un gage de bonne foi par le service contentieux de la banque. Il ne faut en effet pas méconnaître les cas réguliers de fraude déclarative aux banques en vue d'un remboursement indu.

III- Le traitement des signalements

Maintenant que l'usager a fait l'effort de réaliser son signalement aux forces de l'ordre, quelles suites vont être réservées à ce dernier ?

Tout d'abord, comme cela a été présenté à la commission informatique et libertés[3], l'exploitation des signalements ne visera que l'identification d'auteurs d'infraction et la diffusion de

(3) Voir l'arrêté du 23 mai 2018 relatif à PERCEVAL et la délibération de la Commission informatique et libertés publiée au JO le même jour (ie 25 mai 2018).

EN QUOI CONSISTE PERCEV@L ?

Facilement accessible au travers du site service-public.fr , l'application offre une trame complète guidant le signalant dans un processus en quatre étapes (fil d'Ariane). Le téléservice hérite de toutes les garanties et mises à jour du site service-public (intelligibilité, accessibilité pour les mal voyants, proximité de multiples informations en cas d'hésitation, évaluation de satisfaction, etc.). Afin de dissuader les déclarations fantaisistes ou irresponsables, l'usager doit s'authentifier pour initier un signalement. La première étape est donc une authentification par Franceconnect (recours à des identifiants fiscaux, de sécurité sociale ou encore de l'identité numérique fournie par la Poste).
Après avoir franchi les trois étapes suivantes (coordonnées personnelles, relation des usages frauduleux et émission facultative d'hypothèse sur les circonstances de compromission de la carte), la victime n'a plus qu'à relire et valider son signalement. Elle reçoit alors un récépissé reprenant précisément les éléments renseignés. Ce document peut utilement être adressé par l'usager à sa banque.

notes d'analyse à vocation préventive. Bien que la prescription de l'action publique face à un usage frauduleux de carte bancaire soit désormais de 6 années après les faits, la plateforme effacera automatiquement les signalements au terme de deux ans après leur versement par la victime.

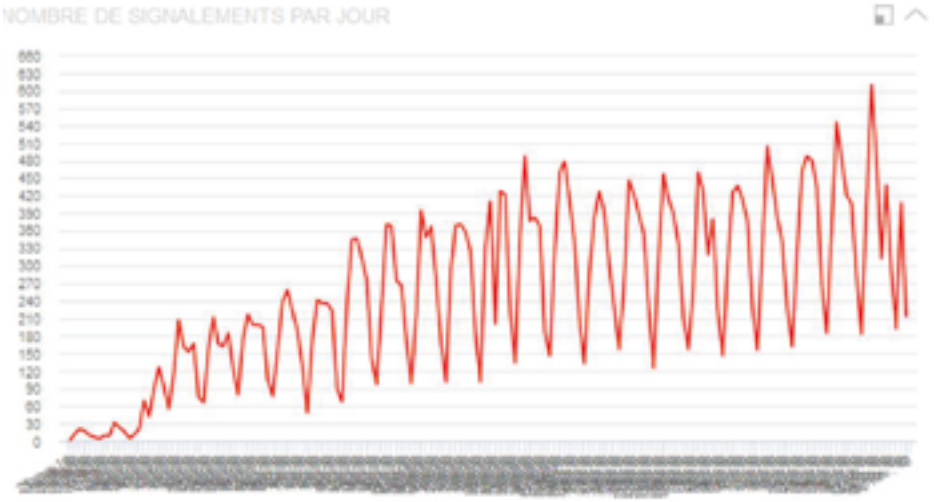
Ensuite, s'est posée la question de la compétence d'un parquet unique, chargé de la direction des enquêtes, pour permettre une analyse et des recoupements judiciaires. Anticipant la réforme législative en cours[4], la Chancellerie a autorisé le parquet de Pontoise à asseoir ce contrôle et à financer les premiers actes d'investigations jusqu'à ce que ressorte un critère territorial lié à un mis en cause.

(4) Projet de loi de programmation 2019-2022 et de réforme de la Justice, examen actuel au Parlement.

Concrètement, les enquêteurs identifient en premier lieu les e-commerçants les plus concernés par les transactions déclarées frauduleuses. Sur la base des transactions identifiées, des recoupements sont réalisés à l'aide de données complémentaires détenues par les sociétés commerciales. Les enquêteurs poursuivent alors des investigations judiciaires plus classiques tant en direction de la commande passée que des lieux de livraison. L'enjeu pour les enquêteurs du SCRCGN n'est pas de conduire l'enquête jusqu'à l'interpellation mais de transmettre des dossiers nombreux aux services et unités territoriaux de police et de gendarmerie dès qu'au moins un mis en cause est identifié.

PERCEVAL EN CHIFFRE

Ce sont près de 192 000 dénonciations d'usages frauduleux qui ont été recueillies depuis l'ouverture de la plateforme. Du 22 mai 2018 jusqu'au 20 novembre 2018 ont été ouvertes 60 Enquêtes dont la moitié est déjà diffusée vers les services territoriaux de police et de gendarmerie.



© gendarmerie nationale.

Nombre de signalements journaliers reçus sur PERCEVAL, depuis la création de la plateforme. Les pics hebdomadaires de faible valeur correspondent au gel des écritures bancaires – compensation au cours du week-end.

Conclusion

PERCEVAL est la cinquième plateforme régalienne de services aux citoyens dans le domaine de la sécurité. Après PHAROS (signalement des contenus illicites publiés sur internet), pré-plainte en ligne (recueil de premiers éléments et obtention d'un rendez-vous physique), opération tranquillité vacances (signaler l'inoccupation de son domicile pendant les congés) et la brigade numérique (accueil multi-services et dématérialisé du public), PERCEVAL constitue la première plateforme destinée aux victimes d'infraction.

Le succès de PERCEVAL justifie pleinement le déploiement de futurs outils similaires. En particulier, le déploiement de THESEE, dédiée au recueil de plaintes en matière d'escroquerie en ligne, est annoncé en 2019.

L'AUTEUR

Au terme de trois commandements variés (GM, école, GD), le colonel PIAT a servi cinq ans comme chef de section « cybercriminalité, criminalistique et renseignement judiciaire » au sein de la sous-direction de la police judiciaire. Titulaire du brevet de l'enseignement militaire supérieur, il a suivi le DU de cybercriminalité de l'université de droit de Montpellier. Il sert depuis 2015 au centre de lutte contre les criminalités numériques de la gendarmerie nationale.

Page d'accueil de la plateforme PERCEVAL

Page d'orientation de l'usager sur Service-public, en vue de se rendre sur la plateforme PERCEVAL

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Service-Public.fr
Le site officiel de l'administration française

S'identifier avec FranceConnect

Logo de la plateforme PERCEVAL (visible dans les 600 000 flyers papier distribués)

UNE DÉMATÉRIALISATION POUR UNE PROCÉDURE RICHE ET INTERACTIVE

La mise en œuvre d'une procédure pénale dématérialisée entre dans l'évolution des métiers du droit. Elle passe par l'abandon progressif de toutes les relations « papier » entre les acteurs de la chaîne judiciaire. Cette nouvelle pratique nécessitera une signature électronique opposable, un circuit de validation hiérarchique et un coffre-fort numérique qui assurera une sauvegarde des actes et des pièces numériques du dossier, notamment celles qui ressortent du régime de la preuve.

Une expérimentation, dès 2019, sur deux sites choisis pour leur implication dans des processus de modernisation et de numérisation préparera à un passage à une procédure pénale numérique. Ce nouveau cycle de la donnée dématérialisée autorisera en temps réel le contrôle effectif du respect des libertés publiques. Il ouvrira une nouvelle relation entre l'enquêteur et le magistrat.

La procédure pénale numérique

Par Ronan Le Floc'h

Voulu par les plus hautes autorités de l'État, le projet de procédure pénale numérique (PPN) porte l'ambition d'arriver, à l'horizon 2019, à une procédure pénale entièrement dématérialisée. Fondée sur une démarche pragmatique capitalisant sur le droit et les outils, existants ou en projet, la procédure pénale numérique repose sur la génération d'actes électroniques de procédure originaux et d'échanges inter-applicatifs entre les différents systèmes informatiques des ministères de l'Intérieur et de la Justice.

RONAN LE FLOC'H

Colonel de Gendarmerie
Chargé de mission Programme « procédure pénale numérique »
Direction des opérations et de l'emploi

Dans son discours, prononcé lors de l'audience solennelle de rentrée de la cour de Cassation du 22 janvier dernier, le président de la République a annoncé sa volonté d'arriver en 2022 à une procédure pénale entièrement dématérialisée, du dépôt de plainte à l'exécution des peines, en passant par tous les actes d'enquête et les audiences.

Cette ambition s'inscrit dans un contexte de numérisation de la société et de banalisation de l'outil informatique. Ni le service public, ni les métiers du droit ne restent en retrait de cette évolution comme en attestent la très forte dématérialisation de l'administration fiscale dans ses relations aux contribuables ou la totale dématérialisation des actes notariés, l'une comme l'autre désormais totalement intégrées dans l'environnement du citoyen-usager.

Les bénéfices d'une telle évolution sont aisés à saisir et peuvent être perçus par toutes les parties prenantes au processus. Ils concernent la facilité d'accès à la donnée, à un service dématérialisé disponible

en permanence et comprennent impératifs liés au stockage des documents.

Le champ du procès pénal ne pouvait rester à l'écart d'une telle évolution pour des raisons de qualité du service public mais aussi du fait de la prégnance de plus en plus forte de la preuve numérique dans l'enquête judiciaire. Le processus de dématérialisation est au demeurant déjà amorcé dans ce domaine avec la plate-forme nationale des interceptions judiciaires qui, outre sa mission d'accès aux échanges téléphoniques, assure le stockage des données sous forme numérique dans un coffre-fort électronique et permet l'accès en ligne aux ayants droit.

Une évolution…

Il s'agit donc pour les acteurs du procès pénal, agents et officiers de police judiciaire, magistrats et greffiers, de passer à une nouvelle étape qui est l'abandon du papier. Pour révolutionnaire que puisse apparaître ce changement de paradigme, il s'apparente cependant plus à une forte mais simple évolution des pratiques, la place du numérique étant déjà importante dans la pratique pénale.

En effet, policiers et gendarmes, lorsqu'ils produisent aujourd'hui des procédures, notamment pénales, le font à partir de logiciels spécialement conçus, et donc produisent un acte numérique ab initio. Cet acte est matérialisé, par une impression, pour être signé et acquérir ainsi une valeur probante. Il est ensuite bien souvent numérisé et exploité sous cette forme par les acteurs du monde judiciaire. Il s'agit d'une copie de travail, après un stockage sur des serveurs protégés via des logiciels dédiés.

Le premier acte de l'évolution est donc la « signature électronique », qui exonère le rédacteur du procès-verbal de l'impression. En apparence anodine, cette évolution résume à elle seule le passage à la procédure pénale numérique : l'original devient un document électronique qui désormais fera foi.

Cette signature étant apposée par le rédacteur, il reste à faire admettre sa validité par un tiers, en particulier une personne entendue qu'elle soit victime, simple témoin ou mise en cause. Pour celle-ci, l'évolution des pratiques sociales a largement préparé le terrain. Il s'agira en effet d'apposer sur une tablette sa signature, à l'instar de ce qui se pratique déjà pour les courriers recommandés ou encore chez le notaire.

Le document ainsi généré et verrouillé par la signature électronique rentre ensuite dans le circuit classique de validation hiérarchique et de transmission. Cette transmission dématérialisée, via des plateformes d'échange, constitue le deuxième changement de paradigme de la procédure numérique.

Après la signature et la transmission, le troisième acte fondateur de la procédure pénale électronique est l'archivage. L'ensemble des documents électroniques

constituant la procédure a vocation à rejoindre des archives numériques, à l'instar de ce qui se pratique pour les actes notariés au « minutier central électronique » du notariat.

Si les principes sont simples et les technologies convoquées *a priori* matures, l'enjeu de transformation est de taille si on considère le nombre d'acteurs impliqués tout d'abord, soit 200 000 policiers et gendarmes et 32 000 magistrats et greffiers, le volume de pièces produites annuellement ensuite, soit 6,5 millions de procédures ouvertes dans les logiciels de rédaction de la gendarmerie et de la police, 4,5 millions d'affaires traitées par les parquets, et 1,2 million de décisions rendues par les juridictions pénales.

...ou une révolution ?

Ce saut dans le moins connu sinon dans l'inconnu doit donc être préparé et mené avec une stratégie claire, minimisant les risques potentiels. Ceux-ci tiennent en effet aux aléas techniques, mais surtout à l'acceptation du changement par les parties prenantes, qu'il s'agisse des acteurs à proprement parler du procès pénal ou des justiciables.

Le choix a donc été fait de partir du connu pour aller vers l'inconnu, en menant la réforme à droit constant, nonobstant quelques modifications réglementaires, en s'appuyant sur les outils existants ou en développement, la plupart éprouvés, et en les faisant communiquer entre eux. L'enjeu technique est donc essentiellement un enjeu d'intégration ou « d'urbanisation » des outils.

Il s'agit aussi de faire cette réforme avec les acteurs, en les impliquant dans la conduite du changement et la définition des outils et des processus métier. Un important effort de formation est naturellement au cœur de cette étape.

Enfin, la mise en œuvre sera précédée d'une expérimentation, sur deux sites pilotes correspondant à deux départements, à partir de 2019, puis suivie, en fonction des résultats, d'un déploiement progressif. Les sites ont été choisis notamment en raison de la forte appétence locale pour la modernisation et leur forte implication dans les processus de numérisation, permettant notamment de procéder à des audiences numériques, dans lesquelles le papier a disparu au profit des documents numérisés.

Enfin, le passage à la PPN se fera de façon progressive, avec dans un premier temps un « calque » de la procédure papier actuellement en vigueur. Chaque procès-verbal (PV) restera rédigé avec les mêmes interfaces et produira un document PDF en format A4. Au lieu d'être imprimé, il sera simplement signé électroniquement.

Pour autant, les perspectives ouvertes par la dématérialisation permettent d'imaginer à terme une procédure plus riche et inte-

© Internet law concept Par phonlamaiphoto

La procédure pénale numérique implique, outre l'adhésion des acteurs, l'intégration aux documents digitalisés des liens des documents connexes notamment ceux qui contiennent les éléments de preuve.

ractive, avec un document de type « wiki » contenant des hyperliens vers les éléments de la preuve numérique. Le PV, rédigé sous cette forme, pourrait renvoyer directement vers un document tels qu'un extrait de vidéo, des photographies numériques ou des factures téléphoniques détaillées, permettant au lecteur de la procédure de disposer de l'ensemble des éléments de preuve à partir d'un document numérique unique. Cette procédure ne peut cependant être mise en œuvre qu'à l'issue du processus d'appropriation de la dématérialisation par l'ensemble des acteurs. Elle suppose également la mise en œuvre d'outils nouveaux qui doivent encore être développés, en particulier une plate-forme multimédia sécurisée, à l'image du « coffre-fort » électronique de la PNIJ[1].

(1) Plate-forme Nationale des Interceptions Judiciaires.

Il est à noter qu'en toute hypothèse, les rôles de chacun des acteurs n'ont pas vocation à changer, mais au contraire à s'affirmer avec la fluidité des échanges ainsi assurée. Le rôle de la hiérarchie en particulier est un point central du fonctionnement de la PPN. Responsable de la qualité de la procédure produite, le commandant d'unité ou le chef de service saisi par la justice des investigations reste le responsable de la procédure, qui n'apparaît à la lecture du magistrat que dès lors qu'il l'a validée.

Une attente et des perspectives

Les perspectives ouvertes par la dématérialisation de la procédure pénale vont même au-delà de la simple automatisation ou suppression de tâches ancillaires telles que l'impression et la mise en forme des dossiers papier, le placement sous scellés de DVD, la saisie de données obtenues au format papier… mais offrent la possibilité de sortir d'un cercle vicieux d'alourdissement constant des diligences formelles de la procédure pénale, entraînant des mesures correctives en termes de simplification ou d'adaptation des moyens.

En effet, le cycle de la donnée dématérialisée autorise la possibilité d'un contrôle effectif et en temps réel du respect des libertés publiques par ceux qui en ont la charge, au premier rang desquels les magistrats. Le meilleur exemple en est sans doute la conduite de la garde à vue. Par les biais des systèmes S@MPL[2] de la gendarmerie, en cours de développement, et iGAV de la police nationale, actuellement expérimenté sur le ressort du TGI d'Évry, l'OPJ se trouve déchargé de l'obsession des diligences relatives au respect des droits, le logiciel rappelant et synthétisant celles-ci, quand le magistrat ainsi que le chef hiérarchique peuvent en temps réel s'assurer de l'effectivité du respect des droits.

(2) Suivi automatisé des mesures privatives de liberté

La PPN va donc introduire une nouvelle relation entre l'enquêteur et le magistrat par la fluidité des échanges, une confiance liée au respect des attributions respectives des parties ainsi qu'à la transparence inhérente à la disponibilité constante des informations. Ce bénéfice, qui n'est pas anecdotique, se double des perspectives impressionnantes ouvertes potentiellement par la fluidité des informations recueillies dans les enquêtes, qu'il s'agisse de la captation de données en mobilité, via les dispositifs « NEO », ou de « l'intelligence judiciaire » permettant de croiser les données concernant des faits ou des individus, et ainsi d'obtenir la réponse pénale la plus juste conformément au principe d'individualisation de la peine.

Si les perspectives sont enthousiasmantes, le défi à relever reste de taille. Il pourra se nourrir de l'attente déjà manifestée par nombre d'acteurs, impatients de changer de siècle dans un domaine central de leur activité.

L'AUTEUR

Ancien élève de l'École Spéciale Militaire de Saint Cyr, le colonel LE FLOC'H est breveté de l'enseignement militaire supérieur et auditeur de la 8e promotion du centre de hautes études du ministère de l'intérieur. Il a exercé le commandement d'un escadron de gendarmerie mobile et d'une compagnie de gendarmerie départementale, ainsi que de la section de recherches de Pau et du groupement de gendarmerie départemental de l'Oise.
Chef de bureau à la sous-direction de la police judiciaire de la DGGN de 2012 à 2016, il est actuellement chargé de mission à la direction des opérations et de l'emploi et directeur du programme « procédure pénale numérique » pour la gendarmerie.

NOTES

NOTES

DIRECTEUR DE LA PUBLICATION

Général de brigade **Laurent BITOUZET**

RÉDACTION

Directeur de la rédaction :
Général d'armée (2S) **Marc WATIN-AUGOUARD,**
directeur du centre de recherche de l'EOGN

RÉDACTEUR EN CHEF

Colonel (ER) **Philippe DURAND**

MAQUETTISTE PAO

Maréchal des logis-chef **Céline MIGNÉ**
SDG

COMITÉ DE RÉDACTION

• Général de corps d'armée **Christian RODRIGUEZ,**
major général de la Gendarmerie nationale
• Général de corps d'armée **Thibault MORTEROL,**
Commandant des écoles de la Gendarmerie nationale
• Général de brigade **Laurent BITOUZET,**
Conseiller communication du directeur général
de la Gendarmerie nationale - chef du Sirpa-gendarmerie
• Lieutenant-colonel **Jean-Marc JAFFRÉ,**
Directeur-adjoint au centre de recherche de l'EOGN

COMITÉ DE LECTURE

• Général d'armée **David GALTIER,**
Inspecteur général des armées – gendarmerie
• Général de corps d'armée **Christian RODRIGUEZ**
Major général de la Gendarmerie nationale
• Général de corps d'armée **Thibault MORTEROL,**
Commandant des écoles de la Gendarmerie nationale
• Général de corps d'armée **François GIERÉ,**
Directeur des opérations et de l'emploi
• Général de brigade **Laurent BITOUZET,**
Conseiller communication du directeur général
de la Gendarmerie nationale - chef du Sirpa-gendarmerie
• Colonel **Laurent VIDAL,**
délégué au patrimoine – DGGN
• Lieutenant-colonel **Édouard EBEL,**
département gendarmerie au sein
du service historique de la Défense

DÉPOT LÉGAL

Raison sociale de l'éditeur :
CREOGN, avenue du 13e Dragons,
77010 Melun cedex
Général (2S) Watin-Augouard
Imprimerie : SDG - 11 rue Paul Claudel
87000 Limoges
Décembre 2018
ISSN 1243-5619

Session nationale
SOUVERAINETE NUMERIQUE & CYBERSECURITE
SEPTEMBRE À JUIN

Avec les *Livres blancs sur la défense et la sécurité nationale* de 2008 et de 2013, le cyberespace est entré dans le champ de la sécurité nationale. Conscients des enjeux pour la défense, la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN proposent, avec l'ensemble de leurs partenaires, une formation inédite de haut niveau qui doit permettre à une quarantaine d'auditeurs, hauts cadres des secteurs public et privé

- ✓ d'acquérir une culture des enjeux de cybersécurité et de souveraineté induits par les transformations numériques
- ✓ de développer une vision stratégique "cyber", au profit de l'entreprise, de l'administration et des armées

CONTACTS

IHEDN
Secrétariat
01 44 42 46 27
sylvie.lievin@ihedn.fr
www.ihedn.fr

INHESJ
Secrétariat
01 76 64 89 93
dominique.henrion@inhesj.fr
www.inhesj.fr