INTERNATIONAL>
Cybersécurité et régulation internationale

DÉFENSE>
Résilience des SIC militaires

DROIT >
Du cybercrime au cyberjuge

REVUE
de la gendarmerie nationale

REVUE TRIMESTRIELLE / DÉCEMBRE 2017 / N° 260 / PRIX 6 EUROS

retour sur images NUMÉRO 259

© Duffaut - gendarmerie

LA PROXIMITÉ TERRITORIALE

La mobilité des populations et l'hyperconnexion créent de nouvelles habitudes de vie et des rapports humains différenciés au sein du territoire. Cela impose une nouvelle définition de la proximité territoriale qui reflète les nouvelles mœurs d'une population urbanisée, connectée et diversifiée. La gendarmerie revisite en conséquence sa stratégie, sans rupture avec une logique d'égalité des territoires et en créant un espace numérique de proximité..

RETROUVEZ EN PAGE 162 L'IMPORTANCE DES ALGORITHMES DANS LE PROCESSUS DÉCISIONNEL

© Blueday2014 - Adobe Stock

Hyperconnexion et résilience

Les groupes humains ont lentement colonisé leur environnement qu'il soit terrestre, marin, aérien ou extra-atmosphérique. Chaque conquête a été accomplie par l'alternances d'avancées scientifiques et philosophiques avec des périodes de chaos, et selon des cycles d'hégémonie de grandes nations. Il en est sorti un ordre mondial évolutif, certes imparfait, mais globalement régulé par de grandes organisations internationales.
Le cyberespace est un domaine pionnier. Qualifié d'immatériel et de virtuel, il relève cependant d'infrastructures et de programmes réels. Les technologies qui s'y sont développées ne sont finalement, sous des modalités différentes et avec des performances accrues, que la translation de savoirs et de pratiques de « l'ancien monde ». Elles sont omniprésentes : information, culture, éducation, commerce, industrie, services, santé, sécurité, défense. Elles sont donc inextricablement liées à la destinée du genre humain.
Le cyberespace est donc naturellement devenu un enjeu majeur et un vecteur de stratégies commerciales, relationnelles et de domination militaire ou politique. L'absence globale et fondamentale d'une volonté de régulation des techniques employées et des contenus modifie les rapports entre les États et entre ces derniers et leurs citoyens. Elle engage également les relations entre les personnes qui voient poindre un nouveau couple homme-machine porteur d'une compétition au regard du développement de l'intelligence artificielle.
Un monde hyperconnecté et peu résilient enfantera un monstre totalitaire ou mafieux s'il n'est pas régulé. Cette régulation ne sera pas le fait d'États-Nations, exsangues et crispés sur des questions de souverainetés, mais par l'instauration d'un partenariat international où les acteurs privés, les groupements d'états ayant un seuil critique de crédibilité financière, politique et militaire, et les représentations des usagers pourront instaurer un système préservant la confiance numérique, la protection des données personnelles et un encadrement strict de l'intelligence artificielle et des développements liberticides. Alors, seulement un droit international homogène pourra s'appliquer et contrer les avancées de la cybercriminalité.

COL(ER) Philippe Durand,
rédacteur en chef

SOMMAIRE

NUMÉRO 260

INTERNATIONAL

DÉFENSE

DOSSIER

TECHNIQUE

ADMINISTRATIONS ET ASCENSEUR SOCIAL

DOSSIER

Hyperconnexion
et résilience

Cybrain - adobe stock

APRÈS L'ÉCHEC DE LA CGE IL EST NÉCESSAIRE DE TROUVER UN ESPACE DE NÉGOCIATION

Sans être abandonné, le concept de régulation internationale de la cybersécurité doit être revisité selon des formules plus souples et partenariales. Toutefois, une dissémination d'initiatives en Asie, dans le pacifique, en Europe et dans la sphère anglo-saxonne ne permettra pas la cohésion et la pertinence des mesures notamment celles qui recèlent une dimension coercitive qui ne peut être parcellaire.

L'OCDE offre une espace juridique qui permettrait par des fora de discussion ou de négociation d'offrir une alternative crédible aux organismes internationaux complexes, au sein desquels il est difficile d'obtenir un consensus, en ouvrant les discussions et des négociations dans un cadre souple et ouvert à de nouveaux partenaires qui vont des multinationales du numérique aux petites et moyennes entreprises. Cette globalité d'approche, étendue au monde économique, permettra une praxis pragmatique et neutre qui évite l'écueil de l'expression prématurée des souverainetés régaliennes.

Cybersécurité et régulation internationale : quel forum après l'échec du GGE de l'ONU ?

Par KARINE BANNELIER et THÉODORE CHRISTAKIS

Alors que l'échec des négociations sur la cyber-sécurité au sein du GGE[1] de l'ONU a créé un grand vide en matière de régulation internationale, les récentes vagues de cyberattaques ont montré qu'il est plus que jamais urgent d'agir. La réflexion sur les normes devrait inclure les acteurs du secteur privé qui, souvent, sont les premières victimes des cyberattaques. Cet article propose de créer au sein de l'OCDE un organe souple et inclusif qui jouerait un rôle de hub pour les différentes initiatives tout en favorisant une coopération étroite entre les Etats, le secteur privé et la société civile pour la promotion de normes de conduite responsable dans le cyberespace.

KARINE BANNELIER

Maître de Conférences-HDR en droit international, Directrice du Master 2 Sécurité Internationale et Défense - Université Grenoble Alpes

THÉODORE CHRISTAKIS

Professeur de droit international - université Grenoble Alpes

(1) *Group of Government experts.* La France a participé aux cinq derniers groupes d'experts gouvernementaux (GGE) de l'ONU sur la cybersécurité. Les travaux ont ancré le cyberespace dans le système international issu de la Charte des Nations Unies et orienté les Etats dans une dynamique de prévention, de coopération et de non-prolifération dans le cyberespace.

Les États se sont saisis ces dernières années du problème de la sécurité du numérique en multipliant les initiatives au sein de diverses organisations intergouvernementales, qu'il s'agisse d'organisations à vocation universelle (telles que l'ONU ou l'Union Internationale des Transmissions) ou d'organisations à vocation régionale ou restreinte comme l'Union européenne (avec, notamment, la récente série de me-

sures annoncées en septembre), le Conseil de l'Europe, l'OSCE - Organisation pour la sécurité et la coopération en Europe , l'OCDE - Organisation de coopération et de développement économique , l'Union africaine, l'Organisation de coopération de Shanghai, l'OTAN, le G7 ou encore le G20. Ces initiatives se développent aussi dans des cadres *ad hoc* dédiés spécifiquement à la cyber-sécurité où l'on assiste à un nombre impressionnant de conférences initiées par des États telles la *Global Conference on Cyberspace* (GCCS) qui a elle-même lancé le Global Forum on Cyber Expertise (GFCE) et ceci sans compter les initiatives académiques comme le processus qui a abouti à l'adoption des Manuels de Tallinn 1 et 2 (largement dominés par l'approche anglo-saxonne du droit international) ou la création de *Think Tanks* comme la récente *Global Commission on the Stability of Cyberspace* lancée par le gouvernement des Pays-Bas et Singapore et présidée par Marina Kaljurand (ancienne ministre des Affaires étrangères de l'Estonie)

L'échec du GGE

Parmi ces nombreux fora de discussion ou de négociation, le plus important a été sans doute le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (GGE) de l'ONU. Ce groupe, composé des représentants de 25 pays, a affirmé l'applicabilité du droit international au cyberespace. Son dernier rapport, publié en 2015, portait de manière précise sur l'application de certains principes et normes du droit international et proposait une série de règles de comportement responsable des États. A la suite de ce rapport, conformément au mandat qui lui avait été donné, le GGE s'est engagé dans un travail visant à préciser et à approfondir ces règles, normes et principes. Un nouveau rapport était ainsi attendu avec impatience par la communauté internationale. Malheureusement ce texte n'a jamais été publié. Alors que des progrès significatifs avaient été faits sur des questions importantes, des désaccords sont apparus sur certains points (notamment concernant la question de la légitime défense et l'applicabilité du droit humanitaire)[2] et les négociations ont finalement échoué cet été.

(2) Pour une illustration, voir les positions respectives du représentant de Cuba (https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf) et du représentant des Etats-Unis (https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm)

Cet échec du GGE laisse la régulation internationale du cyberespace sans forum centralisé et au moment même où l'urgence d'agir se fait plus pressante que jamais – comme en témoignent notamment les cyberattaques *Wannacry* et *NotPetya* ou les controverses liées au *hacking* du parti démocrate américain. L'échec du dernier GGE devrait accentuer la compétition pour combler le vide. On assiste en effet ces derniers mois à une certaine effervescence de part et d'autre et

à des appels divers pour prendre le relais du GGE. C'est ainsi, par exemple, que certains ont appelé l'ASEAN à agir vite pour adopter ses propres normes en réponse tant à l'échec du GGE qu'aux mesures annoncées par l'UE et ceci, ont-ils fait valoir, « *pour ne pas attendre que d'autres organisations fixent les règles de cybersécurité que le monde doit suivre* »[3].

(3) E. Tan, "The Challenge of Getting Responsible Behaviour in Cyberspace", RSIS No. 184 – 6 October 2017.

(4) A. Srivas, "After UN Talks On Cyber Norms Collapse, India Starts Chalking Out Own Strategy", The Wire, 12 septembre 2017.

Plusieurs pays ont aussi pris des initiatives dans ce domaine. Au début du mois d'octobre, l'Australie a ainsi publié l'International *Cyber Engagement Strategy* qui comprend de nombreuses propositions visant à promouvoir la cyber-sécurité dans la région Asie/Pacifique ; les États-Unis ont commandé un rapport sur le thème *Engagement Strategy for International Cooperation in Cybersecurity* ; l'Inde a créé un Comité destiné à reprendre le flambeau du GGE[3] et en Suisse, des voix appellent à donner rapidement suite à la proposition de Microsoft pour une « Convention de Genève Digitale » et proposent la ville de Genève comme « *un cadre neutre pour un dialogue systématique entre gouvernements et sociétés informatiques* » [4].

Un risque de fragmentation du régime juridique

Le foisonnement d'initiatives au sein de fora très divers ne témoigne pourtant pas forcément d'une bonne gouvernance de la sécurité numérique. La multiplication d'institutions internationales pourrait parfois envoyer un message brouillé quant aux droits, obligations et responsabilités des différents acteurs. Il est aussi à craindre que ce foisonnement puisse conduire à une fragmentation du droit international et à un émiettement des principes et normes applicables dans le cyberespace.

Comme remède à cette dispersion, certains ont proposé la création d'une nouvelle organisation internationale intergouvernementale spécialisée dans la sécurité du numérique qui pourrait ainsi agir de façon centralisée. Toutefois, l'ère n'est plus vraiment à l'adoption de structures lourdes passant par des négociations chronophages de nouveaux traités constitutifs d'organisations internationales qui pourraient d'ailleurs n'être jamais ratifiés par certains États. Elle n'est d'ailleurs pas non plus à la création d'organisations internationales à vocation universelle dotées de pouvoirs normatifs.

On voit donc difficilement comment les États pourraient s'engager dans la création d'une organisation internationale intergouvernementale spécialisée dans ce domaine. On voit mal aussi comment ils pourraient

Les négociations internationales ont besoin de structures souples pouvant intégrer les émanations gouvernementales et les acteurs privés.

accepter de lui transférer des compétences importantes en matière de cyber-sécurité qui sont largement perçues comme relevant du domaine de la « sécurité nationale », de la sécurité de leurs populations et de leurs pouvoirs régaliens.

Alors que le besoin de coordination, de cohérence et de rationalisation des initiatives se fait cruellement sentir (tout comme celui de renforcer les mesures de confiance et d'assistance en direction des pays qui accusent un retard en matière de sécurité du numérique), une solution pourrait alors être d'établir une plateforme ouverte, souple et inclusive.

Quelle rationalisation ? La solution OCDE

Comment donc aboutir à cette rationalisation sans passer par la création d'une nouvelle organisation internationale intergouvernementale ? La solution pourrait se trouver au sein de l'OCDE.

Pour comprendre l'intérêt que présente l'OCDE, il faut tout d'abord rappeler que ces dernières années ont été marquées

par des évolutions institutionnelles importantes dans le cadre de la gouvernance internationale. A la création d'organisations internationales s'est souvent substituée celle d'institutions internationales plus informelles sous des dénominations variables comme celles de « forum », « réseau », « groupes » (le G7 ou le G20 étant les plus connus), « agences », « comités » qui, peut-être ne correspondent pas vraiment à la définition classique de l'organisation internationale intergouvernementale mais qui remplissent leurs fonctions avec une certaine efficacité.

Ces institutions présentent plusieurs avantages dont le principal, sans doute, est la souplesse.

Souplesse en termes de représentation et de composition tout d'abord. Il semble désormais nécessaire de faire une véritable place aux acteurs privés à travers une composition multipartite ou, au moins, la création d'un mécanisme formel d'intégration du secteur privé tel qu'un « *Corporate Partnership Board* ». On se rappelle à cet égard la proposition de Microsoft de créer un organe informel composé d'un G20 et d'un ICT20 – à savoir les 20 plus grandes compagnies des Technologies de l'information et des communications (TIC). Cette proposition présente néanmoins des difficultés y compris le fait que des institutions comme le G7 ou le G20 souffrent de ne pas avoir de secrétariat permanent et d'expertise propre, sans parler des problèmes de légitimité démocratique. Toutefois, l'idée d'associer les acteurs privés et les États au sein d'une institution internationale est un élément qui doit être pris en considération. L'association du secteur privé ne devrait d'ailleurs pas se limiter aux grands des TIC, mais inclure aussi d'autres acteurs importants comme les compagnies d'assurances, voire des représentants de PME.

Souplesse aussi à propos des moyens d'agir de ces institutions qui, souvent, sont dépourvues de pouvoirs normatifs propres - ce qui ne les empêche pas d'être des enceintes de discussion et de négociation ni de prendre des initiatives comme l'adoption de codes de conduite.

L'expérience de l'OCDE paraît donc particulièrement intéressante. En effet, l'OCDE, qui est une organisation internationale intergouvernementale de type classique, accueille en son sein des institutions souples et autonomes pour gérer différents domaines et questions qui relèvent de la coopération internationale. On peut

Étude Cyberattaques

K. Bannelier et Théodore Christakis ont récemment rédigé l'étude Cyberattaques. Prévention-réactions : rôle des Etats et des acteurs privés » (Les Cahiers de la Revue défense Nationale) préparatoire à la conférence internationale « Construire la paix et la sécurité internationale de la société numérique. Acteurs publics, acteurs privés : rôles et responsabilités » organisée par le gouvernement français à l'UNESCO les 6-7 avril 2017.

par exemple citer l'International Transport Forum, dans le domaine des transports ; la *Financial Action Task Force* (GAFI) dans le domaine de la finance, ou encore le *Global Forum on Transparency and Exchange of Information for Tax Purposes*. Ce type d'institutions fonctionne de façon efficace et a une capacité de régulation importante passant souvent davantage par la *soft law* que par la *hard law*. Elles sont administrativement intégrées à l'OCDE qui leur prête, entre autres, sa personnalité juridique, tout en étant entièrement autonomes sur le fond. Les 35 pays membres de l'OCDE constituent le moteur de ces institutions mais d'autres pays y participent aussi sur un pied d'égalité, y compris la Chine, la Russie, l'Inde, le Brésil, l'Afrique du Sud. Certaines d'entre elles comportent aussi des *Corporate Partnership Boards* qui permettent ainsi d'associer aux travaux les grands acteurs du secteur privé.

Aussi, pourquoi ne pourrait-on pas envisager la création, au sein de l'OCDE, d'un *International Cybersecurity Forum* qui jouerait un rôle de hub et de coordination pour les différentes initiatives tout en permettant aux Etats, au secteur privé et à la société civile de travailler étroitement ensemble en vue du développement de normes de conduite responsable dans le cyberespace ?

L'OCDE a par ailleurs une véritable légitimité dans le domaine de la cyber-sécurité où elle a déjà joué un rôle précurseur.

L'augmentation spectaculaire des cyberattaques, leur coût impressionnant qui pourrait atteindre, selon certaines estimations, les 6 trillions de dollars d'ici 2021, le fait que les cyberattaques soient devenues, selon les rapports les plus récents, le tout premier facteur de « risque externe » pour les entreprises, indiquent l'OCDE comme un forum presque naturel pour promouvoir des normes de cyber-hygiène, de cyber-résilience ou de cyber-diligence.

Sur le plan diplomatique, les négociations pourraient s'avérer moins difficiles qu'au sein de l'ONU. Compte tenu de sa mission et de sa nature, l'OCDE, ne devrait pas se focaliser sur des questions régaliennes telles que la légitime défense ou le droit des conflits armés qui cristallisent les oppositions entre les États. Le forum créé au sein de l'OCDE pourrait par contre s'intéresser aux questions de cyber-sécurité sous un angle plus économique. Sa mission pourrait ainsi être de promouvoir des normes de comportement responsable pour les Etats et le secteur privé en développant des codes de conduite, des mesures de confiance, des protocoles de notification et de coopération mais aussi en favorisant l'émergence d'instruments juridiques voire de mécanismes de contrôle.

L'AUTEURE

Karine Bannelier est Maître de Conférences-HDR en droit international à l'Université Grenoble Alpes et directrice du Master 2 Sécurité Internationale et Défense. Responsable du Groupe « Cyber/Nano/Bio » au sein du Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes (CESICE). Elle est cofondatrice d'AMNECYS (*Alpine Multidisciplinary Network on Cyber-security Studies*) qui est un réseau multidisciplinaire d'experts sur la cyber-sécurité. Ses recherches portent sur le droit international, le droit de la sécurité internationale, la cyber-sécurité, la gouvernance et la protection des données. Elle a été invitée à présenter des communications scientifiques dans vingt-cinq pays, et a publié ou coédité 8 ouvrages et une cinquantaine d'articles

L'AUTEUR

Théodore Christakis est professeur de droit international à l'Université Grenoble Alpes et membre Senior de l'Institut Universitaire de France (IUF) où il mène un projet de recherche sur la sécurité nationale et le droit international, dont un important volet est dédié au droit de la cyber-sécurité. Il est directeur du Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes (CESICE) et directeur adjoint du Grenoble Alpes Data Institute. Il est fondateur et co-responsable de l'*Interest Group on Peace and Security de la European Society for International Law* et membre de l'*International Committee on Use of Force de l'International Law Association*. Il a été invité à présenter ses travaux dans des conférences, colloques et séminaires organisés dans 28 pays, il a publié ou co-édité 9 ouvrages et il est l'auteur ou co-auteur de plus de 60 articles scientifiques et chapitres d'ouvrages qui portent sur le droit international public, le droit de la sécurité internationale, la protection internationale et européenne des droits de l'homme, le droit de la cyber-sécurité et la protection des données.


Adobe stock Bluedesign

UNE RUPTURE QUI NÉCESSITE DE REVISITER LE RÉGIME DE LA PROTECTION DES DONNÉES INDIVIDUELLES

La Grande-Bretagne, du fait de son expertise et de sa législation, a un poids non négligeable dans le domaine numérique. On peut estimer qu'elle est la tenante d'une certaine liberté et d'un encadrement circonstancié selon sa perception des échanges économiques internationaux et de ses intérêts financiers. Le Brexit pose la question de sa position dans un marché unique renforcé qui fait de la rigueur européenne une exception mondiale quant au traitement des flux transfrontaliers des données.

Le régime juridique de la RGPD, la directive NIS, le projet *eprivacy* disposent de la vie des internautes au travers des principes de protection des données à caractère privé. Cela concerne la coopération anglaise jusqu'au Brexit et surtout l'évolution des positions du Royaume-Uni selon son appariement distancié au bloc européen. Le *privacy shield*, la question de la redéfinition des standards ISO illustrent ces incertitudes quant au règlement des prochains grands rendez-vous internationaux en termes de régulation.

Le Brexit
et la protection des données

Par LUDMILLA VIALLE

Longtemps caractérisé par sa liberté numérique, le Royaume-Uni ne disposait pas d'encadrement équivalents à ceux émergeant en Europe. Si cette situation semblait *a priori* propice au développement des affaires, elle ne permettait pas pour autant de conférer aux entreprises nationales un gage de confiance, notamment lorsqu'elles se voyaient transférer des informations étrangères. C'est la raison pour laquelle l'État se dota dès 1984 d'une législation non-Orwellienne, relative à la protection des données.

LUDMILLA VIALLE

Master 2 Droit des collectivités territoriales. Institut d'études juridiques Paris Nanterre et Assas Paris II.

Le gain d'attractivité en résultant ne permit toutefois pas de résoudre les disparités territoriales. Ainsi, le gouvernement lança un programme d'inclusion numérique au cours de l'année 1990. De même, au niveau européen, la Commission envisagea la création d'une base juridique commune, capable d'instaurer un marché unique 2.0 plus uniforme et compétitif. Les négociations en découlant firent état de nombreuses difficultés, au nombre desquelles figurait l'opposition britannique à toute contrainte stricte.

Forte de cette harmonisation, le Royaume-Uni pèse aujourd'hui lourdement dans l'écosystème numérique. En se dotant dès 2015 du plan d'action audacieux TechNation, il a su constituer un espace digital de près d'1,5 million d'experts, dont la performance lui vaut la 7e position au classement européen DESI (*Digital Economie and Society Index*). Cette attractivité pourrait être encore améliorée par le Règlement Général de Protection des Données (ci-après RGPD), qui se substitue à l'ancienne directive 95/46/CE.

Toutefois, l'annonce du Brexit ouvre une période d'incertitude. Les négociations

ouvertes depuis le 19 juin attestent de cet état, en opposant, sur une temporalité d'au moins deux ans, deux personnalités clivantes : David Davis, eurosceptique en charge de la représentation des intérêts britanniques, et Michel Barnier, fédéraliste aguerri agissant pour le compte de la Commission européenne.
Si cette quête souverainiste ne semble pas avoir d'impact sur le niveau actuel de protection des données, une interrogation se pose sur le long terme.

Un court terme certain : une harmonisation temporaire quasi complète

Jusqu'à la fin du processus de négociation, le Royaume-Uni demeure membre de l'Union européenne. Il est à ce titre assujetti à la mutation du marché unique numérique, tant d'un point de vue théorique que pratique.

L'appartenance à un marché unique numérique renforcé

• Un marché unique en mutation :
À partir des années 80, la société internationale se saisit des problématiques de flux transfrontaliers de données, au moyen de divers instruments normatifs[1]. L'Union européenne fait figure d'exception en élaborant une harmonisation plus approfondie, capable d'instaurer un marché unique numérique performant. C'est ainsi que le Royaume-Uni transpose, notamment, les directives 95/46/CE et 2002/58/CE (vie privée et communication électronique). Pour assurer une bonne mise en œuvre de ces règles complexes et détaillées, la directive 95/46 prévoit, en plus de l'action normative classique de la Cour de Justice[2], la création du "G29". Ce groupe de travail est chargé d'analyser la régulation opérée dans différents États, à des fins de conseils et d'éventuelles propositions de projets de modification à la Commission[3]. En dépit de son activité intense, une étude comparative de la Commission de 2010 fait état de pratiques régulatoires nationales divergentes[4]. Sur le plan juridique, certaines notions ne font pas consensus. La législation autrichienne prévoit, par exemple, qu'il n'est pas possible d'identifier une personne à partir de moyens légaux, tandis que la loi britannique retient le critère de probabilité. Sur le plan pratique, les autorités de régulation anglaise et irlandaise se livrent à une action disciplinaire plus clémente que leurs homologues européens, entraînant ainsi

(1) Métallinos N., *L'évolution du droit européen en matière de protection des données à caractère personnel et sa pénétration dans les droits nationaux : principes fondateurs et instruments de régulation,* L'Observateur de Bruxelles, mars 2013, n°93, p.8-17.

(2) Laudati L., Summaries of EU court decisions relating to data protection 2000-2015, OLAF, 21 janvier 2016.

(3) Kohnstamm J., 14th and 16th reports on the article 29 working party on data protection, publications office of the European Union, 2013 et 2015.

(4) Commission Européenne Direction Générale Justice Liberté et Sécurité, Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques, janvier 2010.

(5) Cherki M., Protection des données : la Cnil plus stricte que Bruxelles, le Figaro, 12 octobre 2012.

une concurrence conflictuelle[5].
Ces éléments, corrélés aux rapports DESI, font état d'une Europe à plusieurs vitesses, pour laquelle il devient impérieux d'approfondir l'harmonisation entreprise, notamment pour appréhender les nouveaux usages numériques.

• Un marché approfondi :

En poursuivant une nouvelle logique de conformité, le RGPD, dont l'application sera directe dès le 25 mai 2018, constitue la norme de référence en matière de protection des données personnelles[6]. Son rayonnement, d'abord continental, s'étend aux responsables de traitement de données (directs et indirects), établis sur l'espace économique européen, ainsi qu'aux services intéressant leur résidents. C'est la raison pour laquelle, tout transfert de données vers l'extérieur nécessite une certaine euro-compatibilité. Il s'agit en effet de respecter les garanties des usagers du service numérique, d'ailleurs renforcées autour du droit à l'effacement des données concernant les mineurs, l'action collective, la réparation des dommages, ou encore la portabilité[7]. Toute violation de ce règlement fera l'objet de sanctions graduées par les autorités nationales puis européennes.
Leurs pratiques devraient être davantage harmonisées, par le Comité européen de la protection des données, qui succède au G29. Une faible marge de manœuvre reste envisageable pour toute question de forme propre à l'organisation administrative ou une certaine culture régalienne.

La directive *Network Information Security* (2016/1148) conforte ce règlement sous un aspect plus technique, en fixant un niveau commun élevé de sécurité des systèmes d'informations, auquel devront se conformer les États membres par le biais d'une stratégie nationale.
Ce corpus juridique devrait être prochainement renforcé par le projet de règlement eprivacy. Ce dernier vise en effet à remplacer la directive 2002/58, par des dispositifs capables d'appréhender les nouveaux usages numériques des internautes, dans un cadre plus respectueux de leur vie privée.
Enfin, s'agissant des données non personnelles, les États membres pourront, à leur convenance, ratifier la directive 2016/943 relative au secret des affaires, afin de protéger plus abondamment les entreprises contre l'espionnage.

L'implication britannique dans le marché unique numérique

Le Royaume-Uni doit s'engager sérieusement dans la transition numérique, d'abord

(6) Lagasse J., Le règlement général de protection des données, vers une grande charte des libertés de l'identité numérique ?, Note CREOGN N°22, mars 2017.

(7) Dans une optique économique, la Commission européenne envisage par ailleurs une extension de cette circulation sous le prisme de la propriété des données non personnelles : voir en ce sens l'avis du Conseil National du Numérique, La libre circulation des données dans l'Union européenne, avril 2017.

Une approche différente de l'identification des personnes dans certains pays européens est un obstacle à la pénétration des droits nationaux de la protection des données à caractère personnel.

parce que son implication européenne donnera le ton des relations postérieures avec l'Union, ensuite, pour satisfaire le lobby digital, fortement attaché à l'existence d'une régulation adéquate. Pour ce faire, le gouvernement a mené une évaluation de ses politiques publiques digitales dont le rapport publié le 21 décembre 2016, faisait état de la nécessité de mieux appréhender la gestion des risques cybernétiques. Il a par la même occasion manifesté son intention de mettre en œuvre le futur RGPD et la directive NIS. Son engagement est conforté par l'action de l'*Information Commissioner's Office* (autorité régulatrice équivalente à la CNIL), qui publie de nombreux guides et conseils pour les professionnels concernés.

Toutefois, certaines questions pratiques restent en suspens. Si la directive NIS prévoit l'instauration d'un système de coopération entre les États membres, capable de gérer les « incybersécurités » rencontrées par les opérateurs numériques, elle n'envisage pas pour autant d'éventuelles participations extérieures. Quid de la position du Royaume-Uni, en cas de sortie de l'Union, et plus largement de l'espace économique européen ? De plus l'exécutif britannique ne s'est pas encore prononcé sur la transposition à venir des directives « *eprivacy* » et « *secrets des affaires* ». S'il respecte ses obligations européennes, le temps du processus de sortie, sa position ultérieure reste pour autant incertaine.

Un long terme incertain : une attractivité priorisée

Si aucun doute ne subsiste quant au champ d'application personnel du RGPD,

rien n'indique que le Royaume-Uni maintiendra après sa sortie un niveau de protection équivalent pour les citoyens non-européens. Il pourrait ainsi développer, de manière stratégique, une « attractivité data » communément acceptable.

Les différentes options data du Brexit

L'application du RGPD pourrait être poursuivie, si le Royaume-Uni décidait de se maintenir dans l'Union – ce qui reste théoriquement envisageable-, mais également en cas d'adoption de l'accord portant sur l'Espace économique européen, à l'instar de la Norvège. Cela permettrait de conserver un certain accès au marché tout en diminuant les contributions budgétaires. Toutefois, aucun contrôle migratoire ne serait admis et l'influence britannique sur les politiques communautaires serait limitée.
D'autres formes de partenariats plus ténues pourraient être envisagées. Une adhésion à l'Association européenne de libre échange, analogue au modèle suisse, permettrait de disposer d'un accès gratuit au marché. Agrémenté d'un traité relatif à la protection des données compatible avec le RGPD, le secteur numérique n'en serait que peu affecté. Pour autant, cette hypothèse semble inadéquate, car elle entraînerait une exclusion de la libre circulation des services financiers, ainsi qu'une impossibilité de restreindre les flux migratoires européens, accompagnée d'une participation budgétaire atténuée. L'Accord économique et commercial global, canado-européen, constitue en revanche un précédant plus pertinent. Il implique un accès au marché unique, par le biais de tarifs préférentiels et de subventions de péréquation. Un traité « data compatible » devrait également être adopté entre le Royaume-Uni et l'Union européenne. Le « *privacy shield* » et les standards ISO offrent alors des illustrations pertinentes. Quoi qu'il en soit, le Brexit ne présente aucune option parfaite, et nécessite des compromis.

Vers un dumping régulatoire communément acceptable ?

Pour le Royaume-Uni, le Brexit renvoie avant tout à une quête souverainiste. Pour preuve, les arguments de campagne des « *brexiters* », ayant prévalu lors du référendum en date du 23 juin 2016 avec près de 51,9 % des voix, font état de la nécessité d'établir un nouvel espace de libre échange, exempt de toutes contraintes budgétaires et réglementaires, tel que peut l'être l'impossible contrôle migratoire. Bien que ce résultat soit profondément discuté, une nouvelle consultation populaire ne devrait avoir lieu, car elle aboutirait à un déni de démocratie. L'hypothèse du maintien du Royaume-Uni apparaît alors en pratique peu probable. Il reste alors à poursuivre le processus de sortie, dans un contexte agité, tant par les contradictions politiques émanant de la Première ministre et du ministre des Finances, que par l'incertitude de leur direction. L'objectif serait en effet de parvenir à un juste équilibre entre une perte

de gouvernance internationale et la mise en place d'un espace économique plus libéral. Pour autant, le Royaume-Uni n'envisage aucunement de se positionner en ermite sur la scène internationale. Du fait de sa dépendance au marché unique, il entretiendra certainement une relation économique avec l'Union, mais de manière plus ténue, et ouverte sur l'extérieur. Il reste à savoir dans quel contexte il pourra négocier.
L'Union Européenne se positionne quant à elle de manière plus éclairée et organisée, parce qu'au-delà d'une désunion apparente, elle perçoit davantage l'opportunité de se renouveler, autour d'un projet plus approprié, pour chacune des parties, évitant ainsi les entraves qu'elles ont connues. Pour ce faire, les 27 sont convenus de grandes orientations visant à guider Michel Barnier dans la négociation. Elles devront d'abord se concentrer sur les modalités pratiques de rupture, avant d'envisager une relation économique constructive. Cela permettra également d'éviter tout risque « d'Europe à la carte », dont pourrait bénéficier injustement le Royaume-Uni, en procédant notamment à un maintien sur le marché accompagné d'une politique de gestion migratoire et de « *dumping* ». Dans cette optique, les modèles suisse et canadien paraîtraient pertinents, à commencer par le plan économique.
L'économie britannique semble résister aux pronostiques désastreux formulés par de nombreux économistes. Si cela s'explique par une certaine stabilité de la consommation des ménages, la situation particulière du secteur numérique est en revanche plus complexe. Contrariés, certains experts, tel que Stephen Hawking, s'alarment de ce « *désastre* » qui affecterait le marché digital et la libre circulation des spécialistes, encore que la migration choisie reste envisageable. De plus, la perspective du Brexit interroge sur le futur niveau de protection des données. C'est pourquoi certaines entreprises soucieuses d'une réglementation stricte, telles que General Electric ou Sup, envisagent de fermer des établissements à l'inverse de Google et Facebook, plus attirés par une souplesse éventuelle, et la conquête de nouveaux marchés sur un territoire disposant d'une culture similaire et d'une connexion à l'Europe. L'abandon futur du RGPD au profit d'une réglementation plus souple conférerait un cadre plus adapté et dynamique aux petites entreprises. Son euro-compatibilité contribuerait par la même à une certaine harmonisation de la régulation disciplinaire. Un tel cadre de protection, constaté par une décision d'adéquation de la Commission, permettrait le transfert de données vers ce nouvel Etat tiers[8], et contribuerait à la stabilité du secteur. Cette hypothèse semble corroborée par la position actuelle de l'Angleterre, qui souhaite négocier un accord UE-UK sur la protection des données à caractère personnel[9].

(8) Transfert fondé sur une décision d'adéquation – article 45 du RGPD

(9) « Brexit : le gouvernement britannique demande un accord UE-UK sur l'échange et la protection des données personnelles Avant sa sortie de l'Union », 26 août 2017, Michael Guilloux, Chroniqueur Actualités, developpez.com

Qu'il soit « *soft* » ou « *hard* », le Brexit n'aura vraisemblablement que peu de conséquences en termes de protection des données. Cette dernière devrait ainsi relever du RGPD, ou tout du moins d'un niveau comparable pour les citoyens non-européens. Il s'agit avant tout d'une quête souverainiste menée par le Royaume-Uni, dont le cap et la portée demeurent indéterminés. «*Tels se laissent gouverner jusqu'à un certain point, qui au-delà sont intraitables et ne se gouvernent plus : on perd tout à coup la route de leur cœur et de leur esprit ; ni hauteur ni souplesse, ni force ni industrie ne les peuvent dompter ; avec cette différence que quelques-uns sont ainsi faits par raison et avec fondement, et quelques-autres par tempérament et par humeur* » - Les Caractères – La Bruyère.

AdobStock

L'OTAN OUVRE UN CINQUIÈME DOMAINE OPÉRATIONNEL

La position de l'OTAN a évolué en fonction de l'évaluation des menaces qui peuvent affecter les pays alliés. La question de la constitution du cyberespace comme un nouveau domaine opérationnel est acquise du fait que la nature et l'intensité des cyberattaques atteignent déjà l'équilibre des institutions démocratiques. Des campagnes de désinformation, une immixtion dans les sphères décisionnelles du monde politique et une désorganisation des systèmes de commandement militaire ou des organisations d'intérêt vital peuvent infléchir les positions d'un pays voire le paralyser. La nouvelle feuille de route de l'OTAN privilégie l'assurance des missions par rapport à celle des systèmes d'information. Elle pose le principe d'une réponse offensive graduée et du partage des capacités des alliés. Sauf certains secteurs sanctuarisés, comme la dissuasion nucléaire et la défense antimissile, l'idée prédominante est la constitution de partenariats avec les industriels compétents, l'exploitation de leurs méthodes de priorisation, d'optimisation des productions, et de constituer des chaînes d'approvisionnement sécurisées.

Cyberdéfense : l'OTAN monte en puissance

Par JAMIE SHEA

NDR : Jamie Shea est le secrétaire général adjoint délégué de l'OTAN pour les défis de sécurité émergents. Les avis exprimés dans cet article n'engagent que leur auteur. Ils ne reflètent nullement une quelconque position officielle de l'OTAN et sont livrés ici à titre purement personnel.

L'élaboration d'une politique se fait généralement en deux temps. Elle commence par une phase de réflexion et de consultation destinée à préparer de nouvelles initiatives ou à actualiser des documents d'orientation existants pour les adapter à de nouveaux enjeux. Elle doit se poursuivre par une phase de mise en oeuvre permettant à ces initiatives d'engendrer des capacités essentielles et des changements organisationnels. Les initiatives qui ne sont pas concrétisées ont aussi peu d'utilité qu'une action improvisée, sans notion de stratégie ou d'objectif à atteindre, ou sans capacité à évaluer périodiquement si une politique va ou non dans la bonne direction.

JAMIE SHEA

Secrétaire général adjoint délégué de l'OTAN

L'année 2016 a été pour l'OTAN une année très active en termes d'élaboration de politique et de prise de décision dans le domaine de la cyberdéfense. À plus d'un titre, elle a aussi été une année charnière, au cours de laquelle il est apparu que la cyberdéfense ne consistait plus seulement à protéger les réseaux contre des cyberattaques de plus en plus diversifiées et complexes, mais qu'elle était aussi désormais un enjeu pour l'intégrité des institutions démocratiques des pays de l'OTAN. L'usage détourné du cyberespace est devenu un moyen non seulement de se procurer ou de manipuler des données, ou encore de perturber le fonctionnement de tel ou tel réseau, mais aussi d'influencer le résultat de processus politiques, voire d'exercer purement et simplement des pressions politiques et des manœuvres d'intimidation. La France n'a pas été épargnée par les cyberattaques stratégiques, comme on l'a vu avec l'interruption des programmes de la chaîne TV5 Monde ou le piratage de boîtes

mail de l'équipe de campagne d'Emmanuel Macron, alors candidat à la présidence.

Des cyberattaques à la guerre hybride

L'année 2016 a véritablement marqué un tournant : la cybermenace, jusqu'alors essentiellement sujet de préoccupation pour des entités qui, comme les banques, les opérateurs d'importance vitale ou les hôpitaux, craignent la perte de données, est devenue un instrument de guerre hybride, qui met l'État et la société à la merci d'attaques permanentes. En 2014 déjà, l'OTAN avait déclaré qu'au-delà d'un certain seuil, une cyberattaque pouvait être considérée comme une attaque armée pouvant justifier le recours à la clause de défense collective énoncée dans l'article 5 du Traité fondateur de l'OTAN. À l'époque, une telle perspective semblait encore hypothétique ou lointaine. Mais, alors même que l'ampleur nouvelle des cyberattaques met en évidence la difficulté de contrer ce type d'activité, et que les États exposés à cette menace commencent à développer un sentiment d'insécurité et de vulnérabilité, il devient de plus en plus vraisemblable qu'une cyberattaque soit un jour assimilée à une attaque armée et qu'elle suscite une réponse collective allant au-delà de la simple protestation diplomatique.

Du tactique au stratégique

C'est sur la base de ce constat que l'OTAN a décidé de muscler sa cyberdéfense.

Trois stades de menaces

La première réponse de notre Organisation a été de déclarer, à l'occasion du sommet de l'Alliance tenu à Varsovie en juillet 2016, qu'elle considérait désormais le cyberespace comme un domaine opérationnel. Cela signifie en substance que l'OTAN a décidé de faire passer l'assurance de la mission avant celle de l'information ; en d'autres termes, d'assurer en priorité la cyberdéfense de chacune de ses activités militaires avant de protéger ses propres réseaux internes. Ce changement de priorité résulte d'une prise de conscience : les cybermenaces seront désormais présentes aux trois stades de l'engagement de l'OTAN :

– D'abord en situation de pré-crise, où l'Alliance peut s'attendre à une intensification des opérations d'espionnage et des tentatives de pénétration de ses réseaux, ainsi qu'à une plus grande sophistication des campagnes de désinformation et à des opérations psychologiques. Toutes ces actions ont pour but de saper le soutien en faveur des décisions de l'OTAN en manipulant les données et en distillant de fausses informations. En témoignent les récentes allégations visant des soldats allemands, du contingent OTAN déployé en Lituanie, accusés d'avoir commis des viols ou de mener des opérations psychologiques à l'encontre de la population locale.

– Ensuite au deuxième stade, celui de la crise proprement dite, où les cyberattaques

pourraient être utilisées à diverses fins : pour perturber le dispositif de commandement et de contrôle ou les activités de renforcement menées par l'Organisation en Europe centrale et orientale, pour conduire des opérations de sabotage contre des infrastructures vitales (systèmes de contrôle de la circulation aérienne, ports, aérodromes, pipelines, *etc.*) et pour bloquer l'accès à d'autres serveurs et réseaux.

– Enfin au troisième stade, celui du conflit déclaré, où l'OTAN doit s'adapter à la nécessité d'opérer dans un environnement cyber dégradé, où l'accès total et permanent à ses réseaux ne serait pas nécessairement assuré et où il faudrait improviser rapidement des solutions de rechange pour disposer d'une fonctionnalité minimale. Nous pourrions aussi devoir faire face à des tentatives de perturbation de nos systèmes militaires, tels que les drones, les satellites, les systèmes de défense aérienne et antimissile.

Une nouvelle feuille de route

Pour s'adapter à cette nouvelle réalité, dans laquelle le cyber est, en tant que tel, un cinquième domaine de la guerre qui influence aussi les quatre autres traditionnels (air, terre, mer, espace), les ministres de la Défense des pays de l'OTAN, réunis en février dernier, ont approuvé une feuille de route précisant les mesures à prendre pour que l'Alliance puisse pleinement mettre en œuvre ce concept de domaine d'ici à 2019.

La feuille de route préconise une relation plus étroite entre, d'une part, le Commandant suprême des forces alliées en Europe et son commandement allié Opérations et, d'autre part, l'Agence OTAN d'information et de communication basée à La Haye. Cette dernière est chargée de la protection et du contrôle quotidiens des réseaux de l'OTAN en temps de paix, ainsi que de la sécurité et de l'acquisition des systèmes informatiques de l'OTAN. Au fur et à mesure que nous passons de l'assurance de nos systèmes d'information à l'assurance de nos missions et opérations, des structures de commandement seront nécessaires pour garantir la coordination entre le Commandement des opérations (ACO) et l'Agence NCIA (NATO Communications and Information Agency), y compris le transfert de responsabilité des civils aux militaires en cas de crise.

Il est entrepris d'actualiser des plans de réponse graduée pour la défense de l'Europe orientale, en vue de mieux intégrer et prioriser les activités de cyberdéfense et d'avoir une vision plus claire des besoins cyber pour les opérations. Il faudrait par exemple réfléchir aux effets cyber à générer très en amont et à la manière de mieux intégrer la dimension cyber, non seulement dans la nouvelle structure de commandement de l'OTAN, mais aussi dans les mesures spécifiques de réponse aux crises que le Conseil de l'Atlantique Nord autoriserait à mettre en œuvre par le commandant suprême des forces alliées

© Sdecoret - Adobe Stock

Un partage des ressources et l'élévation du potentiel des maillons faibles permettant d'offrir une grande cohérence au dispositifs offensifs et défensifs de l'OTAN.

en Europe (SACEUR). À l'évidence, le cyber a favorisé le développement accéléré des crises, d'où la nécessité d'avoir une connaissance très anticipée et affinée de la situation ainsi qu'un processus décisionnel réactif. Agir vite et au moment opportun est devenu le nouveau mot d'ordre. C'est pourquoi les commandants militaires de l'OTAN travaillent actuellement à l'élaboration d'un ensemble de mesures de réponse aux crises devant leur permettre d'effectuer une analyse préalable des réseaux, de prendre des mesures de défense active et d'activer une capacité de réponse OTAN « de réserve » qui pourrait être gérée par un Nouveau centre opérationnel OTAN de réaction aux cyberincidents (NCIRC). Enfin, la décision de faire du cyberespace un domaine opérationnel va également amener l'OTAN à s'informer auprès des Alliés déjà engagés dans cette voie — États-Unis, Royaume-Uni, France et Pays-Bas, notamment — quant au fonctionnement de leurs modèles et à l'emploi des moyens cyber dans leurs opérations militaires. Cela a d'autant plus d'importance que l'OTAN ne développera pas de capacités cyber offensives et qu'elle devra donc pouvoir s'appuyer sur des capacités nationales (sous réserve d'un accord au niveau politique à l'échelle de l'OTAN) dans des situations où les commandants militaires de l'OTAN jugeraient préférable d'utiliser un moyen cyber plutôt qu'une arme conventionnelle pour obtenir l'effet final recherché sur le plan militaire.

Une plus grande transparence et des investissements mieux ciblés

La deuxième initiative majeure prise par l'OTAN au sommet de Varsovie a été l'engagement en faveur de la cyberdéfense. Celui-ci vient compléter une disposition antérieure, prise en 2014 au sommet du pays de Galles, en vertu de laquelle chaque pays de l'Alliance s'engageait à consacrer au moins 2 % de son PIB à la défense. À travers l'engagement en faveur de la cyberdéfense, les Alliés acceptent de consacrer au moins une partie de cet investissement supplémentaire à l'amélioration des capacités nationales de cyberdéfense, sans qu'un montant minimal soit spécifié. Or, pour que la cyberdéfense soit efficace, il faut pouvoir bâtir une communauté de confiance ne comportant aucun maillon faible. Faute de quoi, les pays disposant d'une capacité de cyberdéfense pourraient être réticents à partager leur expertise et des informations sensibles avec d'autres Alliés n'ayant pas amené leurs moyens cyber à un niveau de sécurité minimal. Sachant que, dans presque tous les domaines, l'OTAN s'appuie davantage sur les moyens mis à disposition par les Alliés (exception faite des AWAC) que sur ses moyens propres, son aptitude à opérer dans le domaine cyber dépend de sa capacité à fixer des objectifs capacitaires plus ambitieux aux pays membres et à encourager ces derniers à combler les lacunes recensées. En incitant les Alliés à évaluer plus régulièrement leurs niveaux de préparation, l'engagement en faveur de la cyberdéfense devrait à l'avenir faciliter ce processus. Les pays de l'OTAN ont entrepris d'évaluer l'état de santé de leur dispositif de cyberdéfense dans chacune des sept catégories capacitaires : stratégie, organisation, processus et procédures, renseignement sur la menace, partenariats, capacités, investissements. Il leur a été demandé d'évaluer leurs résultats sur une échelle de quatre niveaux selon que le dispositif est plus ou moins avancé. Sur la base des réponses fournies par les pays, les services de l'OTAN seront à même d'établir des métriques plus précises et plus pertinentes et de constituer une base de référence commune plus fiable répertoriant l'ensemble des capacités OTAN. Cette plus grande transparence les aidera par la suite à identifier les lacunes et à prioriser les besoins. À partir de là, le processus OTAN bien rôdé de planification de défense — qui intègre déjà une série d'objectifs capacitaires de base en matière de cyberdéfense fixés à chaque pays membre — permettra de proposer des objectifs plus ambitieux et mieux adaptés aux besoins futurs de chaque pays. L'émulation que cette transparence accrue devrait susciter entre Alliés incitera les pays à atteindre les objectifs fixés et stimulera l'aide bilatérale.

Bâtir une véritable communauté de la cyberdéfense

Outre les deux initiatives majeures lancées au sommet de Varsovie, une grande part des efforts déployés par l'OTAN pour muscler sa cyberdéfense est destinée à

renforcer son rôle de plateforme, le but étant d'apporter une aide aux Alliés pour tout un éventail de besoins cyber. Les pays membres se sont ainsi vus proposer un mémorandum d'entente actualisé visant à améliorer la coopération entre le siège de l'OTAN et les Alliés pour ce qui est du partage du renseignement, de la gestion de crise et du retour d'expérience concernant les cyberattaques. Les vingt-neuf pays, signataires du mémorandum initial, continuent d'en appliquer les dispositions et vingt-deux d'entre eux ont déjà signé le mémorandum actualisé. L'OTAN a également mis en place une nouvelle Division Renseignement nettement orientée cybermenace, ce qui devrait inciter les pays membres à signaler plus en amont des cyberattaques ou la présence de logiciels malveillants, plutôt que de communiquer uniquement des informations en retour sur un incident survenu plusieurs semaines auparavant. L'amélioration du partage du renseignement entre Alliés aidera non seulement à prévenir les cyberattaques ou à en limiter l'impact, mais aussi à se faire progressivement une idée beaucoup plus précise et complète des groupes de hackers, de leurs intermédiaires, de leurs méthodes, ainsi que des techniques d'attribution.

L'une des contributions les plus utiles que l'OTAN apporte à ses pays membres est l'organisation de formations théoriques/pratiques et d'exercices destinés à améliorer les compétences, non seulement pour les 200 opérateurs travaillant pour le NCIRC et la structure de commandement de l'OTAN, mais aussi pour les équipes de cyberdéfense de chaque pays. L'exercice annuel Cyber Coalition attire désormais plus de sept cents participants ; quant à l'exercice Locked Shields, il est reconnu comme l'un des exercices les plus exigeants et intensifs opposant une équipe rouge à une équipe bleue. Ces deux exercices se déroulent en Estonie avec la collaboration du Centre d'excellence OTAN pour la cyberdéfense, sur un polygone d'exercices de cyberdéfense récemment modernisé que ce pays met à la disposition de l'OTAN. En plus des exercices, il faut que les personnels civils et militaires de l'OTAN suivent régulièrement des formations sur les concepts et les procédures de base en matière de cyberdéfense, et que des séances d'information sur « l'hygiène informatique » soient organisées pour les utilisateurs dans l'ensemble de l'OTAN. Au sein de l'Alliance, le Portugal est le pays de référence pour ce type de formations ; il va bientôt accueillir, à Oeiras, l'École des systèmes d'information et de communication de l'OTAN (NCISS), auparavant implantée en Italie, à Latina.

Parallèlement, l'OTAN apporte son aide aux Alliés qui ont accepté de piloter des projets de défense intelligente dans le domaine de la cyberdéfense. À côté du projet de formation dirigé par le Portugal, un projet de plateforme pour le partage du renseignement sur les logiciels malveillants

a été mené à bien par un groupe piloté par la Belgique ; cette plateforme est non seulement utilisée entre Alliés, mais aussi entre l'OTAN et l'Union européenne. Une variante est également employée pour faciliter l'échange d'informations entre l'OTAN et les acteurs industriels, et on pourrait envisager de déployer d'autres plateformes, plus ouvertes et plus sécurisées selon le niveau d'accès exigé et la sensibilité des informations à partager. Un troisième projet de cyberdéfense porte sur la connaissance de la situation et la coordination en cas d'incident et inclut un contrat d'exploitation et de maintenance. Le dispositif proposé a été mis en place avec succès par les Pays-Bas et la Roumanie. Au total, vingt-cinq pays de l'Alliance et six pays partenaires prennent part à des projets de défense intelligente.

Seule l'union fait la force

Pour cette montée en puissance dans le domaine cyber, l'OTAN doit aussi pouvoir s'appuyer sur des partenariats encore plus forts. La collaboration est bien sûr le maître-mot, car nous savons tous que le succès de la cyberdéfense dépend de la capacité à rassembler autour d'une même table un panel d'intervenants beaucoup plus large qu'auparavant, alors que des problématiques telles que la dissuasion nucléaire ou la défense antimissile étaient traitées dans des cercles nettement plus restreints et globalement homogènes. Toutefois, la collaboration, même si elle est nécessaire, n'est pas pour autant automatique. Il faut déployer en permanence beaucoup d'attention et de ressources pour nouer et entretenir une relation. Il faut aussi avoir des incitants à offrir afin qu'à terme les partenaires soient convaincus qu'ils retirent de cette relation un bénéfice équivalant à l'effort qui leur est demandé.

Dans ce contexte, l'OTAN s'est tournée principalement vers l'industrie, avec laquelle elle a établi un cyberpartenariat. À ce jour, l'Agence OTAN d'information et de communication a conclu avec les acteurs industriels douze arrangements pour le partage de renseignements et d'indicateurs d'alerte précoce sur la menace cyber. La nouvelle série d'ateliers OTAN-industrie, notamment le symposium OTAN sur l'assurance de l'information organisé chaque année à Mons, et les ateliers sur l'analyse des vecteurs de menaces sont pour les représentants de l'industrie et de l'OTAN autant d'occasions de se rencontrer pour parler d'innovation, de meilleures pratiques d'acquisition et de renseignement sur la menace. L'OTAN s'intéresse également à l'expérience de l'industrie en matière de priorisation des ressources — dans un contexte de budgets limités, quand faut-il donner la priorité au personnel et à l'expertise plutôt qu'à la mise à niveau technologique ou à l'amélioration des processus ? Cette collaboration plus en amont avec l'industrie devrait aussi aider l'OTAN à mieux connaître les produits de sécurité disponibles sur le marché et à en tirer parti, tout en aidant l'industrie à mieux anticiper

les tendances des acquisitions futures de l'OTAN. La collaboration OTAN-industrie permettrait également d'optimiser la gestion de la chaîne d'approvisionnement et d'élargir l'offre. Le Forum international sur la cybersecurité qui se tient chaque année à Lille au mois de février est un rendez-vous très fructueux au cours duquel les experts de l'OTAN rencontrent les principales PME françaises et européennes qui, à elles seules, produisent 80 % des innovations cyber au sein de l'Union européenne. Pour les Alliés, ces évènements sont désormais l'occasion d'échanger davantage d'informations concernant leurs industries stratégiques. Ainsi, si l'un d'eux est confronté à un cyberincident, touchant par exemple une centrale électrique ou un réseau de distribution d'eau, il peut plus facilement trouver dans l'un des autres pays de l'OTAN une entreprise capable de lui fournir rapidement une solution technologique certifiée et la garantie d'une chaîne d'approvisionnement sécurisée.

Parallèlement à cela, l'OTAN a entrepris de renforcer ses relations avec d'autres pays ayant conclu un arrangement de partenariat officiel avec l'Alliance. Un accord-cadre politique sur la coopération en matière de cyberdéfense a récemment été signé avec la Finlande. Un fonds d'affectation spéciale OTAN-Ukraine a été créé pour l'acquisition d'équipements de cyberdéfense et de moyens analytiques et inforensiques. Par ailleurs, l'OTAN apporte une aide à des pays comme la Jordanie, la Moldavie et la Géorgie, pour l'organisation de la cyberdéfense au niveau national, ainsi que pour la doctrine ou l'entraînement. Les pays partenaires sont de plus en plus nombreux à rejoindre le Centre d'excellence pour la cyberdéfense en coopération (CCD COE) de Tallin ou à y envoyer des personnels ou des observateurs. À Bruxelles, l'OTAN et l'Union européenne opèrent un net rapprochement dans le domaine de la cyberdéfense. Un arrangement technique sur le partage d'informations non classifiées entre le NCIRC de l'OTAN et le CERT de l'UE est entré en vigueur il y a plus d'un an. Un plan d'action pour la mise en application de la déclaration commune OTAN-UE a été adopté en décembre dernier par les deux organisations, qui entendent renforcer leur interaction à différents niveaux : échange d'informations sur la planification opérationnelle de la cyberdéfense lors de missions militaires, harmonisation des besoins de formation, développement de la coopération en matière de Recherche et développement (R&D) et de la normalisation entre l'Agence européenne de défense et le Commandement allié Transformation de l'OTAN, et participation mutuelle renforcée aux entraînements et aux exercices de type CMX et Cyber Coalition (OTAN) et Cyber Europe (UE). Récemment, le secrétaire général de l'OTAN a participé au premier exercice sur table de gestion de crise cyber (Cybrid) conduit par les ministres de la Défense des pays de l'UE.

C'est là un autre signe fort de l'interaction grandissante entre l'OTAN et l'UE, même dans un domaine aussi sensible que la cyberdéfense.

Durcir les sanctions et réduire les profits

En conclusion, le domaine cyber est différent des autres domaines de conflit. Le rythme de l'innovation y est beaucoup plus rapide. La technologie utilisée est nettement plus décentralisée et les acteurs sont beaucoup plus nombreux, pour le meilleur et pour le pire. Pour qu'une structure de cyberdéfense soit performante, il faut pouvoir répartir les ressources entre des fonctions beaucoup plus nombreuses et les affecter de manière beaucoup plus ciblée que pour un programme capacitaire conventionnel. Il faut aussi pouvoir suivre et évaluer simultanément beaucoup plus de pays, de groupes et de niveaux de menace et de risque que lorsqu'on doit faire face à des adversaires conventionnels ou nucléaires classiques.

L'attribution des cyberattaques pose problème et, comme l'a montré la récente affaire de piratage lors de l'élection présidentielle américaine, il reste difficile de déterminer avec certitude dans quel cas une cyberattaque, qui ne fait pas nécessairement de victimes humaines ou de dommages matériels, peut être véritablement considérée comme un acte d'agression motivant une réponse appropriée. Alors que nous avons une bonne idée des modalités de la dissuasion face à une menace d'attaque nucléaire ou conventionnelle, d'une gestion de crise dans les domaines traditionnels ou des arrangements de maîtrise des armements et des mesures de confiance utiles pour préserver la paix, nous ne savons toujours pas précisément quels moyens de dissuasion ou quelle réponse opposer à des cyberattaques de grande envergure, même lorsque celles-ci visent clairement à déstabiliser nos gouvernements ou nos processus politiques. Nous pouvons tenter en coulisses d'en dissuader les auteurs potentiels. Nous pouvons aussi prendre des sanctions à l'encontre d'individus ou d'organisations, comme l'ont fait les États-Unis en réponse à l'attaque contre Yahoo et aux ingérences dans l'élection présidentielle. Mais si les perspectives de profit compensent largement les risques de sanctions, la dissuasion sera sans effet. Nous allons donc devoir réfléchir à une approche plus stratégique consistant à renforcer les sanctions tout en limitant les perspectives de profit.

DÉFENSE

Sirpa-gendarmerie - Julien Eichinger

LA RECHERCHE DE LA SUPERIORITÉ NUMÉRIQUE EST UN FACTEUR ESSENTIEL DU SUCCÈS DE NOS ARMÉES

L'espace numérique est devenu un théâtre d'opération comme un autre. La défense de la France et de l'Europe nécessite une adéquation au champ de bataille numérique notamment dans le cadre des conflits asymétriques avec des groupes terroristes. La cyber-résilience suppose une capacité à murer nos systèmes vitaux et à réagir offensivement en cas d'attaque dans l'espace numérique. Notre supériorité opérationnelle doit être soutenue par la démonstration de notre capacité dans le cyberespace à maîtriser voire à porter une menace qui paralyse les moyens de commandement et de production de l'adversaire.

La France s'est dotée d'une doctrine et d'une organisation renouvelées propres à engager un combat numérique. Elle promeut un modèle construit dans une logique d'économie des forces, de mutualisation des compétences civiles et militaires et de construction de réseaux d'expertise. Elle assume un rôle moteur au sein de l'OTAN, de l'Europe de la Défense et dans le développement de la coopération internationale.

La Cyberdéfense :
un modèle solide et agile pour le combat numérique

Par OLIVIER BONNET DE PAILLERETS

Cette année, le FIC 2018 se projette dans l'ère de l'hyperconnexion et de l'« *Internet of Everything* ». Dès 2020, les individus et les machines seront connectés en permanence par l'intermédiaire de réseaux d'infrastructures, de services numériques et de systèmes d'informations, eux-mêmes interconnectés. Cette hyperconnexion exige que le défi de la cyber-résilience soit relevé dès maintenant.

OLIVIER BONNET DE PAILLERETS

Général (armée de Terre), commandant la cyberdéfense, état-major des armées

La révolution numérique, à l'œuvre depuis une trentaine d'années déjà, modifie profondément nos modes de vies et nos organisations, à commencer par ceux du ministère des Armées. La cyber-résilience suppose une capacité de notre système, composé d'experts, de processus et de techniques, à faire face aux conséquences d'une attaque dans l'espace numérique et à maintenir notre aptitude à agir et réagir. La cyber-résilience est le gage de la confiance numérique. Celle-ci s'inscrit aujourd'hui dans une vision européenne de la cybersécurité et de la cyberdéfense.

Une révolution technologique qui modifie totalement le spectre de menaces

L'espace numérique ou cyberespace est un domaine d'innovation, d'adaptation continue et de confrontation à la fois nouveau, en comparaison des autres domaines de confrontation, et en constante évolution. Nouveau, il demande à être enraciné de façon solide pour continuer à se développer, tout en assurant la sécurité et la protection de ceux qui y opèrent ; en évolution constante, il requiert une approche agile qui nécessite de repenser nos

organisations et nos rapports de pouvoir. Depuis 2011, le ministère de la Défense, puis des Armées, et plus spécifiquement le Commandement de la cyberdéfense construisent de façon solide et pérenne un modèle agile et efficace de cyberdéfense.

L'espace numérique dispose de sa propre dynamique liée à une expansion technique qui semble ne pas connaître de limite : hier l'interconnexion des réseaux, aujourd'hui le développement des puissances de calcul dans l'exploitation des données, demain l'explosion du nombre d'objets connectés, après-demain les processeurs quantiques. Internet constitue probablement la révolution technique humaine la plus innovante : il est source de richesses et vecteur de connaissances, de nouveaux modèles économiques et culturels ; il raccourcit les distances, rapproche les hommes et les femmes. Le centre de gravité de nos sociétés, jusqu'alors essentiellement lié à des populations et des territoires, se déplace progressivement dans ce nouvel espace. La dépendance au numérique s'accroît au rythme des progrès techniques et renforce par-là même l'exposition à des vulnérabilités nouvelles.

Nous pouvons aujourd'hui définir quatre grandes catégories de cyber-menaces : l'atteinte à l'image (défiguration de sites officiels, campagne de dénigrement, usurpation d'identité, propagande, amplification de rumeurs, déstabilisation…), l'action « mafieuse » (arnaque à la carte bancaire, rançons, trafics en tous genres,…), l'espionnage (détournement discret d'informations circulant sur les réseaux numériques d'une cible) et le sabotage (altération du fonctionnement d'un système par le biais d'une attaque informatique).

Ces menaces qui naissent dans l'espace numérique ont les mêmes caractéristiques que celles de l'espace physique : des individus malfaisants y préparent des actes terroristes, désinforment, leurrent, volent ou encore détruisent. Les frontières qui séparent ces acteurs (cybercriminels, hacktivistes, États, groupes terroristes, etc.) sont poreuses et la diversité des menaces qu'ils génèrent est extrêmement grande (de l'attaque sur un système de vote électronique, à la paralysie de médias, en passant par l'extinction d'un système électrique, par exemple). Ces scénarios de paralysie ou de destruction s'appuient sur des réalités profondément asymétriques : de faibles moyens permettent d'obtenir des effets importants, analogues à ceux d'actions plus conventionnelles, en particulier lorsqu'ils visent des infrastructures civiles critiques, voire des cibles militaires.

La fréquence et l'ampleur des attaques augmentent sans cesse dans le cyberespace, témoignant d'une prolifération préoccupante des moyens d'agression. Si peu d'États disposent à l'heure actuelle des moyens de mener des actions cyber offensives de grande ampleur, causant des dommages importants, leur nombre

et leurs capacités devraient s'accroître rapidement sous l'effet du faible coût et de la diffusion rapide des technologies numériques. Ensuite, l'arme cyber, dont la conception nécessite parfois des moyens colossaux, est susceptible d'être copiée et répliquée très facilement. Utilisant actuellement Internet à des fins de planification, de propagande et de recrutement, les groupes terroristes pourraient ainsi devenir des acteurs à part entière du domaine cyber. Et nous connaissons tous les difficultés qui existent dans la détermination de l'origine des attaques.

Une doctrine renouvelée pour asseoir une cyberdéfense évolutive

Pour protéger, défendre et agir vis-à-vis de ces cyber-menaces, la cyberdéfense française s'est construite à partir d'efforts conséquents. À son arrivée au ministère de la Défense en 2012, M. Jean-Yves Le Drian, à présent ministre de l'Europe et des Affaires étrangères, avait fait de la cyberdéfense l'une de ses priorités. Confrontée à des adversaires, des ennemis, ou des concurrents dotés de capacités informatiques offensives, la France a bénéficié d'un ambitieux plan d'action ministériel, fondé sur une doctrine et une organisation renouvelées, permettant à nos forces de se déployer et de conduire, face à cette menace, le combat numérique.

Le Livre Blanc de la Défense et de la Sécurité nationale avait fait état, pour la première fois en 2008, de la menace portée par le développement de l'espace numérique. La création de l'Agence Nationale de Sécurité des Systèmes d'Information a suivi en 2009, puis celle du poste d'officier général de cyberdéfense en 2011. La structure de cyberdéfense n'a ensuite cessé, tout au long de ces six années, de se développer pour s'adapter aux nombreux enjeux opérationnels. Le Livre Blanc de la Défense et de la Sécurité nationale de 2013 est venu préciser qu'« au sein de la doctrine nationale, la capacité informatique offensive, associée à une capacité de renseignement, concourt de façon significative à la posture de cybersécurité. » Le Centre opérationnel de cyberdéfense est ainsi indissociable de la planification et de la conduite des opérations ; il commande et contrôle l'ensemble des actions conduites par les armées dans l'espace numérique.

Le Pacte Défense Cyber 2014-2016 a également mobilisé tout le ministère de la Défense dans l'objectif de faire de la France une grande puissance militaire de la cyberdéfense et de faire émerger une communauté nationale de cyberdéfense. Plus de 150 citoyens sont dorénavant prêts à relayer l'esprit de cyberdéfense à travers leur engagement dans la réserve citoyenne de cyberdéfense. Un groupe de 4400 citoyens, dès 2019, sera en mesure d'intervenir auprès des forces, en cas d'attaque cyber majeure, dans la cadre de la réserve de cyberdéfense opérationnelle. La France a aussi organisé plusieurs exercices DEFNET (2014-2015-2016-2017)

La supériorité opérationnelle passe par une posture crédible en termes d'action numérique dans le cyberespace.

pour la chaîne de commandement cyber et ses partenaires de la société civile, et a participé activement aux grands exercices internationaux comme Cybercoalition ou Locked Shields. Elle assume un rôle moteur au sein de l'OTAN et de l'Europe de la Défense, et dans le développement de la coopération internationale.

Pour garantir la souveraineté nationale dans l'espace numérique, le ministère des Armées dispose de capacités à se protéger contre les attaques informatiques, à les détecter et à en identifier les auteurs. Il dispose également de la capacité à exploiter les failles informatiques d'un ennemi, en contexte de confrontation, et à maîtriser toutes les facettes du combat numérique. Le Commandant de la cyberdéfense est ainsi placé sous l'autorité directe du chef d'état-major des armées, à l'image du commandement des opérations spéciales. Il est chargé de la protection, de la défense des systèmes d'information du ministère et de la conduite d'actions numériques à l'encontre des systèmes d'information adverses.

La cyberprotection consiste à bâtir d'épaisses murailles autour des systèmes d'information, ainsi qu'à mesurer en permanence leur efficacité face à une menace toujours évolutive. La défense vient en complément : plus dynamique, elle consiste à patrouiller, guetter, surveiller et intervenir sur les systèmes d'information en cas d'attaque, pour éradiquer la menace et reconstruire la muraille. L'action numérique, quant à elle, enrichit, avec l'arme numérique, la palette des options possibles à la

disposition de l'État. L'espace numérique est devenu un espace de confrontation à part entière au même titre que l'espace maritime, terrestre ou aérien. Aujourd'hui, aucune opération militaire ne se conçoit plus sans cette dimension.

Le modèle actuel du Commandement de la cyberdéfense a été construit dans une logique d'économie des forces, de mutualisation des compétences et de concentration des efforts, mais aussi dans une logique de réseau, à l'instar de l'espace matériel et immatériel sur lequel il agit. Il permet une interaction fructueuse entre les acteurs du numérique et assure une maîtrise des actions par l'intermédiaire d'une chaîne fonctionnelle de cyberdéfense. Ce modèle français de cyberdéfense suit l'évolution sociétale actuelle : pour les citoyens utilisateurs de l'espace numérique, le ministère des Armées inspire sécurité et confiance ; il est le lieu privilégié de la création et de l'émulation d'une cyber-résilience. Le Commandement de la cyberdéfense se veut fédérateur au sein des armées, du ministère des Armées, ainsi que porteur d'une logique de renforcement des capacités interministérielles.

La défense de la France et de l'Europe doit s'adapter aux enjeux actuels et futurs du champ de bataille numérique. La supériorité opérationnelle de nos forces armées, c'est-à-dire la capacité à maîtriser des crises, comme la capacité d'entrer en premier sur un théâtre de conflit et à y contraindre un adversaire, passent désormais par la recherche et l'obtention de la supériorité dans l'espace cyber. C'est pourquoi la cyberdéfense au ministère des Armées est pensée dans l'action et construite dans la réalité d'un monde moderne qui a déjà réalisé sa transformation numérique.

L'AUTEURE

Le général de brigade Olivier Bonnet de Paillerets a exercé des responsabilités dans les domaines des opérations et du renseignement. Saint-cyrien, il a servi pendant plusieurs années comme pilote d'hélicoptère. Il a par la suite exercé ses fonctions au cœur de la planification et de la conduite des opérations, mais aussi du renseignement, et a notamment servi dans le Golfe Persique, en ex-Yougoslavie et à Djibouti. Breveté de l'école de guerre en 2001, il a contribué à l'anticipation des nouvelles menaces et des crises au travers d'un parcours varié qui l'a conduit à commander des opérations dans l'espace numérique.

AdobeStock

L'HYPERCONNEXION DES DONNÉES EST UN FACTEUR DU SUCCÈS DES ARMÉES

La numérisation du champ de bataille entraînera l'intégration des données issues des terminaux des théâtres d'opération et des centres de commandement au sein d'un seul référentiel : le *cloud* Défense français. Ce dernier permettra la mutualisation de toutes les ressources informationnelles des trois armées en ayant la capacité de traiter un fort volume de données hétérogènes et fluctuantes ainsi que de leur appliquer des algorithmes décisionnels selon les besoins du commandement. Néanmoins, la résilience de ce système résidera dans le durcissement des processus affectant les data center militaires et en veillant à l'instauration de *cloud* redondants permettant une permanence opérationnelle en cas d'attaque cyber ou affectant les centres névralgiques informatiques.

Résilience des SIC militaires : cloud défense et hyperconnectivité des théâtres d'opérations

Par CLOTILDE BÔMONT

L'hyperconnectivité croissante des champs de bataille a de considérables implications dans la conduite des opérations militaires et conditionne le bon fonctionnement des systèmes d'information et de communication. Le cloud défense actuellement développé par le ministère des Armées est apparu en réponse aux nouveaux enjeux que pose cette digitalisation. Il est un outil de résilience mais soulève de nouveaux enjeux sécuritaires qui, mal appréhendés, pourraient créer des vulnérabilités.

CLOTILDE BÔMONT

Doctorante DGRIS, Chaire de cyberdéfense et de cybersécurité. Saint-Cyr, Sogeti, Thalès (CREC). Université Panthéon-Sorbonne

Hyperconnexion et « datafication » du champ de bataille

Depuis leur apparition il y a quelques décennies, les technologies numériques connaissent un essor continu. Elles sont de plus en plus prégnantes dans les sociétés modernes et la digitalisation concerne aujourd'hui tous les secteurs d'activité. La transformation numérique, passage obligé dans un monde guidé vers et par les avancées techniques, s'est ainsi imposée au monde de la Défense.

La Numérisation de l'espace de bataille (NEB) entraîne l'intégration et le développement des Nouvelles technologies de l'information et de la communication (NTIC) dans l'environnement militaire aux niveaux tactique, opératif et stratégique. Elle provoque logiquement un besoin croissant de connectivité, cette dernière conditionnant le bon fonctionnement des dispositifs cyber militaires. Le maillage des réseaux numériques est alors de plus en plus dense et il en résulte une hyperconnexion du champ de bataille.

Les milieux militaires sont d'importants producteurs et consommateurs de données endogènes et exogènes. Cela se traduit notamment par la multiplication et la diversification des senseurs sur le théâtre des opérations, directement en lien avec les principes de « Surveillance (S) » et de « Reconnaissance (R) » des C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). Le Félin (Fantassin à équipements et liaisons intégrées), qui intègre plusieurs senseurs directement dans les éléments qui le composent, est l'une des meilleures illustrations de ce phénomène au sein de l'Armée française. Il est l'un des éléments du programme SCORPION qui vise à moderniser les groupes tactiques interarmes et prévoit la réunion des Systèmes d'information et de communication (SIC) de combat de l'armée de terre. Le programme SIA (Système d'Information des Armées) a, quant à lui, pour projet le rassemblement des SIC des trois armées, au niveau stratégique comme tactique.

Le but de ces initiatives est d'augmenter l'interopérabilité et la capacité informationnelle des forces grâce à la collecte d'un maximum de données et à l'augmentation du volume des flux d'informations entre toutes les composantes de l'écosystème militaire. Cela conduit à la transcription progressive de l'ensemble de l'environnement de bataille en données numériques. La « datafication » des théâtres d'opérations – dont l'hyperconnexion est à la fois un prérequis et une conséquence – est donc à l'origine d'une massification des données dont la gestion et le traitement deviennent des enjeux à part entière.

Le *cloud* défense français

Afin de correctement traiter ces masses de données et d'assurer la pérennité des SIC, de nouvelles techniques ont vu le jour. L'une des plus récentes et des plus marquantes est la technologie du cloud computing, apparue en réponse aux nouveaux défis que pose la digitalisation. Le « *cloud computing* » ou « *cloud* » est un système de stockage, de traitement et de mutualisation de données numériques.

Devenu incontournable dans la configuration des SI, il ne pouvait être ignoré par l'Armée française. Une gestion locale des SIC ne convient effectivement plus aux débits croissants d'informations et n'est pas adaptée aux nouveaux besoins soulevés par l'interopérabilité (partage des données, diversité des sources…). C'est la raison pour laquelle la DIRISI (Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la Défense) est en charge, depuis 2014, de l'élaboration d'un cloud militaire national français – dit *cloud* défense – qui prévoit la réunion des ressources et des moyens des trois armées (Terre, Mer, Air). L'initiative française, qui doit s'achever fin 2017, repose aujourd'hui sur cinq *datacenters* basés sur le territoire national. Le premier

Ministère des armées

Le Cloud Défense par l'état-major des armées.

centre de données du projet a été inauguré en 2015 ; situé à Rennes, il a coûté 13,5 millions d'euros au ministère.

Pour l'instant, l'usage du *cloud* se limite surtout à l'environnement de travail du personnel et, bien que cela soit imminent, il n'intervient pas encore dans la dimension opérationnelle des missions militaires. Il présente pourtant de sérieux avantages. Dans le cas d'une utilisation au sein des forces armées, ses trois principaux atouts sont la rationalisation par le partage et l'économie d'échelle (effectifs, infrastructures...), un gain d'efficacité opérationnelle, et l'interopérabilité par la mutualisation. Il offre de meilleures capacités techniques grâce à une grande puissance de calcul, augmente la mobilité des forces grâce à son ubiquité et sa facilité d'accès, et améliore la réactivité grâce à la rapidité de la circulation de l'information entre les plateformes. Alors qu'il est en cours d'élaboration, au moins deux dimensions du cloud défense peuvent dorénavant être identifiées :

– l'échelle stratégique, qui gère par exemple les données recueillies par des engins autonomes surveillant des zones sensibles ; c'est le cas des drones qui survolent le Mali et permettent de repérer des mouvements ennemis.

– l'échelle tactique, à travers le développement d'un cloud « de théâtre » ; ce cloud tactique assure, à l'Arrière[1], le stockage des données du théâtre d'opérations et leur traitement au moyen, par exemple, d'algorithmes précis qui sont trop lourds pour des équipements de contact. Ce cloud peut être mobile (composants déplacés dans des caissons aéro-transportables) et est soutenu par un *datacenter* de théâtre.

(1) L'Arrière est la zone située en retrait de la ligne de contact.

(2) . Pour davantage d'informations sur la cyberrésilience, voir de Boisboissel Gérard, 2017, « La Cyberrésilience des systèmes d'armes », DSI cyberguerre : l'heure de l'action, hors-série n°52

Le *cloud*, outil de résilience et d'optimisation des SIC militaires

Le *cloud computing* est également une solution de résilience, entendue en informatique comme la capacité d'un système à continuer de fonctionner en cas d'incident ou de sur-sollicitation et à revenir à son état fonctionnel initial[2].

Le stockage déporté des données et le caractère ubiquitaire du cloud sont les premiers aspects de cette résilience. Dans une configuration basée sur cette technologie, les ressources sont hébergées sur des infrastructures physiquement distantes.

Cela présente deux avantages :

1) Les terminaux sont de simples appareils de consultation ; leur destruction n'a alors qu'un impact limité sur le fonctionnement des SIC puisque les données peuvent être récupérées sur le cloud. Dans le cas d'un cloud de théâtre, un VAB (Véhicule de l'avant blindé) peut par exemple stocker des duplicatas en arrière des zones de combat. Les unités peuvent alors poursuivre leur mission même si l'une d'entre elles est détruite.

2) Tant que le réseau est opérationnel (intranet ou internet), il est théoriquement possible d'accéder aux bases de données en tout temps et en tout point du globe.

La réunion des bases de données, la possibilité d'analyser des données en temps réel et la diversité des appareils connectés au dispositif *cloud* sont d'autres réels atouts pour la résilience des systèmes de communication. La mutualisation des ressources autorise en outre la mise en place d'une gestion centralisée ; cela entraîne une meilleure surveillance des SIC (détection de comportements anormaux) et une plus grande régularité dans leurs mises à jour, ce qui permet de prévenir les défaillances et contribue donc également à leur résilience.

S'il existe des alternatives, le *cloud* computing est le dispositif le plus adapté pour faire face au volume et aux nombreuses variations des flux de données. Grâce à la virtualisation qui permet de faire tourner plusieurs machines virtuelles sur un même serveur physique, les capacités de traitement peuvent y être augmentées et la gestion facilitée. L'efficacité du *cloud* en matière de résilience tient aussi au fait que le déploiement de ces nouvelles capacités ne nécessite pas ou peu de nouveaux matériels ; il ne génère donc pas de coûts supplémentaires importants et sa mise en place est rapide grâce à la standardisation des dispositifs, ce qui limite le temps de latence en cas de pics de demandes. Son élasticité[3] lui permet de répondre à des demandes de calcul et d'analyse soudainement variables, sans interruption du service. Enfin, il permet la centralisation des traitements et donc une sélection des informations transmises dans un contexte opérationnel où la bande passante est limitée.

(3) Voir http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf pour une présentation des caractéristiques du cloud computing.

Assurer la résilience du système cloud lui-même

La résilience des SIC apportée par le cloud suppose la résilience du cloud lui-même. Cela passe par la sécurisation des infrastructures et des réseaux et par la préservation des données qu'il héberge.

Sécuriser les infrastructures et les réseaux

En réunissant dispositifs, applicatifs et données, le *cloud computing* constitue

une nouvelle forme de centralisation dans le monde digital. Les *datacenters*, lieux tangibles de cette concentration, sont les infrastructures maîtresses du système cloud ; leur résilience est essentielle.

Les centres de données sont de grands énergivores et nécessitent une alimentation électrique conséquente, de qualité et continue sans laquelle ils seraient paralysés. En 2015, une partie du réseau électrique belge a été touchée par la foudre ; cela a provoqué une coupure d'électricité au sein d'un datacenter de Google et la perte définitive de quelques données. Une panne dans la gestion des bases de données de l'entreprise Salesforce a eu des conséquences similaires en 2016. Les *datacenters* sont également exposés aux cyberattaques, qu'il s'agisse de DDoS, relativement fréquentes, ou d'attaques ciblées. Si dans le cas d'une panne électrique des générateurs de secours peuvent être utilisés, la répartition des ressources dans plusieurs centres informatiques est la solution la plus fiable pour assurer la résilience du système. Cela permet aussi de le protéger en cas de destruction logicielle ou physique (catastrophe naturelle, attaque ennemie…). Les données présentes sur le *cloud* défense sont ainsi doublées et stockées dans au moins deux lieux différents.

La sécurisation des réseaux est un autre aspect de la résilience du *cloud*. Du fait de leurs fonctions, les datacenters requièrent une connectivité constante aux réseaux. De leur côté, les forces doivent pouvoir accéder aux informations présentes sur le cloud, ce qui peut s'avérer problématique dans des zones mal couvertes. Le *cloud* reste ainsi dépendant de l'hyperconnexion et les réseaux sont des cibles privilégiées de la guerre électronique (brouillage…) et des cyberattaques.

Garantir la disponibilité des données

Il s'agit de l'aptitude à préserver, conserver et sauvegarder des données en cas de défaillance. Le premier enjeu de cet aspect de la résilience est capacitaire. L'un des avantages majeurs du *cloud computing* pour les milieux militaires est effectivement d'assurer la disponibilité d'informations nombreuses et contextualisées. Plusieurs phénomènes sont concomitants à cette qualité : la mutualisation systématique des données, de grandes capacités de traitement et la rapidité des processus. Si le cloud n'est pas correctement dimensionné, il ne peut alors plus assurer ces fonctions et ne garantit plus une bonne gestion des ressources.

Le second enjeu est la lutte contre la perte de données. Pour y faire face, la redondance des systèmes (qu'elle soit froide ou chaude)[4], des sauvegardes et des copies de données peuvent être instaurées. Toutefois, la résilience est efficace

(4) Les équipements critiques sont en général redondés, c'est à dire en deux exemplaires. Cette redondance peut être froide ou chaude. Froide, l'équipement de secours est éteint et il n'est allumé qu'après la perte de l'équipement primaire. Dans le cas de la redondance chaude, l'équipement de secours est en mode veille.

seulement si les sauvegardes sont régulières ou s'il existe une synchronisation. Il convient également d'avoir prévu une hiérarchisation et une structuration des données afin, en cas d'incident, de prioriser la récupération des plus critiques. Une réversibilité des données en cas de corruption -soit la possibilité de revenir à un état antérieur fiable- renforce aussi la résilience du système.

Hyperconnectivité et résilience du cloud : de nouveaux enjeux sécuritaires

L'hyperconnectivité des théâtres d'opérations et la résilience du cloud sont vecteurs d'efficacité, de performance et de fiabilité. Elles sont cependant à l'origine de nouvelles préoccupations d'ordre sécuritaire pour les cercles de Défense.

Sensibilité des données militaires

Afin de préserver les données, des duplicatas sont sauvegardés sur divers serveurs du *cloud*. Des avantages et une certaine sécurité pour les SIC découlent de cette permanence, mais elle génère des risques dans un contexte militaire et stratégique. En effet, la destruction de certaines données sensibles est parfois compliquée. Cela est d'autant plus préoccupant que l'hyperconnexion crée davantage de points d'entrée dans le système.

Le *cloud computing* repose sur les principes de confidentialité, d'authenticité et d'intégrité des données. Dans le cas d'un usage militaire, ces principes ne peuvent souffrir aucun manquement et l'accessibilité au cloud et, in fine, aux données doit être contrôlée. Les méthodes usuelles de résilience, comme celles proposées aux entreprises et qui supposent par exemple le recours à plusieurs fournisseurs, ne peuvent donc être envisagées. Le besoin impérieux de sécurisation des données empêche effectivement que leur gestion soit assurée par des prestataires extérieurs : l'externalisation induit une dépendance auprès des fournisseurs et occasionne une potentielle faille dans la restriction de l'accès aux données. Le caractère ubiquitaire du *cloud* nécessite par ailleurs de mettre en place des modes d'accès multi-facteurs pour ne pas risquer de compromettre l'ensemble des SIC dans l'éventualité où un terminal viendrait à tomber dans des mains ennemies. Un cloisonnement des informations au sein du *cloud* peut également être considéré, en particulier pour faire face aux risques inhérents à l'interopérabilité, à l'interconnexion des SIC militaires et aux points d'accès externes (connexion au réseau internet).

A fonctionnement systémique, risque systémique

Si le *cloud computing* augmente la résilience des SIC militaires, mal élaboré, il peut être une vulnérabilité. Ses nombreux attraits expliquent qu'une partie des capacités informationnelles de l'Armée française migre progressivement vers cette technologie. Les nombreuses interactions entre les composantes d'un même cloud

et les interdépendances qui en découlent obligent à considérer son fonctionnement systémique. Un système est défini comme un ensemble organisé constitué de parties qui interagissent et forment un tout. La protection de chacune de ses composantes est alors impérative, au risque de voir l'ensemble des systèmes compromis. La moindre faille pourrait avoir de graves conséquences puisque les données sont à la base du processus décisionnel, que celui-ci soit humain ou automatique (dans le cas par exemple des engins autonomes ou de tout autre dispositif fonctionnant sur le principe du *machine learning*). La résilience des SIC militaires dépend donc également du degré de sécurisation du *cloud défense*.

L'AUTEURE

Clotilde Bômont est doctorante allocataire de la Direction Générale des Relations Internationales et de la Stratégie (DGRIS). Elle est rattachée à l'Université Panthéon-Sorbonne et à la Chaire de cyberdéfense et de cybersécurité Saint-Cyr, Sogeti, Thalès (CREC), et travaille sur le cloud défense. Elle est titulaire d'un Master en géopolitique de l'Ecole Normale Supérieure et de l'Université Panthéon-Sorbonne.

Adobestock

UN NOUVEL ART DE LA GUERRE FONDÉ SUR L'INTELLIGENCE ARTIFICIELLE

Les SALA, systèmes d'armes létaux autonomes, ouvrent de nouveaux champs opérationnels pour la défense et la sécurité des nations. De la dronification des systèmes d'armes à leur autonomie, liée à la conduction d'actes de guerre par une intelligence artificielle, la problématique essentielle reste de limiter la perte de nos propres ressources humaines et de sanctuariser nos systèmes de commandement tout en écrasant l'appareil militaire de l'adversaire par le déploiement d'un corps de bataille mécanisé, robotisé et soutenu par une architecture logicielle. Le questionnement subsiste sur la prise en compte du niveau d'autonomie de ces armements dans un corpus juridique de la guerre. En effet, un risque majeur réside dans la méthodologie d'apprentissage d'une intelligence artificielle, dans la capacité de reprise de contrôle d'un superviseur humain et dans la difficulté à distinguer une responsabilité dans le déroulement d'une opération.

Vers une dissuasion technologique fondée sur les systèmes d'armes autonomes

Par THIERRY BERTHIER

Au centre des débats stratégiques, économiques et éthiques, l'Intelligence artificielle (IA) s'apprête à transformer l'art de la guerre en introduisant de nouveaux acteurs sur le champ de bataille, les SALA ou systèmes d'armes létaux autonomes. S'ils focalisent les craintes entourant les récents progrès de l'IA, les SALA constituent également les éléments fondateurs d'une nouvelle doctrine militaire qui cherche à exclure les hommes de ses propres forces ou de ses alliés de la zone d'immédiate conflictualité.

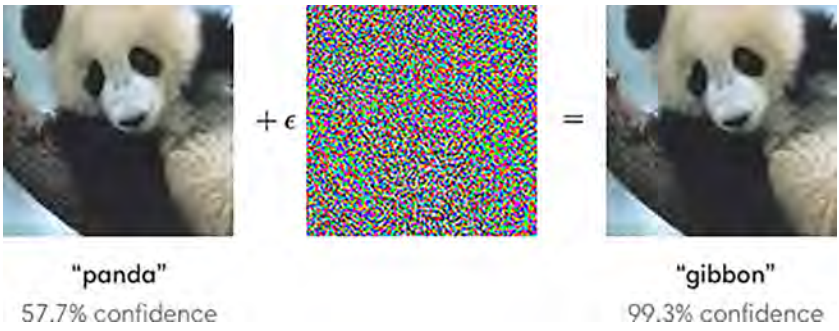
THIERRY BERTHIER

Maître de conférences en mathématiques à l'Université de Limoges (IIRCO. Chaire de Cybersécurité & Cyberdéfense, Saint-Cyr - Thales – Sogeti

L'intelligence artificielle, vecteur de puissance stratégique

L'autonomie des systèmes qui émerge des progrès de l'IA ouvre ainsi de nouveaux champs opérationnels pour la défense et la sécurité des nations. Elle induit une compétition mondiale qui peut être qualifiée aujourd'hui de course à l'IA militaire. L'importance des enjeux stratégiques et géopolitiques de l'IA a fait déclarer, le 4 septembre 2017, au dirigeant russe Vladimir Poutine: « *L'intelligence artificielle est l'avenir, pas seulement de la Russie, mais de toute l'humanité. Elle présente des opportunités colossales, mais également des menaces qui sont difficiles à prévoir. Quiconque devient le leader de ce secteur deviendra le maître du monde* ». Les dirigeants chinois souhaitent que leur nation devienne à très court terme la puissance leader en matière d'IA. Sur un plan militaire, la Chine développe une nouvelle génération de missiles de croisière[1] équipés de systèmes d'apprentissages performants leur donnant, une

(1) http://www.dailystar.com.lb/News/World/2016/Aug-19/367933-china-eyes-artificial-intelligence-for-new-cruise-missiles.ashx



Bruitage de l'image d'un panda reconnue ensuite comme un gibbon par un réseau de neurones.

fois lancés, une forte autonomie. Les États-Unis occupent la pôle position en matière de systèmes d'armes autonomes. La recherche et l'innovation américaine résultent d'un écosystème qui fait coopérer les grands acteurs du numérique mondial (Google, Apple, Facebook, Amazon), les grands laboratoires de recherche nationaux (MIT, Stanford, Berkeley, Caltech,...), et les organismes liés à la Défense (DARPA, laboratoires de l'US AirForce, de l'US Navy...). Il en résulte une alchimie propre à l'innovation qui rend sa diffusion optimale, notamment vers la robotique militaire.

La question de l'autonomie

La première phase de robotisation des systèmes d'armes consiste à faire sortir les équipages des engins pour les relocaliser dans un poste de pilotage extérieur sécurisé tout en conservant le même niveau de capacités opérationnelles. Ce principe de "dronification" des matériels existants fait baisser le risque létal de l'équipage et participe à une "économie du sang" que les opinions publiques de la plupart des nations démocratiques réclament. Un exemple emblématique de dronification de matériel concerne le char de combat russe T14 Armata présenté en 2015. Dans la première version, l'équipage n'est plus situé dans la tourelle totalement automatisée, mais dans une capsule blindée isolée à l'arrière de l'engin. La seconde version déporte l'équipage hors du "char-drone" dans un poste de pilotage délocalisé. Le T14 "dronisé" peut alors s'intégrer au sein d'unités de combat robotisées à l'image des unités russe Platform-M qui entrent en phase d'exploitation. On notera que cette première phase de robotisation maintient un contrôle direct de l'opérateur humain sur la machine qui fonctionne en mode télé-opéré.

La seconde phase de robotisation consiste à introduire un niveau d'autonomie dans les systèmes armés. Cette opération est beaucoup plus complexe que la première. L'intelligence artificielle intervient ainsi dans chaque composante fonctionnelle : déplacement, positionnement, acquisition d'images par différents capteurs, traitement des images, reconnaissance de formes, de contextes et de situations par apprentis-

sage automatisé, décision d'ouvrir le feu. Les premiers systèmes armés semi-autonomes ont fait leur apparition : robot sentinelle SGRA1 Samsung déployé le long de la frontière entre les deux Corées, navire autonome chasseur de sous-marins SeaHunter issu d'un programme de recherche DARPA - US Navy, gamme Kalachnikov de robots armés autonomes présentée en juillet 2017, programme de vol autonome Dassault NEURON. La liste des démonstrateurs de systèmes armés autonomes s'allonge et concerne désormais tous les milieux : terrestre, maritime, aéronautique et spatial. Elle suscite également des craintes et des protestations d'une fraction de la communauté scientifique et de personnalités du numérique. Elon Musk, inventeur visionnaire, dirigeant de Tesla et de SpaceX et grand acteur de l'intelligence artificielle, multiplie les lettres ouvertes demandant l'interdiction pure et simple des systèmes armés autonomes et de l'intelligence artificielle utilisée à des fins militaires. Désireux de "sauver le monde", il en appelle à l'ONU pour voter cette interdiction en 2018[2]. Dans ses différentes lettres ouvertes, Elon Musk n'argumente jamais ses prévisions de dérive malveillante de l'IA qu'il considère *a priori* comme capable d'avoir conscience de ses propres actions (IA forte).

(2) Lettre ouverte d'Elon Musk à l'ONU (du aout 2017) : https://www.dropbox.com/s/g4ijca-q6ivq19d/2017%20Open%20Letter%20to%20the%20United%20Nations%20Convention%20on%20Certain%20Conventional%20Weapons.pdf?dl=0

Cyber-résilience des systèmes armés autonomes

La question de la cybersécurité des systèmes armés autonomes conditionne leur déploiement. L'objet des mises en garde répétées d'Elon Musk oscille d'ailleurs entre le fantasme d'une IA forte, consciente de son action, décidant de se retourner contre son concepteur et des scénarii plus pragmatiques d'IA faibles trompées ou détournées par l'adversaire. Le risque principal associé à la mise en œuvre de systèmes armés autonomes relève en premier lieu de la cyber-insécurité liée à l'apprentissage automatisé. L'autonomie accentue la complexité d'une éventuelle reprise de contrôle du superviseur en cas d'attaque.

Des équipes de recherche[3] ont montré en 2016 et 2017 qu'il était possible de "leurrer" des réseaux de neurones pourtant très performants en reconnaissance d'objet dans une image (vision artificielle). Des attaques par "exemples contradictoires - *Adversarial Attacks on Neural Network*" ont été menées sur plusieurs grandes plateformes d'apprentissage automatisé reposant sur des réseaux de neurones. Ces attaques consistent à perturber l'image d'un objet ou d'un animal bien reconnue par le réseau de neurone. Cette perturbation s'effectue par ajout d'un bruit spécifique sur l'image initiale de sorte que l'image bruitée reste totalement identifiable

(3) Ian J. Goodfellow, Jonathon Shlens & Christian Szegedy "Explaining an harnessing adversarial examples", Conference paper ICLR 2015

par un humain mais entraîne une fausse identification par le réseau de neurones. L'expérience a été réalisée à partir d'images de pandas que le réseau de neurone sait reconnaître avec un haut niveau de fiabilité. Le bruit appliqué sur l'image de panda demeure quasiment invisible pour un humain alors que le réseau de neurones l'identifie de façon presque certaine comme un gibbon.
Le même type d'expérience a été mené avec des panneaux de signalisation : l'image d'un panneau stop, légèrement bruitée, a été perçue par le réseau de neurones comme un panneau de priorité... On imagine facilement les ravages causés par ce type d'attaque sur un véhicule autonome.
Au-delà du volet technique du processus de leurre, les attaques par exemples contradictoires montrent que l'état de l'art de l'autonomie présente aujourd'hui des vulnérabilités qu'il convient de prendre en compte et de résoudre avant tout déploiement massif d'unités armées autonomes. C'est le rythme de résolution de ces vulnérabilités qui déterminera le rythme de mise en production des systèmes armés autonomes.

En conclusion...
Une fois les questions de cyber-résilience résolues et présentant un niveau admissible sur le plan opérationnel, on peut parier sur l'établissement d'une forme de dissuasion technologique fondée sur un équilibre entre les puissances de feu des unités robotisées que les grandes nations pourront mettre en œuvre sur le champ de bataille. Les capacités réciproques de "leurre" des systèmes adverses influenceront le point d'équilibre de cette nouvelle dissuasion. De manière très utopique, on peut imaginer une économie totale de vies humaines dans un conflit du futur où la première armée remportant le combat robotisé serait tacitement considérée par ses adversaires comme celle qui remporte la guerre. La technologie rendrait inutile et irrationnel l'engagement de combattants humains voués à une défaite certaine. La guerre hybride dépasserait ainsi le prix du sang dans un rapport de force relevant purement du niveau d'intelligence artificielle déployé par les belligérants...

L'AUTEUR

Thierry Berthier
. Maître de conférences en mathématiques à l'Université de Limoges (IIRCO)
. Institut International de Recherche sur la Conflictualité .
. Membre de la Chaire de Cybersécurité & Cyberdéfense, Saint-Cyr - Thales – Sogeti; . Membre de l'Institut Fredrik Bull.
. Cofondateur du site d'analyse stratégique EchoRadar et du blog Cyberland.

DOSSIER

Hyperconnexion et résilience

Nouvelles compléxités
nouvelles menaces

Par GILLES HILARY

La complexité du monde, notamment informatique, augmente exponentiellement. Elle est maintenant telle qu'aucun humain ne peut la comprendre dans sa totalité. Une nouvelle vision est nécessaire pour gérer les bouleversements que cela entraîne.

De nouvelles menaces

On estime que quatre-vingt-dix pour cent des données mondiales ont été générées au cours des deux dernières années. Une grande partie de cette expansion est attribuable à l'Internet des objets (IdO), le réseau des périphériques physiques « intelligents » qui recueillent et échangent des données. Outre leur quantité, la nature des données a aussi changé. De nouveaux points de connexion capturent des informations sur des installations industrielles, des machines domestiques et même sur les corps humains puis les transmettent ailleurs où elles sont stockées et analysées pour une meilleure prise de décision. Cela peut naturellement mener à plus de sûreté et de sécurité mais cela crée de nouvelles menaces. Cette complexité est maintenant telle que les approches traditionnelles pour gérer les risques sont en train de devenir inopérantes et même contre-productives.

GILLES HILARY

Professeur - Georgetown University - Chercheur associé CREOGN

Intégrité

Traditionnellement, le risque était qu'un intrus puisse extraire des éléments auxquels il n'est pas censé avoir accès. Une menace émergente concerne la corruption d'informations ou de processus automatisés. Au lieu de voler ces données, l'intrus les manipule. Par exemple, la modification des informations sur les containers dans un réseau informatique portuaire peut faciliter le trafic de drogue. On peut facilement imaginer la modification de résultats cliniques dans une entreprise phar-

maceutique pour la déstabiliser. Le potentiel de l'IdO résidant dans le transfert constant de données entre différents dispositifs, il devient de plus en plus difficile d'en contrôler l'intégrité.

Disponibilité

Des attaques programmées peuvent rendre les données inaccessibles pendant une période plus ou moins longue. Cette menace augmente avec le nombre de points de connexion. Mais, même sans malversation, une plus grande intégration des réseaux peut avoir des conséquences systémiques importantes. Par exemple, une indisponibilité générale des moyens de paiements pourrait avoir des conséquences sanitaires graves en empêchant les paiements urgents (pour les transports médicaux ou même les soins, par exemple). Une catastrophe naturelle pourrait rendre l'évacuation plus difficile en affectant l'utilisation d'ascenseurs ou de feux de circulation intelligents. D'une manière générale, la plus grande interconnexion crée une incertitude vis-à-vis des conséquences d'une dégradation partielle d'un système.

Ubiquité

Les comportements individuels peuvent être suivis avec beaucoup plus de précision grâce à de nouveaux équipements connectés. Des compagnies d'assurance offrent donc maintenant de meilleurs tarifs à ceux qui peuvent démontrer des modes de vie plus sains. Toutefois, cela amène aussi naturellement des menaces sur la vie privée. Elles sont d'autant plus présentes que les données deviennent de plus en plus intégrées. La Chine, par exemple, a lancé un programme pilote pour établir des « *scores de sociabilité* » pour tous les citoyens du pays. Ce partenariat public-privé agrège des donnés aussi disparates que les casiers judiciaires, les achats en ligne et les connections sur les réseaux sociaux. Ce programme permet d'établir des partenariats de confiance (par exemple la location de véhicules sans caution). *A contrario*, il permet aussi de limiter des opérations de la vie courante (l'achat de billets de train par exemple) pour les individus aux scores trop bas. Le projet devrait être étendu aux entreprises dans le futur. On pourrait estimer que de tels développements ont vocation à rester cantonnés dans des pays avec des dispositifs juridiques différents des systèmes occidentaux. Toutefois, des consulats, dont au moins un d'un pays européen, ont déjà commencé à utiliser ce score pour l'attribution de visas.

Changement de culture

L'hyper-connexion nous éloigne d'un monde dominé par le risque dans lequel les menaces sont clairement identifiées et indépendantes les unes des autres. Elle nous entraîne dans un monde d'incertitude où les menaces, mal identifiées, s'intègrent les unes aux autres. Dans un monde de risques, le traitement d'une menace de façon systématique rend le système plus sûr. Par exemple, la standardisation de la vaccination réduit les risques d'épidémie. Dans un monde d'incertitude, cette approche peut déstabiliser les systèmes. Par exemple, l'utilisation de protocoles de sécurité identiques facilite la propagation de virus

informatiques si une faille apparaît.De fait, les approches traditionnelles de traitement du risque se révèlent souvent contre-productives dans un monde interconnecté. Par exemple, l'assurance cyber a un effet déresponsabilisant sur les entreprises. La création de scores de confiance encourage l'interconnections de fichiers. Même le renforcement des outils de sécurité peut se révéler contre-productif. Par exemple, le développement d'identifiants biométriques à la place de mots de passes implique l'utilisation de données permanentes. L'utilisation d'empreintes digitales par des opérateurs mal sécurisés peut conduire à la perte définitive d'une partie importante d'identité individuelle.

Ebauches de solutions

Traçabilité-Responsabilité-Pricing

Une première approche est de s'appuyer sur le triptyque « *Traçabilité-Responsabilité-Pricing* ». Par exemple, des objets ou des composants peuvent avoir des failles intrinsèques ou être incompatibles avec d'autres composants. En cas de problème, il est important de pouvoir remonter à la source rapidement. Toutefois, la traçabilité manuelle devient de plus en plus difficile. Le développement de la technologie dite du « *blockchain* » peut améliorer cet aspect en utilisant des « *contrats intelligents* » (*smart contracts*). Ce sont des protocoles informatiques destinés à faciliter, à vérifier ou à faire respecter l'exécution d'un contrat. Idéalement, ils permettent des clauses auto-exécutoires (avec ou sans validation) qui permettent une efficacité opérationnelle accrue. Par exemple, on peut imaginer que des sous-traitants de rang inférieur ne seront payés que lorsque les donneurs d'ordre auront confirmé l'intégration de divers composants provenant de sources multiples. Une alarme automatique peut être donnée à partir du moment où un composant spécifique devient défectueux. Cette traçabilité augmente les incitations pour les producteurs de produits connectés à offrir une plus grande sûreté (on peut d'ailleurs envisager cette approche dans d'autres domaines tels que la chaîne alimentaire, la production de médicaments ou la prévention de l'emploi d'enfants dans la production de biens de grande consommation). Cependant, la traçabilité sans une bonne attribution de la responsabilité est probablement insuffisante. Or, celle-ci semble être insuffisante à l'heure actuelle. Par exemple, la réaction boursière moyenne, en cas de fuite de données, est proche de zéro pour les grandes entreprises américaines. Dans une large mesure, le risque lié à la confidentialité a été externalisé vers les individus qui en sont victimes plutôt que vers les organisations qui en sont le vecteur. Même si on assiste à l'émergence de législations plus contraignantes (en Californie, par exemple, ou plus récemment en Europe), le pouvoir est actuellement du côté des collecteurs de données. Il est aussi important de donner des incitations aux producteurs de composants pour qu'ils considèrent la sûreté dès la conception des produits plutôt que traiter le problème en bout de chaîne.

Le dernier aspect du triptyque est la mise en place d'un système de prix pour les

différentes menaces. Les marchés sont des instruments généralement efficaces pour agréger des signaux faibles et largement distribués. Par exemple, les marchés prédictifs peuvent jouer un rôle important. Ces outils sont des marchés créés pour négocier des titres virtuels autour d'un événement. Le prix représente l'estimation commune de la probabilité qu'il se réalise. Des organisations aussi diverses que la CIA, Orange ou les studios de cinéma MGM utilisent ou ont utilisé ces outils. Ces marchés ne sont pas la panacée mais ont déjà montré leur utilité. Ils permettent une approche plus systématique et ordonnée d'allocation des ressources.

Une hétérogénéité intelligente

Les chocs se propagent plus facilement dans des systèmes homogènes. Un deuxième axe de réflexion est donc l'introduction d'une hétérogénéité intelligente. Au niveau des sociétés humaines, cela peut vouloir dire refuser l'utilisation d'identifiants uniques pour les différentes activités de la population (comme le numéro de sécurité sociale aux Etats-Unis). Sur le plan de la politique industrielle, cela peut signifier une action vigoureuse contre la formation des monopoles dans le domaine des algorithmes. Dans la gestion opérationnelle, cela peut représenter l'utilisation conjointe de contrôles humains et automatiques. Cette complémentarité homme-machine est apparue clairement en 2005 lors d'un tournoi d'échecs. Des grands maîtres et des machines à hautes performances ont concouru. L'équipe gagnante s'est avérée être constituée de deux joueurs amateurs utilisant des ordinateurs portables relativement faibles. Leur avantage comparatif était de déployer leurs ordinateurs plus efficacement pour prendre les meilleures décisions. Kasparov conclut de ce tournoi que le triptyque « humains faibles + machine + meilleur processus de décision était supérieur à un ordinateur puissant mais isolé et, de façon plus remarquable, supérieur à un individu fort + machine puissante + processus de décision faible.» Dès lors, des coupe-circuits humains deviennent importants comme l'ont démontré les différents « flash crashes » qui ont affecté les places financières.

En conclusion, l'hyper-connexion est désormais une composante majeure de notre environnement. Elle engendre beaucoup de bénéfices mais aussi des menaces nouvelles. Pour contrer ces menaces, l'enjeu n'est pas tant de développer de nouveaux outils ou même de nouvelles méthodologies que de développer une nouvelle culture. Cela nécessite une approche rénovée qui s'appuie sur ces relations plutôt que sur les nœuds du système proprement dits. Cela implique une logique souvent contre-intuitive pour les gestionnaires de risques.

L'AUTEUR

Gilles Hilary est professeur à l'Université de Georgetown. Il est Chercheur Associé au Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN) et Membre Fondateur du Cercle K2 (think tank qui rassemble dans une dimension multi-disciplinaire les experts et professionnels capables d'aider les décideurs publics et privés à anticiper les risques économiques pour leur permettre de développer leurs activités.)

Une convention de
Genève pour le numérique ? Non !

Par ANNE-THIDA NORODOM

En février 2017, lors d'une conférence RSA rassemblant principalement des industriels concernés par la sécurité de l'information, le président de Microsoft, Brad Smith, appelait les États à l'adoption d'une convention de Genève pour le numérique[1]. Si la comparaison établie par Microsoft entre l'assistance apportée par la Croix-Rouge aux civils en cas de conflit armé et celle des entreprises du numérique en cas de cyberattaques est douteuse, cette proposition a au moins le mérite de lancer le débat sur l'utilité d'un instrument international contraignant dans le domaine de la cybersécurité.

(1) Pour la vidéo de l'intervention : https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

ANNE-THIDA NORODOM

Professeur de droit public - Secrétaire générale de la SFDI. Université de Rouen - UFR droit, sciences économiques et gestion

Par analogie avec la quatrième convention de Genève du 12 août 1949, relative à la protection des personnes civiles en temps de guerre, le projet de convention de Genève pour le numérique aurait pour objet, selon Microsoft, de protéger « *les civils sur Internet en temps de paix* ». L'analogie montre rapidement ses limites : la quatrième convention de Genève a vocation à s'appliquer en temps de guerre ; choisir cette dénomination pourrait dès lors prêter à confusion, sauf à considérer que les cyberattaques s'inscrivent nécessairement dans un contexte de conflit armé, voire à les qualifier de cyberconflit, ce qui entraînerait l'application d'un régime juridique particulier. Là n'est pas l'objet de ce projet de convention : il s'agit de protéger les utilisateurs et les acteurs privés d'Internet des cyberattaques provenant des États. Il est ainsi envisagé d'obliger les États à limiter et contrôler le cyberarmement, à s'abstenir de recourir à la cybersurveillance et aux cyberattaques lorsque celles-ci visent des sites sensibles. Cette proposition vient s'ajouter

aux nombreuses réflexions menées sur la gouvernance de l'Internet de la part du Groupe d'experts gouvernementaux (GGE) de l'ONU, de l'OTAN, de l'OSCE[2] ou encore de l'UIT[3] pour ne citer qu'eux. Pourtant elle est loin de convaincre : le projet paraît curieux à de nombreux égards, lacunaire sur certains aspects et finalement non pertinent par rapport aux besoins actuels d'encadrement international de la cybersécurité.

(2) L'Organisation pour la sécurité et la coopération en Europe (OSCE), anciennement Conférence sur la sécurité et la coopération en Europe (CSCE).

(3) L'Union internationale des télécommunications (UIT, en anglais : International Telecommunication Union ou ITU) est l'agence des Nations unies pour le développement spécialisé dans les technologies de l'information et de la communication.

Une proposition curieuse

Le projet de convention de Genève pour le numérique est curieux d'abord parce qu'il relève d'une initiative privée. Rappelons que la place des acteurs privés est prépondérante dans la gouvernance de l'Internet. La plupart des institutions relatives aux aspects techniques de cette gouvernance sont composées d'acteurs privés, les Etats disposant d'une part résiduelle. La réforme de l'ICANN qui visait en principe à favoriser le multilatéralisme a finalement circonscrit l'influence des États à un *Governemental Advisory Committee*. On peut donc légitimement s'étonner qu'un opérateur privé d'Internet demande aux Etats d'adopter un instrument contraignant alors que la tendance générale est plutôt à la réticence des acteurs privés à toute intervention publique dans la régulation de l'Internet. Cette initiative de Microsoft ne dit d'ailleurs rien de la place que les acteurs privés entendent occuper dans le processus d'élaboration de cette convention.

La proposition interpelle également quant au caractère contraignant de la proposition. Il n'existe pas d'instrument contraignant à portée universelle, relatif à la cybersécurité, à l'exception de la convention de Budapest sur la cybercriminalité, adoptée le 23 novembre 2001 et ratifiée par 56 États, dont l'objet est plus restreint que le projet de convention de Genève pour le numérique. La plupart des instruments normatifs régissant la gouvernance de l'Internet relèvent du droit souple : on peut citer notamment la déclaration adoptée à la suite du *NETmundial* de São Paulo en 2014, le manuel de Talinn 2.0 ou les rapports du GGE énonçant un certain nombre de règles relatives à la responsabilisation des États dans le cyberespace. L'UNESCO a ainsi publié en 2015 une étude rassemblant une cinquantaine de déclarations et de cadres relatifs aux principes régissant l'Internet[4].

(4) Disponible en version française sur : http://unesdoc.unesco.org/images/0023/002353/235370f.pdf

Une convention internationale a pour avantage d'assurer une certaine sécurité juridique dans un domaine sensible, la cybersécurité, qui peut le justifier, encore faut-il pouvoir faire aboutir ce processus conventionnel, souvent long et difficile. Or, au regard des discordances existant entre les États et le secteur privé et entre les États eux-mêmes pour l'élaboration de règles non contraignantes, on a du mal à croire qu'il leur sera possible de s'entendre sur un instrument contraignant.

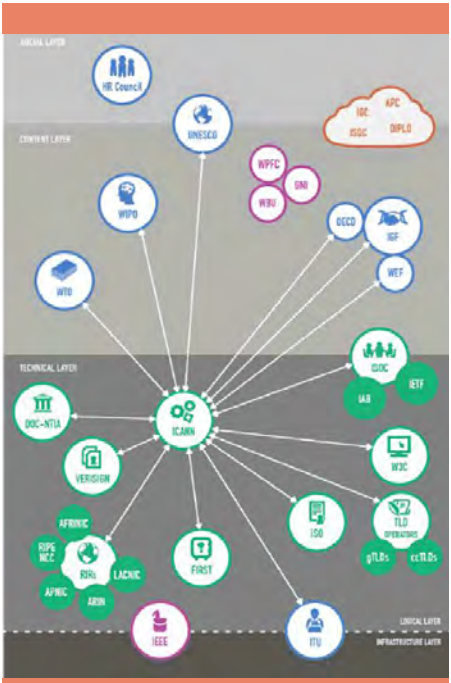


Schéma de l'ICANN montre la segmentation de la gouvernance de l'Internet (Rapport Sénat 2014, pour l'image v. http://www.senat.fr/rap/r13-696-1/r13-696-110.gif

Enfin, mais de manière moins problématique néanmoins, la proposition de Microsoft s'inscrit dans une perspective particulière. Brad Smith propose un instrument dont l'objet est limité à la cybersécurité à l'exclusion de toute autre question relative au fonctionnement d'Internet. Si actuellement la gouvernance institutionnelle de l'Internet est critiquée, cela vient notamment du fait qu'elle est sectorisée : les institutions internationales qui régulent les aspects techniques d'Internet ne sont pas les mêmes que celles qui s'intéressent à la régulation du contenu, les premières n'étant pas composées comme les secondes, si bien que l'ensemble manque de cohérence. Les questions techniques et de contenu sont pourtant liées. Limiter l'objet de cette convention à la cybersécurité constitue un objectif moins ambitieux qu'une convention internationale générale sur le numérique mais sans doute plus facile à atteindre. En ce sens, la proposition faite par Microsoft n'est pas totalement dénuée de sens mais elle reste lacunaire.

Une proposition lacunaire

S'il peut être utile de se pencher sur la question de la codification voire du développement progressif des règles de droit international relatives à la cybersécurité, il est nécessaire de penser correctement son objet. La proposition de convention est centrée sur l'Etat et les cyberattaques d'origine étatique alors que les cyberattaques peuvent également venir d'acteurs non étatiques. La délimitation du champ d'application personnelle de la convention est d'autant plus importante dans le contexte actuel de lutte contre le terrorisme, argument souvent avancé pour justifier le renforcement des législations nationales en matière de cybersurveillance par exemple. Le projet positionne les entreprises et les utilisateurs d'internet uniquement en tant que victimes de ces cyberattaques. Il prévoit ainsi que les États portent assistance au secteur privé pour faire face aux cyberattaques et à leurs conséquences. La situation est en réalité plus complexe : les acteurs non étatiques peuvent être auteurs des cyberattaques tout comme les États peuvent être victimes de celles-ci. Le choix de cette perspective conduit Microsoft à

n'envisager que des obligations à la charge des États. L'idée est juste en ce qu'ils restent les premiers destinataires des règles de droit international. Néanmoins l'implication directe ou indirecte des acteurs privés dans les cyberattaques nécessite de réfléchir aux moyens de responsabiliser leurs comportements. Le Haut-commissaire aux Nations Unies aux droits de l'homme a établi en 2011 des principes directeurs relatifs aux entreprises et aux droits de l'homme (HR/PUB/11/4)[5] qui ne sont pas contraignants mais constituent un exemple utile pour ce type de projet.

(5) http://cop-advanced.org/sites/default/files/docs/RESSOURCES/Droits_de_lHomme/Principesdirecteurs-relatifsauxentreprisesetauxdroitsdelHommes.pdf

La proposition de Convention de Genève du numérique n'intègre pas non plus les aspects institutionnels du problème. Or, se pose actuellement la question de savoir s'il serait nécessaire de créer une organisation internationale dédiée à la cybersécurité ou plus modestement, mais de manière fondamentale, un organe international dont l'objet serait de centraliser la décision d'attribution des cyberattaques. L'objectif serait d'éviter qu'un État puisse unilatéralement attribuer une cyberattaque à un autre État afin de justifier ensuite le recours à la force à son encontre. Ainsi pour être complète cette proposition de convention devrait envisager d'élargir son champ d'application personnelle, de ne pas considérer que les États sont les seuls acteurs de ces cyberattaques et d'intégrer les aspects institutionnels de la réglementation internationale relative à la cybersécurité.

Une proposition non pertinente

Il apparaît finalement que ce projet n'est pas pertinent. Sur le principe, il s'inscrit dans cette tendance qui consiste à proposer l'élaboration de nouvelles règles de droit sous prétexte qu'il existe un nouvel objet. Nombreux ont été les instruments et les institutions internationales rappelant que le droit international s'applique au cyberespace ; les règles de droit international existent donc déjà. En créer de nouvelles semble une solution séduisante *a priori* mais comporte des risques. Le temps du droit n'est pas celui des nouvelles technologies. Il est préférable de conserver et d'appliquer des règles et principes généraux dont l'interprétation permettra une adaptation du droit à des situations particulières plutôt que des règles précises répondant à une évolution technologique propre à un moment spécifique et qui, de fait, pourraient s'avérer rapidement obsolètes.

On l'aura compris, cette proposition de convention internationale ne convainc pas. Son intérêt est néanmoins d'ouvrir le débat et de souligner que, contrairement à l'idée souvent répandue selon laquelle le cyberespace serait l'affaire des acteurs privés pour l'essentiel, ces derniers ont besoin des États, au moins dans le domaine de la cybersécurité. Il importe que les États gardent le contrôle sur cette question. S'ils ne se saisissent pas du sujet, le risque serait alors que la régulation de ce secteur s'opère par les acteurs privés. Pour ne prendre qu'un exemple : quelles seraient la crédibilité et la légitimité des acteurs privés dans l'attribution d'une cyberattaque ? Les conséquences de ce type de décision sont suffisamment graves pour que les Etats s'emparent pleinement et exclusivement de la formation du droit international dans ce domaine.

WannaCry et la diffusion des « zero day exploits »

Par GILLES HILARY

Le vendredi 12 mai 2017, WannaCry a commencé à affecter les ordinateurs dans le monde entier. L'épidémie a commencé en Asie au début de la matinée et s'est répandue dans la journée. Plus de 200 000 ordinateurs auraient été infectés.[1] À titre d'exemple, seize hôpitaux britanniques n'ont pas pu accéder à leurs systèmes. Des entreprises comme *Renault*, *Deutsche Bahn* et *Telefonica* ont également été touchées. Le 14 mai, les effets de WannaCry se sont fait sentir sur tous les continents.

(1) Cependant, l'estimation semble avoir été faite en examinant le nombre de machines qui ont accédé à une URL liée à WannaCry, ce qui a pu conduire à une exagération significative du nombre de machines réellement infectées.

GILLES HILARY

Professeur - Georgetown University - Chercheur associé CREOGN

Que s'est-il passé ?

L'origine de l'incident peut être attribuée à la *National Security Agency* (NSA). L'agence américaine chargée du renseignement *via* l'analyse des signaux électroniques a développé un exploit, EternalBlue, pour profiter d'une vulnérabilité dans les anciennes versions du système d'exploitation de Microsoft. Cette faille de sécurité, MS17-010, qui touchait toutes les versions de Windows, avait déjà été résolue par Microsoft par une mise à jour de sécurité publiée le 14 mars 2017. Toutefois, de nombreux utilisateurs de Windows n'avaient toujours pas installé ce correctif de sécurité lorsque, le 12 mai 2017, le ransonware WannaCry avait utilisé cette faille de sécurité pour se propager. D'autre part, certains logiciels obtenus illégalement ne pouvaient pas télécharger le correctif. EternalBlue permettait aux machines de recevoir des fichiers sur des ports réseaux censés être bloqués. Cet exploit peut désactiver les machines, collecter du renseignement et atteindre d'autres objectifs en exploitant des vulnérabilités non connues des éditeurs de logiciel.

Wannacry a eu un impact limité mais a démontré la capacité de nuisance de groupes inconnus utilisant des produits logiciels connus mais assemblés et implémentés pour une attaque spécifique.

Naturellement, les outils tels que EternalBlue devaient rester confidentiels mais la NSA a connu plusieurs fuites au cours de ces dernières années. Par exemple, le *Federal Bureau of Investigation* (FBI) a arrêté Harold Martin en 2016. Cet employé de Booz Allen Hamilton, un sous-traitant pour la NSA, a été mis en examen pour la détention illégale dans son garage de téraoctets de données et de codes informatiques confidentiels. En avril 2017, les Shadow Brokers, un groupe ayant des liens supposés avec les services de renseignement russes, mirent les outils de la NSA en ligne. Dès lors, toute personne possédant un minimum d'expertise technique pouvait les utiliser pour ses propres besoins.

D'autres logiciels tels que Wannacry et Adylbuzz ont ensuite été développés pour profiter d'EternalBlue. WannaCry est un rançongiciel (*ransomware*), un type de logiciel malveillant qui bloque l'accès aux données de la victime jusqu'à ce qu'une rançon soit payée. Le 12 mai 2017, lorsque tôt le matin WannaCry a commencé à affecter les ordinateurs en Asie, les victimes ont été invitées à payer 300 dollars en bitcoins dans les trois jours (le prix augmentant ensuite à 600 dollars). Le logiciel malveillant (*malware*) s'est ensuite répandu dans le monde entier. Cependant, un expert indépendant britannique a rapidement identifié une faille critique dans le programme : WannaCry essayait systématiquement d'accéder à une URL particulière, qui était directement codée dans le logiciel

malveillant, et se désactivait s'il ne pouvait pas y accéder. Il est possible que cette procédure ait été conçue comme un dispositif de sécurité pour empêcher un examen du logiciel dans des environnements stériles (sandboxes) où l'accès à l'URL aurait été impossible. Dans le cas où le logiciel ne pouvait accéder à cette URL, il se désactivait pour empêcher l'examen du code. Lorsque l'analyste britannique a acheté le nom de domaine (pour moins de 11 dollars), il a réussi à ralentir considérablement la propagation de WannaCry. Le 15 mai, Microsoft a publié un patch de sécurité en urgence qui protégeait les utilisateurs de la version XP de son système d'exploitation. Le 15 mai, l'attaque était essentiellement contenue. Le 18 mai, trois chercheurs français identifièrent un moyen de décrypter les fichiers infectés par WannaCry dans certains cas.

En parallèle du développement de WannaCry, un logiciel distinct baptisé Adylkuzz exploitait aussi la vulnérabilité EternalBlue. Le but de ce deuxième logiciel malveillant était différent de celui de WannaCry. Les crypto-monnaies telles que Bitcoin ou Ether sont des actifs numériques créés par des communautés décentralisées grâce à la mise en œuvre d'algorithmes sur des ordinateurs individuels. Ce processus, appelé « extraction minière » ou « mining », nécessite du temps informatique et de l'électricité et coûte donc cher. Adylkuzz s'est concentré sur l'extraction de Monero, une crypto-monnaie axée sur la protection de la vie privée, dont la capitalisation boursière augmente régulièrement depuis 2014. Cependant, Adylkuzz s'assurait que les bénéfices de l'extraction allaient aux pirates informatiques. Ironiquement, l'une des fonctionnalités d'Adylkuzz était de combler la faille exploitée par EternalBlue. En d'autres termes, Adylkuzz a complètement protégé les machines infectées de WannaCry.

Quelles ont été certaines des conséquences de WannaCry?

WannaCry a été la plus grande attaque de rançongiciel de l'histoire. Son effet a été global avec, selon les estimations, des ordinateurs infectés dans plus de 150 pays en seulement 72 heures. La Russie, l'Ukraine et plus généralement les pays de l'ancienne Union soviétique ont été particulièrement touchés. Les ordinateurs des ministères de l'Intérieur de la Russie et de la Chine ont été infectés. Cependant, les autorités conseillèrent au public de ne pas payer la rançon, ce qui a été largement suivi. Les comptes *Bitcoin* mis en place par les pirates informatiques ont reçu un peu plus de 100 000 dollars et ce montant n'a pas été transféré jusqu'à présent. Si la motivation était financière, WannaCry a été un échec.

Les autres coûts sont difficiles à estimer. Aucune atteinte aux infrastructures critiques et aucun effet durable majeur n'a été signalé. Par exemple, les hôpitaux britanniques ont récupéré des données sau-

vegardées et ont rapidement repris leurs opérations. Malgré l'ampleur de l'attaque, ses effets semblent être relativement peu importants pour l'économie mondiale et même pour les pays les plus touchés.

En réaction à WannaCry et à l'exploitation des actifs de la NSA, les législateurs des États-Unis ont décidé d'examiner la politique concernant la divulgation des *zero day exploits*. La décision de publier une vulnérabilité identifiée par les services de renseignement américains est actuellement prise dans un cadre administratif, le *Vulnerability Equities Process* (VEP), qui suit une approche basée sur une analyse coût-avantage. Maintenir le secret autour des *zero day exploits* préserve un avantage certain pour les services de renseignement ou même les forces de l'ordre mais rend l'écosystème cyber plus vulnérable en préservant des failles de sécurité. Le 17 mai, cinq jours seulement après l'émergence de WannaCry, les législateurs américains ont présenté un projet de loi, le *Patch Act* (*protecting our Ability To Counter Hacking*), pour formaliser le processus de décision et garantir l'examen des « *exploits* » par un conseil indépendant. Si elle était adoptée, la loi Patch créerait un cadre légal et non plus seulement administratif et donc soumis au bon vouloir du pouvoir exécutif.

Qui était derrière WannaCry?

L'attribution de la responsabilité de WannaCry reste incertaine à ce stade et repose largement sur des preuves circonstancielles. WannaCry possède deux composantes, le vecteur d'infection des réseaux (la partie qui installe le logiciel malveillant dans les ordinateurs) et le crypto-verrouilleur (la partie qui crypte les fichiers).

La première composante peut être attribuée directement à la fuite provenant de la NSA. Divers acteurs ont noté des similitudes dans la deuxième composante avec des codes informatiques qui ont été utilisés dans le passé par un groupe baptisé « Lazarus ». On a déjà attribué la responsabilité d'incidents cyber à ce groupe, probablement lié aux services de renseignement nord-coréens. Par exemple, Lazarus a été accusé d'exécuter différentes attaques par déni de service (DDoS) visant des organisations sud-coréennes dès 2009. Une attaque DDoS tente de rendre un service en ligne indisponible en le submergeant par du trafic provenant de sources multiples comme des chapelets d'ordinateurs préalablement infectés. Le groupe a aussi été accusé en 2014 d'avoir organisé le piratage de Sony Pictures qui entraîna la fuite d'un grand volume d'informations confidentielles et de films inédits. En 2016, Lazarus a été accusé d'avoir orchestré des cyberattaques contre trois institutions financières. En particulier, une attaque sophistiquée et intégrée sur la banque centrale du Bangladesh a presque conduit au vol d'un milliard de dollars (les paiements ont été arrêtés après la disparition de 80 millions de dollars).

Ces épisodes ont mis en évidence un degré croissant de sophistication dans le codage, le renseignement et la technique financière. A l'opposé, WannaCry a été mal exécuté avec de nombreuses erreurs de programmation qui ont ralenti sa progression et ont rendu difficiles les paiements en ligne. Cela a conduit certains commentateurs à suggérer que le but de l'attaque était d'embarrasser la NSA plutôt que de collecter de l'argent. Une autre possibilité est que des individus associés à Lazarus aient exécuté l'attaque sans le soutien de l'organisation. L'analyse linguistique suggère que les notes de rançon ont été écrites par des individus parlant une forme de Chinois méridional et non le coréen, Macao étant souvent décrite comme une base majeure d'opérations pour les services nord-coréens.

Que pouvons-nous apprendre de WannaCry?

Sur le plan technologique, WannaCry n'a pas introduit d'innovations dans le codage et la menace de rançongiciel était déjà connue. EternalBlue a déjà été utilisé comme vecteur de pénétration par d'autres logiciels malveillants mais ceux-ci avaient des objectifs plus ciblés. Cependant, nous pouvons faire deux observations.

Premièrement, les ordinateurs infectés exécutaient des versions anciennes de Windows qui ne bénéficient plus du support technique de Microsoft. Par exemple, les médias ont indiqué qu'une étude, menée par la société de cyber-sécurité Citrix, a révélé que 90% des hôpitaux britanniques du NHS utilisait encore Windows XP en 2016. Il peut être tentant d'attribuer cette dépendance à une technologie obsolète, à l'incompétence et à un financement inadéquat. Cependant, il est important de noter que de nombreux dispositifs médicaux utilisent des logiciels spécialisés qui ne peuvent pas migrer facilement vers des systèmes d'exploitation plus récents. Ce problème d'évolution va probablement croître avec le développement des objets connectés qui font partie de systèmes complexes. Beaucoup de ces périphériques ne seront pas conçus avec des fonctionnalités de sécurité robustes et perdront le support technique de leur fabricant après quelques années de service. L'identification rapide des composants défectueux du système et l'installation de correctifs de sécurité qui ne dégradent pas leur interopérabilité vont devenir de plus en plus critiques.

Deuxièmement, WannaCry a fait la une des médias internationaux avec des titres tels que «la catastrophe de rançongiciel de WannaCry expliquée» (un exemple pris sur le site du Washington Post). Les dommages réels ont été plus limités que ce que ces manchettes suggèrent. Le prix des actions des entreprises vendant des produits de cyber-sécurité sophistiqués a augmenté de manière significative bien que les solutions techniques (par exemple, l'installation des correctifs de sécurité, les sau-

vegardes de données) étaient relativement faciles à mettre en œuvre. L'impact perçu de WannaCry a été probablement plus grand que son effet réel. Les problèmes de sécurité informatique sont souvent difficiles à expliquer et peuvent être source d'anxiété pour le grand public. Les entreprises qui vendent des solutions de cyber-sécurité exacerbent naturellement ceci avec des messages alarmistes. Cette anxiété peut être directement exploitée dans le futur par des adversaires. Les grands États ont la capacité d'infliger des dommages très significatifs sur les infrastructures critiques mais de telles attaques engendreraient probablement des ripostes tout aussi dévastatrices. En revanche, il serait difficile pour des états démocratiques de répondre à une campagne cyber qui infligerait des dommages symboliques importants mais des dégâts physiques minimaux, en particulier si cette attaque se déroule sous une fausse signature. Les exemples incluent des attaques à grande échelle visant les médias, comme sur TV5, par exemple, ou sur des panneaux électroniques dans des gares ou des aéroports, couplées à des attaques limitées sur des objectifs importants (par exemple, en ciblant un petit nombre de systèmes de contrôle industriel dans les usines chimiques). Dans des scénarios comme celui-ci, l'impact des événements rares mais graves créerait l'impression de conséquences catastrophiques tandis que les cas bénins à fort impact médiatique auraient une caisse de résonance. Les auteurs de telles attaques pourraient estimer qu'elles restent sous le seuil d'escalade en dépit de leurs conséquences politiques importantes. Dans ce contexte, une communication efficace des autorités est cruciale pour prévenir les réactions irrationnelles du public et pour minimiser les conséquences psychologiques des attaques cyber.

La notation
de cybersécurité

Par GUILLAUME TISSIER

Dans un monde hyperconnecté et largement dérégulé, la notation de cybersécurité va progressivement s'imposer. Qu'il s'agisse de rassurer un consommateur sur le niveau de sécurité d'un objet connecté ou de permettre à une entreprise de s'assurer du niveau de sécurité d'un sous-traitant, voire même d'un pays dans lequel elle souhaite s'implanter, la notation permet de créer la confiance, clé de la transformation numérique.

Entreprises, produits… : pourquoi la notation de cybersécurité va s'imposer

GUILLAUME TISSIER

Directeur général
CEIS

La note traduit et objective une réalité technique, complexe de façon simple. Elle donne la possibilité à une entreprise de se comparer à d'autres, à un consommateur de choisir un produit en fonction de ses options de sécurité, notamment en matière de gestion des données personnelles. La notation concerne aujourd'hui les entreprises, demain les objets connectés et peut-être après-demain les utilisateurs eux-mêmes. Son essor est la meilleure preuve que la cybersécurité est devenue une véritable exigence opérationnelle mais aussi un argument marketing. Attention cependant : cette « *gamification* » complète les certifications techniques mais ne les remplace pas.

Aujourd'hui les entreprises

L'affaire Equifax, du nom de la société de « *risque crédit* » américaine qui a récemment été l'objet d'une fuite massive de données, est un cas d'école par son ampleur : 140 millions de clients potentiellement concernés, - 20,7 % de valeur en bourse en 2 séances, plus de 30 procédures judiciaires, *etc.* mais aussi par sa cause, très basique : une application web non « *patchée* » plus de 2 mois après la sortie de la mise à jour. La gestion de crise de l'entreprise fut catastro-

phique : 6 semaines pour notifier la fuite, un site, lui-même vulnérable, permettant aux utilisateurs de vérifier si leurs données étaient concernées, une tentative d'acheter le silence des consommateurs en échange d'un produit gratuit. Elle éclaire d'un jour nouveau le principe de la notation en matière de cybersécurité. L'agence de notation BitSight, l'un des leaders américains, avait en effet récemment attribué à Equifax un F pour sa sécurité applicative et un D pour sa réactivité en matière de « patching »[1]… La fuite du rapport de notation, qui offre à BitSight un joli coup de pub, confirme donc *post-mortem* l'utilité et l'efficacité de la notation de cybersécurité.

(1) https://securityboulevard.com/2017/09/equifax-rated-f-application-security-breach/

D'abord utilisée en matière financière, la notation des entreprises touche progressivement tous les domaines : responsabilité sociale et environnementale, gestion des ressources humaines, conformité éthique et financière, et aujourd'hui la cybersécurité. Comme la conformité, elle est le fruit de la mondialisation et de la dérégulation. Pour compenser la moindre effectivité des règles nationales et l'absence de réelle régulation supranationale, il s'agit en effet de recréer de la confiance entre les acteurs du marché grâce à des standards de fait, dont l'autorité découle principalement de la reconnaissance du marché. Quand on ajoute à cela l'explosion des risques « cyber »[2], par définition transnationaux, il est logique que la notation finisse par toucher la sphère de la cybersécurité, d'abord aux États-Unis, puis maintenant en Europe. Le domaine suscite même l'engouement du marché et des fonds d'investissement américains si l'on en croit l'importance des levées de fonds réalisées (49 millions de dollars pour BitSight en 2016, 29 millions de dollars pour CyberGRX en 2016) et la croissance rapide des entreprises. Quelques entreprises américaines se partagent aujourd'hui le marché : BitSight, CyberGRX, SecurityScorecard, FICO (société de risque crédit qui a racheté QuadMetrics en 2016), RiskRecon, UpGuard et iTrust (l'entreprise américaine et non la société française du même nom).

(2) Définis au plan assurantiel comme étant les événements informatiques, qu'ils résultent d'une erreur ou d'une malveillance, générant des dommages immatériels sur les actifs de l'organisation.

Comment cela fonctionne-t-il ?

Le principe de la notation en cybersécurité est simple : offrir une solution de notation externe, automatique, indépendante, basée sur un standard de mesure n'utilisant que des informations librement accessibles de l'extérieur de l'entreprise, et donc captables sans que son consentement soit nécessaire. Il s'agit par exemple d'examiner les vulnérabilités des applications web, la réputation des adresses IP de l'entreprise, les configurations DNS, la qualité des certificats SSL et leur configuration, la cadence de mise à jour des serveurs web, les fuites d'informations concernant l'entreprise dans le darkweb. Autant de données

qui permettent d'élaborer et de suivre dans la durée une note représentative du niveau de sécurité de l'organisation. BitSight donne ainsi une note globale allant de 250 à 900 et de A à F pour chacun des points examinés, les indicateurs étant regroupés autour des 5 fonctions de sécurité du référentiel NIST (identifier, protéger, détecter, répondre, remédier).

Quels cas d'usage pour quels bénéfices ?

- L'amélioration et le suivi de ses performances : si la notation ne remplace pas une approche « *par les risques* » couplant audit interne et externe, elle peut constituer un réel apport au plan opérationnel pour suivre et améliorer des performances dans la durée. Mais il faut pour cela que la note soit détaillée et explicable. A un niveau plus stratégique, la notation permettra également au responsable sécurité des systèmes d'information de disposer d'indicateurs utiles pour son COMEX. Quel RSSI n'a pas rêvé un jour de disposer d'éléments de comparaison simples et objectifs avec ses concurrents pour justifier une demande de budget mais aussi valoriser son action ?

- La maîtrise du risque fournisseur : avec l'avènement de l'entreprise étendue et le développement du *cloud computing*, la chaîne de valeur est de plus en plus fragmentée avec tous les risques que cela comporte. Des sous-traitants seraient ainsi impliqués dans 63 % des fuites d'information[3]. En témoignent l'affaire Target et le rôle du prestataire de climatisation. Avec le Règlement européen sur la protection des données personnelles et le principe d'accountability, ce cas d'usage a de beaux jours devant lui et devrait durablement tirer le marché de la notation.

(3) http://www.computerweekly.com/news/2240178104/Bad-outsourcing-decisions-cause-63-of-data-breaches

- L'évaluation des risques en amont de la souscription d'une assurance cyber. Parce qu'il est difficilement modélisable, géographiquement dispersé, qu'il engendre un risque de cumul non linéaire, que les données existantes sont dispersées et surtout non partagées, le cyber risque est difficile à assurer. Disposer d'une note avant toute souscription permettrait ainsi de booster le marché de l'assurance cyber[4].

(4) Voir le livre blanc réalisé à ce sujet par l'association des Alumni de Telecom ParisTech : http://www.amrae.fr/sites/default/files/fichiers_upload/LB_Cyber_assurance_comment_d%C3%A9bloquer_le_march%C3%A9_de_l%27assurance_cyber_en_France_AMRAE_C.PDF

- L'évaluation d'une cible dans un processus de fusion-acquisition.

- L'évaluation du niveau de maturité d'un secteur d'activité.

- L'évaluation du niveau de sécurité d'un pays : BitSight propose ainsi depuis

quelques mois une « note souveraine » élaborée à partir des notes des principales entreprises et agences publiques du pays.

Quelles limites ?

Si les bénéfices de la notation sont bien réels pour l'entreprise, il faut néanmoins être conscient de ses limites. Pour être actionnable, la note doit tout d'abord être élaborée grâce à un processus explicable et transparent en termes de données collectées, de pondération utilisée et d'indicateurs. Une note « boîte noire » ne servirait strictement à rien… Autre limite : la note ne porte, la plupart du temps, que sur des données observables depuis l'extérieur et sur un nombre d'indicateurs limités. Les processus et les comportements ne sont donc pas pris en compte. La note est par ailleurs élaborée principalement à partir de l'analyse des vulnérabilités de l'entreprise. Les menaces, c'est à dire le contexte interne ou externe, ne sont pas ou peu prises en compte. Enfin, la comparaison n'a logiquement de sens et d'utilité qu'entre organisations comparables (secteurs d'activité, surface d'exposition, taille…). La notation doit donc respecter un certain nombre de principes. C'est la raison pour laquelle une quarantaine de grandes entreprises américaines se sont accordées, en juillet 2017, avec les principales agences de notation en cybersécurité sur quelques principes et bonnes pratiques[5]. Parmi ceux-ci : la transparence, la gestion des contentieux *via* un système de médiation, l'indépendance et la confidentialité. La fuite du rapport de BitSight sur Equifax dans les médias, suscite d'ailleurs un débat sur ce dernier point : la note d'une société doit-elle être publique ? Difficile en effet d'imaginer que la note puisse rester confidentielle longtemps compte tenu de la dimension virale du phénomène. Les entreprises bien notées pourraient même y voir un intérêt pour valoriser leur engagement en matière de sécurité, ce qui aurait un effet vertueux sur le niveau de sécurité global. Il n'en demeure pas moins un vrai risque de confidentialité, non sur les notes, mais sur les informations techniques ayant permis d'élaborer la note. Même si ces informations sont librement accessibles, leur concentration en un point unique permettrait à un pirate qui réussirait à y accéder de disposer d'une véritable cartographie des points sensibles d'une entreprise, voire d'un pays.

(5) https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

Quels risques ?

Ce défi technique se double d'un enjeu majeur en termes de souveraineté du fait de l'oligopole américain qui s'est constitué depuis 3 ans. « *Il existe seulement deux puissances capables de détruire l'économie d'un pays : l'aviation américaine sous un tapis de bombes... et Moody's en dégradant sa notation* », disait-on dans les années 70. Certes, la crédibilité des agences financières s'est un peu émoussée avec la crise des subprimes, mais

Thèmes	*Familles de critères*	*Critères*
Sécurité	Qualité du développement	Application des meilleures pratiques en sécurité Stabilité du produit
	Sécurité des données	Programme de *bug bounty* Chiffrement Résistance aux exploits connus Gestion des mots de passe Gouvernance interne de la sécurité Maintien en condition de sécurité dans la durée
	Sécurité personnelle de l'utilisateur	*La société doit aider les utilisateurs en cas d'abus ou harcèlement.*
Gestion de la vie privée	Accès et contrôle des données	Contrôle de l'utilisateur sur ses données
	Rétention des données	Rétention et destruction des données de l'utilisateur
	Collecte des données	*Toutes les données collectées doivent apporter un bénéfice à l'utilisateur* Transparence sur la collecte de données Minimum de données collectées « *Privacy* » par défaut
	Partage de données	Traçabilité des tierces parties
Gouvernance et conformité	Business model	*Transparence quant aux sources de profit de l'entreprise*
	Droits de l'homme et RSE	Gouvernance
	Open innovation	Contribution de l'entreprise à l'innovation
	Open source	Le code est publiquement disponible
	Politique en matière de protection de la vie privée et conditions générales	Accès, clarté et lisibilité des conditions générales Notification des changements en matière de protection de la vie privée et des conditions générales
	Transparence	Requêtes externes en matière de données Politique en matière d'identité (pseudonymat) Notification des fuites de données *Reporting* régulier en matière de transparence (nombre de requêtes externes reçues etc.) Notification des utilisateurs en matière de requêtes externes sur les données
Propriété	Propriété	Interopérabilité (l'entreprise n'interdit pas l'utilisation d'un produit complémentaire) Propriété (lorsque j'achète le logiciel, je suis propriétaire de tous ces composants) Possibilité de revente
	Permanence	Maintien en conditions opérationnelles Processus de clôture de compte
		Transparence quant à la clôture de comptes
	Droit à la réparation	Accessibilité de la réparation (la solution peut être réparée par une entité différente du fabriquant) Pénalités liées à réparation (je ne suis pas pénalisé si je répare mon produit moi-même ou le fait réparer par un tiers)

Liste des points d'évaluation dans le projet Digital Standard.

leur pouvoir normatif reste bien réel. Il en va de même en matière de cybersécurité : la notation pourrait être instrumentalisée, selon des raisons politiques et financières, pour favoriser telle ou telle entreprise dans l'obtention d'un contrat, pour minorer la valeur d'une entreprise dans une opération de fusion-acquisition, pour obérer l'attractivité économique d'un pays, *etc*. Faute d'agences européennes, la notation de cybersécurité pourrait donc devenir demain un nouvel outil au service de la domination commerciale américaine, à l'image du *Foreign Corrupt Practices Act* (FCPA) de 1977 qui s'est progressivement imposé comme la norme universelle en matière de conformité éthique et financière. Mieux vaut donc s'emparer rapidement du sujet et créer un standard de notation

européen pour ne pas dépendre uniquement d'agences américaines. Une nouvelle agence, CyRating, vient d'ailleurs de naître en France avec une ambition résolument européenne.

Demain les objets connectés

Après les entreprises, la notation touche aussi depuis peu le monde des objets connectés. Le constat est simple : ces équipements, qui seront 21 milliards en 2020, collectent, traitent et stockent des données sensibles et surtout interagissent de plus en plus avec leur environnement, physique ou vivant, avec tous les risques que cela peut générer. Le rappel par Chrysler de 1,4 millions de véhicules après la démonstration faite par deux hackers de la prise de contrôle à distance d'une Jeep[6] a sonné comme une prise de conscience : même s'ils ne sont qu'une moitié à accepter de payer un surcoût pour plus de sécurité, les consommateurs sont désormais conscients des enjeux. Selon une étude[7], 72 % des consommateurs connaissaient ainsi le *hacking* de la Jeep. 41 % disaient qu'ils allaient considérer le risque de cybersécurité quand ils achèteraient une voiture. 78 % estimaient que le *hacking* allait se multiplier à court terme. 81 % pensaient qu'il revenait au constructeur automobile de sécuriser les voitures. 64 % voulaient retourner voir le concessionnaire pour faire installer un patch de sécurité. 48 % étaient prêts à payer pour un logiciel destiné à prévenir le piratage. 56 % envisageaient de prendre une assurance spécifique.

(6) https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

(7) Kelley Blue Book Car hacking survey, 2016.

Dans ce contexte, la notation permet au fabricant de valoriser son investissement en cybersécurité en mettant en avant les qualités de son produit. Il peut en outre vendre plus, en proposant différentes options et niveaux de sécurité, en particulier en matière de gestion des données personnelles. Le marché ne lui laissera de toute façon pas le choix... *Consumer Reports*, une association américaine de protection des consommateurs, en collaboration avec plusieurs autres organismes comme *Cyber Independant Testing Lab*, a ainsi proposé en mars 2017 un premier standard ouvert baptisé *Digital standard* pour évaluer, à partir de la documentation disponible et de différents tests de fonctionnement, les solutions logicielles ou matérielles, qu'il s'agisse de webcams, de routeurs, d'enregistreurs vidéo, *etc.*[8] Avec 4 priorités : les produits doivent avoir été construits et développés de façon sécurisée ; ils doivent préserver la vie privée de leurs utilisateurs ; les produits doivent préserver le concept de propriété ; Les fabricants de ces équipements doivent agir de façon éthique.

(8) https://www.thedigitalstandard.org/

Des projets de loi aux Etats-Unis et en Europe sur la certification

Même si elle initie une dynamique vertueuse, cette démarche de notation des produits sous l'angle de la cybersécurité ne saurait cependant remplacer la certification de ces mêmes produits sur la base de référentiels techniques par des tiers agréés. C'est le cas, en particulier, pour les objets ou les fonctions les plus critiques utilisés dans des contextes sensibles. Aux États-Unis, un projet de loi intitulé *Cyber Shield act* vient ainsi d'être déposé au Congrès américain le 30 octobre 2017 par les sénateurs Edward Markey et Ted Lieu[9]. L'objectif est de créer un standard volontaire comportant différents niveaux pour vérifier et labéliser les IoT. On note la même préoccupation en Europe avec le *Cyber Act* proposé par la Commission européenne en septembre 2017[10]. A côté de la certification des produits et composants de sécurité, il s'agit donc de certifier la sécurité de produits génériques, tant pour les entreprises que pour le grand public.

9) https://www.scmagazine.com/lieu-markey-introduce-cyber-shield-act-of-2017-for-iot-devices/article/703633/

(10) http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505290611859&uri=COM:2017:477:FIN

Le défi est cependant immense. La sécurité d'un produit est plus difficile à noter et à certifier que son efficacité énergétique. Elle dépend en effet largement de facteurs externes et évolutifs. Le choix d'un niveau de certification dépendra par exemple largement du contexte d'utilisation de l'objet en question, de l'analyse de risques qui aura été faite et des besoins de sécurité qui en résulteront. Contrairement à ce qui est proposé dans le *Cyber Act* européen, il est ainsi essentiel de prévoir différents niveaux d'exigence selon une triple matrice : nature du produit ou de la fonction considérée, contexte et secteur d'utilisation, type de certification. Quel que soit le référentiel, il ne faut pas confondre une vérification de conformité qui consiste à cocher des cases et une certification technique, de type critères communs pour les produits de sécurité informatique, cette dernière reposant sur une évaluation technique approfondie menée par un laboratoire indépendant. Or, le risque existe aujourd'hui de voir l'Europe, en grande partie sous la pression américaine, adopter des standards de certification qui nivelleraient par le bas les exigences de sécurité et pourraient entamer la compétitivité de ses propres industriels.

Après demain les utilisateurs ?

Après les entreprises et les solutions logicielles ou matérielles, la question de noter les utilisateurs en fonction de leurs comportements en matière d'hygiène informatique pourrait un jour se poser. Un salarié qui cliquerait systématiquement sur des mails de *phishing* dans un cadre professionnel se verrait ainsi contraint par

son employeur de suivre une sensibilisation appropriée. C'est intéressant quand on sait que 30 000 agents sur les 140 000 que compte le ministère de l'Économie et des Finances ont récemment cliqué sur le lien contenu dans des mails signés Emma Bovary ou Jean-Baptiste Poquelin lors d'une campagne de sensibilisation….

L'AUTEUR

Titulaire d'un DESS de droit des affaires internationales, Guillaume Tissier a d'abord été journaliste spécialisé dans les affaires économiques et juridiques, puis consultant chez DATOPS. Il a rejoint la compagnie européenne d'intelligence stratégique - CEIS - en 1997 à la direction de l'activité « Management des Risques et des Crises » où il intervenait notamment dans le cadre de missions de conseil en sécurité de l'information et d'analyse des cyber-risques. Il est aujourd'hui Directeur Général de CEIS.

Mieux vaut guérir
que prévenir

Par DIDIER DANET

L

Le maillon faible

Il est admis depuis longtemps que le maillon faible des systèmes d'information interconnectés se trouve dans l'espace compris entre la chaise et le bureau. De fait, les tests effectués pour vérifier la résilience des systèmes d'information face à des menaces courantes comme le *Phishing* montrent que sous toutes les latitudes et à toutes les époques, les individus « cliquent » assez facilement sur les liens malveillants qui leur sont proposés. Les taux de réussite des attaques varient selon les études mais ils ne semblent pas diminuer significativement au cours du temps. La diffusion généralisée des outils de traitement de l'information et l'utilisation quotidienne qui en est faite par des millions de personnes ne semblent donc pas favoriser la constitution d'un capital d'expérience qui prémunirait les utilisateurs contre les tentatives massives et répétées qui les prennent pour cible. Plus troublant encore, une étude récente menée aux États-Unis montre que les individus demeurent fragiles malgré les modules de formation qui peuvent leur être dispensés. L'étude en question consistait en une série de trois campagnes de courriers électroniques contenant un lien malveillant adressés aux employés d'une organisation à quelques semaines d'intervalle. Entre deux campagnes, certains employés recevaient des modules de formation plus ou moins approfondis. L'hypothèse de recherche consistait à vérifier si les employés, ayant bénéficié de ces modules, devenaient moins sensibles aux attaques par « Phishing », en particulier lorsqu'ils avaient bénéficié des formations plus développées. Or, la conclusion de l'étude est claire : le fait d'avoir bénéficié d'un module de formation, même approfondi, n'influence pas sensiblement le comportement de l'individu. Celui-ci conserve

DIDIER DANET

Chaire Saint-Cyr / SOGETI / Thales Cyber défense et cyber sécurité

L'utilisateur des systèmes d'information est un maillon faible qui doit être formé au signalement des incidents.

© Fotolia

presque inchangée sa propension à se laisser prendre (ou non) à une campagne de *Phishing*. L'étude montre aussi que les individus qui se laissent piéger ne sont pas nécessairement ceux qui n'ont pas eu de formation de même que ceux qui ne cliquent pas sur les liens malveillants ne sont pas nécessairement ceux qui ont été formés. Comment expliquer ces résultats décevants ? Le succès des campagnes de *Phishing* s'explique par trois séries de variables : les caractéristiques fondamentales du cyberespace, les avantages des attaquants, la fragilité des défenseurs.

Internet, le royaume de l'insécurité

Le cyberespace est un domaine où règne désormais l'insécurité. A l'origine, le réseau Internet était parfaitement sûr puisqu'il reliait un petit nombre d'acteurs publics qui se connaissaient et souhaitaient échanger entre eux des fichiers de données. Depuis, le cyberespace est devenu un champ de l'activité humaine dans lequel se traitent des objets de toute nature (images, sons, textes…) en vue d'opérations diverses (achats à distance, opérations bancaires et financières, consultation de bases de données, organisation de flux logistiques…) menées par des acteurs à la fois plus nombreux et plus divers. Il est donc inévitable, compte tenu de la complexité du système et de sa diversité, que des acteurs malhonnêtes s'emploient à s'approprier indûment les richesses qui y circulent ou y sont entreposées. Cet état d'insécurité doit être considéré comme une règle fondamentale et permanente du cyberespace car les mesures qu'il conviendrait de prendre pour retrouver la sécurité des origines seraient dignes de la Corée du Nord : déconnexion du réseau national et du réseau interna-

tional, passage obligé par un opérateur étatique pour s'équiper en ordinateurs et autres matériels permettant d'intervenir dans l'espace numérique, monopole des organismes publics sur la création de sites professionnels ou non professionnels, surveillance administrative des échanges passant par le réseau…

L'asymétrie profite aux attaquants.

Le succès des campagnes de « Phishing » est lié aux caractéristiques des attaquants et des attaques. Les attaquants se montrent de plus en plus habiles dans leur démarche. Le temps est loin de campagnes presque grotesques où, dans une langue pour le moins approximative, une riche veuve proposait au destinataire de son mail de lui verser une partie substantielle de son héritage à charge pour ce dernier de lui fournir les coordonnées bancaires indispensables afin de procéder au virement promis. Les manœuvres malveillantes sont aujourd'hui beaucoup plus subtiles et sophistiquées. Elles déploient des trésors d'ingénierie sociale pour déterminer des profils auxquels seront associées des attaques personnalisées. Les sites servant de support aux attaques sont ainsi des copies parfois parfaites des sites institutionnels ou officiels qui sont utilisés à leur insu. Par ailleurs, les attaques sont d'un coût très limité. Elles peuvent donc être multipliées et menées à grande échelle. Selon la société Kaspersky, 8,3% des utilisateurs de ses produits ont subi une tentative de « Phishing » au cours du seul deuxième trimestre de 2017. Plus de quarante-six millions de tentatives de redirection vers un site compromis auraient été empêchées sur la même période. L'avantage est donc clairement du côté de l'attaquant qui peut renouveler sa manœuvre autant de fois que nécessaire pour obtenir satisfaction.

La cible est en situation de fragilité.

Dernier élément d'explication du succès des campagnes de *Phishing*, les vulnérabilités de l'individu visé. Même s'il est prévenu, voire formé, l'individu est fragile face à des attaques bien menées. Cliquer sur des liens est quasiment devenu un réflexe quotidien dans la vie professionnelle comme dans la vie personnelle. Dans le cas d'anomalies grossières (langage défaillant, expéditeur inconnu, pays d'origine incohérent…), il est probable qu'un niveau d'attention limité soit suffisant pour détecter le piège. Mais, comme nous l'avons vu, ces pièges sont de mieux en mieux conçus et mis en place. Qui pourrait dès lors se dire à l'abri d'un geste malencontreux causé par la fatigue, le nombre élevé de mails à traiter, l'inattention… ? Une très intéressante étude le montre à propos d'un test réalisé dans une académie militaire. Les « clics » malencontreux interviennent surtout lors des phases de consultation intensive des messageries (début de matinée, pause méridienne et début de soirée) où le nombre de mails à traiter est important et où les utilisateurs recourent prioritairement à des objets connectés personnels qui conduisent à une intrication poussée du

monde professionnel (où les consignes de sécurité font l'objet de rappels explicites) et du monde privé où l'utilisateur est le responsable de sa sécurité.

Quelle politique de résilience humaine ?

Le constat dressé ci-dessus doit permettre de poser trois principes fondamentaux d'une politique de cyber résilience au niveau des individus qui utilisent le système et qui en constituent la vulnérabilité principale. Cette politique doit avoir pour devise : « *Mieux vaut guérir que prévenir* ».

Principe n°1 : L'erreur est humaine

Nous l'avons vu, les conditions dans lesquelles se produisent les attaques par *Phishing* sont éminemment favorables aux assaillants et aucune personne visée, quelle que soit sa formation, son grade ou sa position dans l'organisation ne peut se prétendre à l'abri d'un « clic » malencontreux sur un lien malveillant qui déclenchera la contamination de son poste de travail avec un risque d'extension à l'ensemble du réseau dont il fait partie.

Selon les études, les taux de « clic » sur des liens malveillants sont extrêmement variables mais ils sont toujours significativement élevés : 80 % est souvent cité comme une sorte de jauge dans les organisations non préparées. Ce pourcentage pouvait paraître cohérent il y a une dizaine d'années. Il semble aujourd'hui moins élevé comme le montrent les travaux de Jean-Philippe Perrottet. Pour autant, ce taux reste significatif, de l'ordre de 30 à 40 %, au regard du nombre de mails malveillants qui peuvent être envoyés à chaque instant. Toutes les organisations seront donc confrontées à des erreurs humaines et refuser de l'accepter ne peut que rendre hypothétique toute politique de résilience en prise avec la réalité.

Principe n°2 : La sanction est contre-productive

Toute personne qui intègre une organisation du XXIe siècle est amenée à signer une charte informatique qui définit les droits et les devoirs de tout utilisateur d'un système d'information. La valeur juridique de cette charte dépend de ce que l'organisation souhaite en faire. Il peut s'agir d'un simple guide de bonnes pratiques expliquant le fonctionnement du système d'information à l'utilisateur. Elle prend alors la forme d'une note de service.

Le plus souvent, la charte se donne pour mission de fixer les droits et obligations des utilisateurs par rapport à l'institution et aux moyens informatiques qu'elle met à leur disposition. La charte est alors insérée dans une annexe au règlement intérieur et elle prend une tournure beaucoup plus juridique donc, à tort ou à raison, beaucoup plus inquiétante pour l'utilisateur. La charte stipule les règles d'utilisation, les procédures et moyens de contrôle à la disposition de l'employeur, les sanctions disciplinaires en cas de non respect de

ces règles. Lorsqu'un incident se produit, par exemple lorsque l'utilisateur clique sur un lien malveillant intégré dans un courrier électronique personnel ou dans une page visitée en dehors des besoins professionnels, le souvenir d'avoir signé une charte prévoyant des sanctions se ravive et l'utilisateur n'a plus qu'une idée en tête : ne pas se faire prendre. Le mal peut se manifester d'une manière qui implique de signaler l'incident au service *ad hoc* : blocage de la machine, message exigeant une rançon… L'utilisateur n'a pas alors d'autre solution que de faire remonter l'incident. Il va cependant retarder le signalement en espérant que le problème disparaîtra de lui-même ou qu'il trouvera une solution, par exemple auprès de collègues de confiance. Mais, lorsque le problème ne provoque pas ce type de blocage évident, l'utilisateur se contentera de « *faire comme si de rien n'était* », permettant alors à l'attaquant de s'infiltrer en profondeur dans le réseau.

Juridiquement, les sanctions peuvent être justifiées dès lors qu'elles répondent aux principes généraux qui gouvernent les sanctions disciplinaires. Elles satisfont à une logique de rétribution qui associe une faute et la punition ou la sanction qui doit lui correspondre. Elles sont cependant contre-productives au regard de la lutte contre l'attaque puisqu'elles aboutissent à retarder le signalement, à la dissimulation de la séquence des faits ou des actes ayant abouti à la réussite de l'attaque, à retenir l'information qui permettrait de réduire l'impact de l'attaque grâce à une action immédiate et en connaissance de cause.

Principe n°3 : Le signalement est essentiel

Partant du constat que l'attaquant a l'avantage et que toute organisation peut être victime de l'erreur commise par un « clic » malencontreux d'un utilisateur du système d'information, l'objectif prioritaire doit être de traiter le problème le plus rapidement possible pour éviter qu'il ne se répande et ne s'installe en profondeur dans le système. La condition *sine qua non* de réalisation d'un tel objectif est la remontée systématique et immédiate de tout incident ou « presqu'incident » rencontré par les utilisateurs. Or, c'est précisément le point le plus inquiétant des enquêtes qui peuvent être menées. Dans la plupart des cas, le taux de signalement est faible ou très faible. Le résultat est logique dans la mesure où se combinent de nombreux facteurs favorables au non signalement : le sentiment d'avoir commis une faute, la crainte de sanctions qui sont d'ailleurs mal identifiées, l'ignorance des procédures à enclencher… Cette quasi-absence de signalement menace directement la résilience de l'organisation et c'est contre elle qu'il convient de prendre toutes les mesures utiles. Ces mesures peuvent revêtir deux colorations. D'une part, éliminer les freins au signalement, le plus important étant le caractère punitif de la charte informatique. Une mesure simple peut consister à poser un principe de non sanction pour toute faute qui n'est pas intentionnelle.

La logique de rétribution y perd ce que la logique de riposte à l'attaque y gagne. D'autre part, il convient de favoriser la connaissance des mécanismes d'attaque (notamment les signaux qui doivent déclencher une mise en alerte) et des procédures à engager en cas de menace ressentie.

En conclusion, les difficultés rencontrées par les politiques visant à prévenir les comportements malencontreux devraient céder le pas, compte tenu du peu d'effet qu'elles produisent, à celles dont le centre de gravité serait porté sur la riposte aux attaques réussies. En quelque sorte, chercher à renforcer la résilience de l'organisation en inversant le dicton qui vaut généralement pour la santé humaine : « *Guérir plutôt que prévenir !* »

L'AUTEUR

Didier Danet est Maître de conférences (HDR) aux écoles de Saint-Cyr Coëtquidan. Il est directeur du mastère spécialisé en Cyber défense qui prépare les experts de la planification et de la conduite des opérations dans l'espace numérique et de la gestion des crises en cyber défense. Il est également responsable du pôle d'excellence "Mutation des conflits" qui traite notamment de l'adaptation des forces armées aux révolutions technologiques que sont la robotisation du champ de bataille et le développement de l'espace numérique.

Data
Stratégie

Par FRANÇOIS CAZALS

La démocratisation totale de l'Internet, du téléphone mobile et des machines connectées fait du traitement des données un enjeu stratégique pour les organisations, en général, et la gendarmerie nationale, en particulier. Nous analyserons ici ce véritable phénomène des données omniprésentes et comment il est possible de les valoriser pour augmenter la qualité des stratégies et des organisations. Nous envisagerons finalement quelques pistes de réflexion qui s'appliqueraient spécifiquement pour la gendarmerie nationale.

FRANÇOIS CAZALS

Professeur adjoint à HEC Paris - Consultant en stratégie - Lieutenant-colonel (réserve citoyenne) cabinet DGGN

Un monde de données

L'explosion de la production de données dans le monde est un phénomène relativement récent qui commence réellement en 2012. Avec une démocratisation réelle de l'Internet (50 % de personnes connectées au niveau mondial), des médias sociaux (2 milliards d'inscrits actifs sur Facebook), du téléphone mobile (autant de cartes SIM que d'humains sur la planète) et la montée en puissance des objets connectés (50 milliards en 2017), ce phénomène va s'inscrire dans la durée. Cette génération massive et exponentielle de données fonde le phénomène *Big data*.

Évidemment, la possibilité pour chacun d'accéder très facilement à toutes ces données transforme profondément la nature même de nos comportements et crée de nouveaux modèles économiques. Google a déjà théorisé le fait que la consultation d'Internet s'inscrit désormais en amont de tous nos processus de décision, professionnels ou personnels, au travers de son modèle ZMOT (*Zero Moment of Truth*)[1]. Parallèlement, nous voyons également émerger une véritable économie des plateformes numériques,

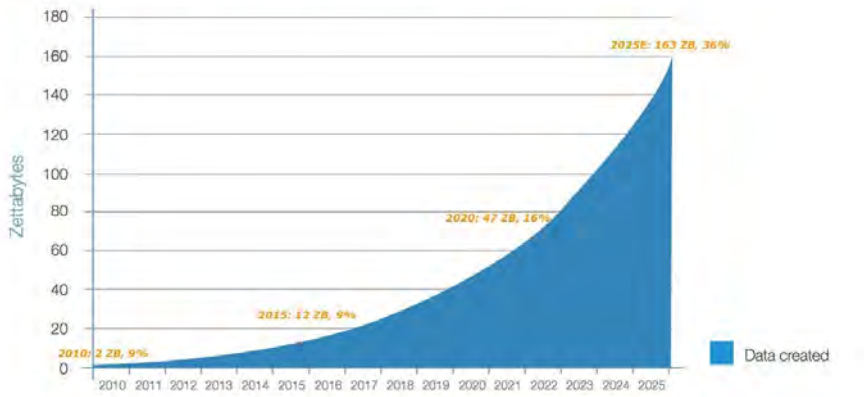
(1) Le ZMOT évoque donc le fait que le consommateur utilise désormais les moteur de recherche, les réseaux sociaux et les mobiles pour obtenir des avis ou informations sur le produit/service pour lequel il a reçu un stimulus. La personne initie cette pratique au moment de la recherche d'informations mais également après que sa décision d'achat ait été prise pour donner à son tour un avis suite à l'utilisation du produit/service.

qui disruptent avec violence les modèles existants. Ainsi, les Uber, AirBnB et autres Netflix modifient profondément les équilibres économiques et sociaux de pans entiers des industries traditionnelles. Cette nouvelle étape du développement de l'économie numérique se traduit de manière spectaculaire dans les valorisations boursières des entreprises internationales. Ainsi, six entreprises du numérique figurent parmi les dix premières capitalisations planétaires. Cette numérisation du monde représente une véritable révolution dont nous ne vivons que les prémices et la convergence des technologies NBIC (nanotechnologies, biotechnologies, technologies de l'information et technologies cognitives) ne va que l'amplifier. Il va de soi que cette nouvelle donne est porteuse autant d'espoirs que de dangers. La croissance des cyberattaques, la criminalité numérique, l'utilisation des technologies par les organisations terroristes et les réseaux cryptés (*DarkNets*, messageries cryptées) posent évidemment de nombreux défis très préoccupants pour la sécurité publique.

Créer de la valeur avec les données

L'enjeu principal pour les organisations est de tirer profit de ces gisements de données et de les valoriser. Mais de quelles

Figure 2. Annual Size of the Global Datasphere



Source: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

source idc via @mikequindazzi

COMPANY: MARKET CAPITALIZATION

RANK	APRIL 2017	Q4 2011	Q4 2006
1	Apple: 741	Exxon Mobil: 406	Exxon Mobil: 447
2	Alphabet: 585	Apple: 376	General Electric: 384
3	Microsoft: 505	PetroChina: 277	Microsoft: 294
4	Amazon: 432	Royal Dutch Shell: 237	Citigroup: 274
5	Facebook: 408	ICBC: 228	Gazprom: 271
6	Berkshire Hathaway: 404	Microsoft: 218	ICBC: 255
7	Exxon Mobil: 344	IBM: 217	Toyota: 241
8	Johnson & Johnson: 330	Chevron: 212	Bank of America: 240
9	JPMorgan Chase: 303	Walmart: 205	Royal Dutch Shell: 226
10	Alibaba Group: 278	China Mobile: 196	BP: 219

Data-driven company

Source: S&P Capital IQ, "Top 10 Companies with Highest Market Capitalization Worldwide."
Note: Market capitalization figures have been rounded and are in $billions.

données parle-t-on ? En effet, celles-ci sont très loin d'être homogènes. Si l'on reprend la métaphore bien connue des données constituant le « *pétrole du XXIe siècle* », celle-ci suggère avec justesse que les données brutes ne sont pas « *raffinées* » et exigent d'être purifiées pour pouvoir être exploitées. De manière plus précise, on distingue trois grandes catégories de données. Les données structurées, ou données opérationnelles, sont générées par les organisations et stockées dans leurs systèmes d'information. Il s'agit essentiellement de données de gestion. Elles ne représentent qu'environ 10% du phénomène *Big data*. La majorité des données sont non-structurées ou semi-structurées (étiquetées par une ou plusieurs variables descriptives) . Il s'agit de textes, de sons, d'images et de vidéos. Ces données sont issues d'Internet (sites Web et messageries), des médias sociaux et des machines connectées.

Valoriser ces données si variées consiste à relever un quintuple défi. Le volume des données, en expansion exponentielle, pose un défi en termes de captation et de stockage. La vitesse de production et de circulation des données amène à devoir également traiter et analyser les données très rapidement. La variété des données (structurées ou brutes, chiffres, textes, images, son, vidéos, …) rend les traitements et analyses nettement plus complexes.

La valeur des données est très difficile à apprécier, au plan de leur qualité intrinsèque et de leur véracité. La visualisation constitue le dernier enjeu critique en termes d'aide à la décision : comment passer de traitements analytiques complexes à des restitutions suffisamment simples et explicites pour les décideurs ?

L'évolution des technologies constitue donc un point clé du développement des Data Stratégies. Aujourd'hui, il est possible et assez économique de capter, stocker et traiter de très grandes masses de données grâce à de nouvelles infrastructures informatiques dites distribuées. Les plus connues des plateformes, disponibles en Open Source, sont Hadoop (stockage distribué) et Apache Spark (traitements distribués) qui peuvent être associées harmonieusement. La puissance des matériels a parallèlement évolué de manière spectaculaire, avec des solutions relativement accessibles au plan financier. À titre d'illustration, le nouveau super calculateur NVIDIA DGX-1, capable

de fournir une puissance de traitement de 170 Tflops (170 000 milliards d'opérations par secondes), coûte moins de 130 000 $.

Concernant les traitements des données proprement dits, un socle très robuste de modèles informatiques, analytiques et mathématiques existe déjà. L'informatique décisionnelle (*Business Intelligence*) permet depuis longtemps d'analyser les données opérationnelles des organisations. De nombreux modèles statistiques explicatifs et prédictifs (*Data Mining*) permettent d'en extraire une véritable valeur opérationnelle.

Les technologies d'apprentissage automatique des ordinateurs (*Machine Learning*) augmentent la puissance et la complexité des traitements. Si elles sont déjà anciennes, un véritable bond conceptuel et technologique a été réalisé dans les années 2010 avec les modèles d'apprentissage profond (*Deep Learning*). Le chercheur français Yann LE CUN, aujourd'hui directeur de l'intelligence artificielle chez Facebook, en a été un des pionniers principaux au niveau mondial. Grâce aux réseaux de neurones artificiels profonds ainsi imaginés, la résolution de traitements très complexes est possible. L'ensemble de ces progrès technologiques permet le développement d'applications d'intelligence artificielle, qui constituera certainement un des piliers principaux des Data Stratégies, à l'avenir.

Concevoir et déployer une Data Stratégie

Cela semble trivial, mais élaborer une Data Stratégie découle évidemment du management stratégique d'une organisation et d'une vision de direction générale. Or, la tentation est grande de considérer que la valorisation des données ne relève que de considérations technologiques, en général, et surtout informatiques, de manière plus spécifique. Ainsi, il est fréquent de rattacher des entités de Data Stratégie (souvent nommées *DataLab*) à la direction des systèmes d'information. Le risque est grand, dans cette configuration, de multiplier les tests (*Proof of Concept* ou POC), sans qu'une ligne directrice n'existe et avec des taux d'échecs importants.

Les organisations les plus avancées adoptent une démarche très différente. Il s'agit, au préalable, de cartographier les données dans les différentes structures managériales, de définir les principes et règles de base d'accès et de traitement et ce en conformité avec les lois et règlements existants. Ces fonctions centrales de gouvernance des données et des traitements sont généralement confiées à une fonction de direction de l'entreprise : la direction du pilotage stratégique des données. Les Anglo-Saxons ont imaginé une dénomination spécifique pour le dirigeant d'une telle structure : *le Chief Data Officer*.

Au-delà des règles et principes liés aux données, la direction générale de l'organisation doit définir un certain nombre d'axes stratégiques applicables aux domaines où les données semblent susceptibles de dégager des gisements de valeur : meilleure connaissance opérationnelle, potentiels d'économie et d'efficience managériale, alertes critiques,

pilotage plus fin et en temps réel des performances… Ces orientations doivent procéder d'une démarche participative avec les grandes directions métiers de l'organisation, qui doivent en constituer les parties prenantes principales au niveau opérationnel. Il est notable de constater que les créations de valeur concernent potentiellement toutes les fonctions régaliennes d'une organisation : direction générale, évidemment, mais également direction du marketing et de la relation client (ou usagers, voire citoyens, dans des contextes publics), direction financière, directions opérationnelles (production, logistique, distribution…) et direction des ressources humaines.

Sur le fondement d'orientations stratégiques claires, au service des métiers de l'organisation, une démarche agile doit être imaginée pour dégager les potentiels de valeur cibles. L'observation des meilleures pratiques actuelles suggère une démarche en trois macro-étapes.

La première phase est celle de l'expérimentation. Elle consiste à développer un prototype de test, pour résoudre une problématique donnée. Une équipe pluridisciplinaire est nécessaire, à ce stade, pour évaluer l'environnement dans sa globalité : experts techniques des données (*Data Engineers*), spécialistes de la modélisation informatique et statistique (*Data Scientists*) et spécialistes métiers. Lorsque le modèle *In Vitro* dans la structure d'étude (DataLab est valide, il convient de le confronter à la réalité *In Vivo* pour vérifier sa robustesse opérationnelle.

La dernière étape n'est pas la moindre puisqu'il s'agit d'intégrer le modèle dans une logique de déploiement industriel. Cette étape cruciale nécessite évidemment une adaptation de certains processus de l'organisation et une véritable intégration au système d'information.

Quelle Data Stratégie pour la gendarmerie nationale ?

L'Institution s'est naturellement engagée dans la voie de la valorisation de ses données, compte tenu des nombreux enjeux qui en découlent.

Le premier enjeu est opérationnel et consiste à pouvoir accéder aux données « Métiers », en temps réel, dans le contexte de mobilité consubstantiel aux missions des gendarmes (prévention, sécurité publique « à chaud »). Il concerne également les unités de commandement (DGGN, régions, groupements, …) pour affiner le pilotage de la performance, et être alerté, en temps réel ou quasi-réel, des informations critiques issues du terrain.

Le second enjeu est économique. Il s'agit d'identifier des gisements de valeur financière et d'optimiser l'efficience opérationnelle, par un management prédictif, la numérisation et l'automatisation de certains processus.

Le troisième enjeu est relationnel. Il intéresse, en temps réel, la surveillance de l'e-réputation de la gendarmerie nationale, notamment en période de crise, et l'orientation de sa communication institutionnelle

grâce, en particulier, à l'analyse des données sémantiques du Web et des médias sociaux.

Ces enjeux ont évidemment été perçus par la DGGN et plusieurs initiatives matérialisent la structuration de la Data Stratégie de l'Arme. Une structure dédiée à l'expérimentation des projets de traitement de données existe déjà : le DataLab. Elle est rattachée à la direction commune des systèmes d'information de la gendarmerie nationale et de la police nationale (ST[SI]2). Plusieurs projets pilotes ont été menés concernant à la fois des sujets liés à la sécurité publique (modèles prédictifs liés à la délinquance) et à l'efficience opérationnelle (maintenance préventive de la flotte automobile, par exemple).

Au niveau de la DGGN, une entité spécifique définit la stratégie numérique de l'institution : la mission numérique. Son impact sur la transformation du modèle opérationnel de la gendarmerie nationale est évident, notamment au travers du déploiement en mobilité des applications Métiers avec NEOGEND, qui constitue « le nouvel assistant du gendarme » ! Une gouvernance stricte des données et des algorithmes est évidemment nécessaire, compte tenu des évolutions juridiques et surtout de l'application dès le mois de mai 2018 du règlement général pour la protection des données. Ces sujets font déjà l'objet de réflexions et d'études, comme le démontre le dernier atelier du centre de recherche de l'EOGN, le 26 septembre 2017 sur le thème des « Algorithmes prédictifs : quels en sont les enjeux éthiques et juridiques ? ».

Ces premières initiatives démontrent l'importance du développement d'une Data Stratégie structurée pour la gendarmerie nationale. Il ne s'agit pourtant que des premières étapes d'un plan plus ambitieux.

Intercepter des signaux faibles de l'environnement, réagir avec agilité et en temps réel à l'imprévu, optimiser les moyens et ressources, valoriser l'image institutionnelle, restituer au citoyen une information utile : voici quelques axes de développement évidents pour renforcer l'efficacité de l'institution et la relation avec les citoyens, à partir d'une stratégie de valorisation de ses données.

Au-delà de la vision stratégique et des contingences technologiques, une véritable transformation de l'organisation et un renforcement des compétences doivent être imaginés. La formation initiale et continue des gendarmes sur les thèmes du numérique et des données constituera certainement un facteur clé de succès de la conduite du changement nécessaire.

L'AUTEUR

François CAZALS est professeur adjoint à HEC Paris. Il y enseigne la stratégie et le marketing et s'est spécialisé sur les sujets des stratégies et de la transformation numériques et les stratégies de valorisation des données grâce à l'intelligence artificielle. Dirigeant d'un cabinet de conseil sur ces thèmes, il est également auteur de nombreux livres et articles, notamment « Stratégies digitales » (De Boeck, 2015). Il intervient régulièrement pour la DGGN et le centre de recherche de l'EOGN, en qualité de lieutenant-colonel (réserve citoyenne) affecté au cabinet du directeur général

La cybersécurité
"marétique", bilan et perspectives

Par MICHEL BENEDETTINI

Jusqu'à un passé assez récent, l'extraordinaire transformation numérique qu'ont connues les activités maritimes et portuaires, appelée "marétique", ne s'était accompagnée d'aucune mesure significative de renforcement de la cybersécurité. Il y a moins de trois ans, un armateur disait même ne pas vouloir consacrer une seconde à ce sujet, tant la menace lui paraissait lointaine et théorique à côté de toutes celles qu'il devait gérer au quotidien. La situation a bien évolué. Où en est-elle ? et que pourrait-on faire de plus ?

MICHEL BENEDETTINI

Vice-Amiral (2S), Compagnie européenne d'intelligence économique - CEIS

Une lente prise de conscience malgré une apathie systémique

Quatre ans après la publication par l'ENISA d'un rapport alarmant sur l'absence totale de prise en compte de la cybersécurité dans le monde maritime, un rapport interne à l'administration françaises, de 2015, alertait les autorités sur l'urgence de lancer une série de mesures concrètes aux niveaux national, européen et international pour éviter que leur mise en œuvre, inévitablement longue, n'arrive que tardivement face à une cybermenace en perpétuelle croissance et aux conséquences potentiellement systémiques.

L'heure était en effet à l'attentisme entre les débats d'experts , pour savoir si le Code international pour la sûreté des navires et des installations portuaires (ISPS) pouvait s'interpréter comme prenant en compte la cybersécurité malgré l'absence totale de toute mesure explicite, et le renvoi de sessions en sessions de tout débat par le comité de sécurité maritime (MSC) de l'Organisation maritime internationale (OMI) au motif que le sujet était complexe et trop transversal pour

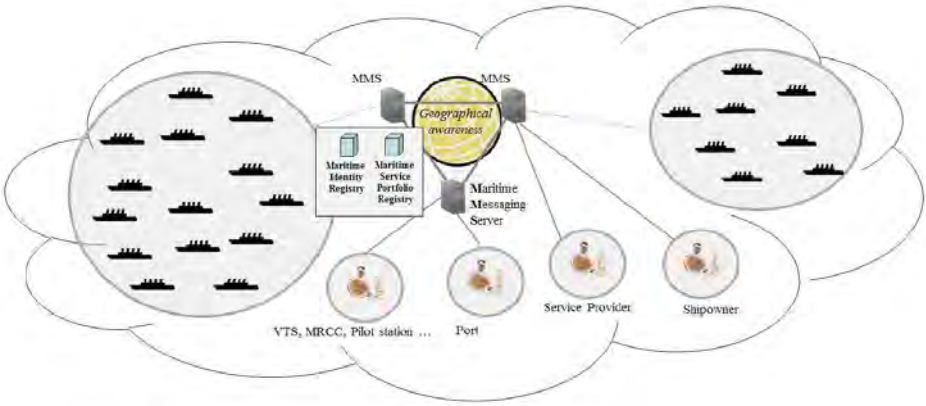
être traité par lui. L'Organisation hydrographique internationale avait bien sécurisé les cartes numériques, plus d'ailleurs pour interdire les copies illégales que résister aux cyberattaques, mais rien n'avait été fait pour sécuriser l'ECDIS, l'équipement servant à les exploiter, par ailleurs de plus en plus relié à la fois aux organes vitaux de propulsion et de manœuvre du navire et au cyberespace extérieur. Dans ses presque 500 pages, la convention internationale STCW fixant les normes minimales de formation des gens de mer restait muette sur la sécurité informatique, même pour une simple sensibilisation des opérateurs embarqués.

Des opérateurs déterminants initient le processus

Au milieu du brouhaha des grandes déclarations d'intention dénuées de tout projet, quelques voix plus concrètes cherchaient à se faire entendre, notamment par le MSC puisque la cybersécurité de secteurs aussi mondialisés et concurrentiels ne peut progresser dans tout son périmètre que par des mesures prises au niveau international s'imposant à tous les États et pavillons. Quelques nations éclairées ont présenté des propositions avec insistance. L'IEC, un comité international de normalisation, a publié une norme prévoyant la mise en place de pare-feux protégeant les navires des menaces du cyberespace, avec une mise en vigueur en 2018 (mieux vaut tard que jamais !). La principale et heureuse surprise est venue de ceux dont on pensait qu'ils s'opposeraient à toute avancée : dès début 2015, quatre associations d'armateurs et d'opérateurs portuaires, dont BIMCO, forte de ses 2100 membres, ont proposé au MSC de rédiger des mesures concrètes, qui, malgré le coût de leur mise en œuvre, pourraient être reprises par l'OMI dans les recommandations internationales.

Une menace se transformant en réalité

Ces armateurs éclairés avaient en effet compris la gravité des impacts qu'ils pourraient subir en cas d'attaques informatiques. L'actualité récente a montré à quel point ils avaient raison. Victime collatérale du logiciel malveillant *NotPetya*, en juin 2017, l'armateur danois Maersk a subi des pertes évaluées de 200 à 300 millions de dollars. Bien d'autres scénarios, paraissant techniquement plausibles, peuvent être redoutés pour leurs graves impacts potentiels sur les activités des "cinq marines" ou sur la sécurité et la sûreté des navires et des ports. Ils ne seraient pas sans incidences sur la vie socio-économique de régions entières, voire sur les vies humaines et sur la sécurité nationale : arrêt ou prise de contrôle à distance d'un navire, d'installations portuaires ou de systèmes de positionnement, favorisant par exemple une attaque physique terroriste, une demande de rançon ou provoquant un accident de mer, l'obstruction d'un port ou d'un canal essentiel sans compter l'explosion, dans une zone peuplée, de navires ou de capacités portuaires remplis de produits dangereux… On peut également envisager une attaque sur les systèmes de gestion et de contrôle du fret maritime, comme celle découverte en 2013 dans le port d'Anvers, qui pourrait permettre des trafics illicites voire l'introduction de terroristes ou d'une "bombe sale" dans des conteneurs.



© Gendarmerie maritime.

L'imbrication des systèmes informatiques embarqués avec les réseaux terrestres et spatiaux oblige les armateurs et les responsables de structures portuaires à prendre des mesures pour assurer une confiance numérique et économique.

De réelles avancées depuis 2015

On peut se réjouir que depuis 2015, de nombreuses démarches, tant internationales qu'européennes ou nationales, font sensiblement progresser la cybersécurité des activités maritimes et portuaires.

Après une longue période d'atonie sur la cybersécurité de la marétique, l'Union européenne et certains de ses États-membres, dont notamment la France, sont devenus forces de proposition tant au MSC que pour la législation communautaire. La directive européenne du 6 juillet 2016 dite "NIS" (*Network and Information Security*), qui édicte de nombreuses dispositions pour atteindre un niveau élevé commun de cybersécurité dans l'Union, s'impose notamment aux activités maritimes et portuaires jugées essentielles. Sa transposition en droit français permettra, avant mai 2018, d'élargir le périmètre d'application d'une bonne part des mesures de cybersécurité déjà en vigueur pour les opérateurs d'importance vitale (OIV). Lors de sa session de juin 2017, le MSC approuvait une courte circulaire officielle de l'OMI recommandant l'application des grands principes de cybersécurité dans toutes les activités maritimes, en s'appuyant sur les normes internationales en vigueur et toutes les bonnes pratiques existantes, citant en particulier les "recommandations pour la cybersécurité à bord des navires" publiées par BIMCO. Quelques semaines plus tard, BIMCO, désormais en partenariat avec près de 20 associations et organisations à vocation maritime, publiait la seconde version de ce guide particulièrement bien conçu.

Au plan national encore, la cybersécurité est désormais à l'ordre du jour des Comités interministériels de la mer, et a fait l'objet d'un long développement dans la Stratégie

nationale de sûreté des espaces maritimes publiée en octobre 2015. La Direction des affaires maritimes et la Direction des services de transport ont chacun publié, en liaison avec l'ANSSI, des instructions et guides pratiques pour faire prendre en compte concrètement la cybersécurité à bord des navires et dans les ports.

L'impulsion est donnée, poursuivons les efforts

Les quelques mesures citées à titre d'illustration dans ce billet, et bien d'autres encore, plus concrètes, prises à tous les niveaux de responsabilité dans les sphères publiques comme privées, montrent que l'impulsion est lancée avec pertinence et détermination. Cela ne doit pas masquer qu'un travail immense, et qui ne sera jamais achevé, reste à faire pour que le monde maritime et portuaire soit protégé à la hauteur des risques et menaces croissants qui pèsent sur la marétique. Les grands principes de la cybersécurité nous indiquent les voies de progrès. Citons en quelques-uns : une prise en compte sur les systèmes dans leur globalité, dès leur conception et tout au long de leur vie ; une architecture résiliente alliée à une défense dynamique et en profondeur, comme Vauban avait su l'organiser dans les fortifications qui protégeaient nos ports dans le passé, s'appuyant sur des mesures de protection et de prévention, sur une veille permettant de détecter les attaques qui ne manqueront pas de déjouer ces mesures, et sur des réactions, aussi planifiées et testées que possible, pour en limiter l'impact et restaurer les fonctions essentielles ; un maintien en condition de sécurité de tous les logiciels pouvant être atteints par une attaque, en particulier ceux des systèmes industriels, les fameux SCADA ; une implication forte de la hiérarchie, qui doit fixer les objectifs de sécurité face aux menaces les plus graves ou les plus probables, donner les moyens financiers, humains et organisationnels permettant de les satisfaire, et accepter tous les risques résiduels que les moyens consentis n'ont pas permis de parer ; enfin faire de la cybersécurité l'affaire de tous, ce qui suppose un énorme effort de sensibilisation et de formation des gens de mer et "de port"…

Voilà qui fait aussi prendre conscience de l'ampleur de la tâche. Il appartient à tous les acteurs des secteurs maritime et portuaire, chacun à leur niveau, de contribuer à relever le défi.

L'AUTEUR

Michel Benedittini a achevé une longue carrière dans la marine nationale avec le grade de vice-amiral. Il a été détaché en 2006 auprès du secrétaire général de la défense et de la sécurité nationale pour exercer les responsabilités de directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information Il a notamment contribué à la définition de la stratégie française de cybersécurité et, en liaison avec les hautes autorités de l'État, les ministères et les principaux opérateurs publics et privés, à la montée en puissance du dispositif national de cybersécurité. Il a ensuite assuré, en 2012 et 2013, la fonction de secrétaire général de la commission du Livre blanc sur la Défense et la sécurité nationale. Il poursuit depuis des travaux de recherche sur la cybersécurité et la cyberdéfense, notamment avec CEIS.

Cybersécurité maritime : le cap est donné !

Par BARNABÉ WATIN-AUGOUARD

Les océans, par leur immensité et la liberté qu'ils procurent, sont propices au développement des activités criminelles les plus diverses. Vecteurs, auteurs ou cibles, les navires et les ports sont abondamment visés par cette criminalité mondialisée. Dans le contexte actuel, les attaques cyber apparaissent bel et bien comme une des principales menaces du futur pour le secteur maritime... Seulement, la menace est bel et bien actuelle !

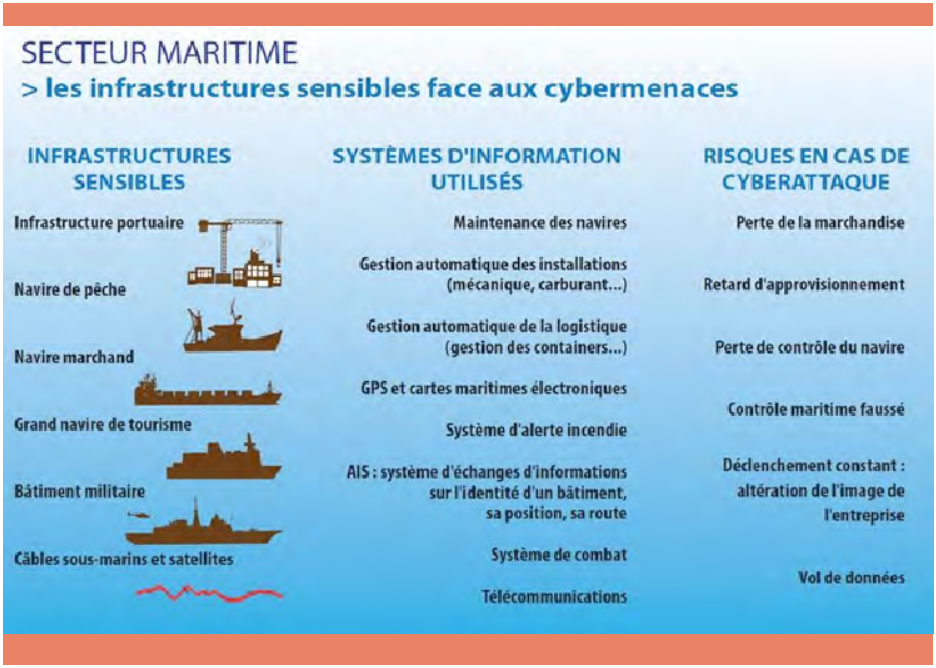
BARNABÉ WATIN-AUGOUARD

Colonel de gendarmerie - Commandant le groupement de gendarmerie maritime de la Manche et de la Mer du Nord

Un certain nombre d'événements touchant le secteur maritime ont ainsi amené les institutions européennes ou internationales ainsi que les autorités françaises à prendre en considération les spécificités du milieu maritime en entraînant dans la réflexion l'ensemble des acteurs, dont la gendarmerie maritime.

Bruits de fond dans l'océan cyber

Si le monde maritime ne semble pas plus particulièrement visé qu'un autre par des cyberattaques, plusieurs facteurs cumulés montrent que le secteur requiert une attention particulière. En effet, il a connu une informatisation galopante (navigation, conduite de la propulsion, gestion de la cargaison, réservation de billets, communications…) sans nécessairement prendre en compte les exigences de cybersécurité. En outre, l'éloignement potentiel d'un navire ou d'une plate-forme, victimes d'une attaque informatique, rend toute mesure corrective extrêmement difficile voire impossible. Enfin, les interconnexions terre-mer, au premier rang desquelles figurent les ports, représentent une véritable vulnérabilité dans un secteur qui irrigue par la suite tout le territoire et dont l'importance pour l'économie nationale n'est plus à démontrer.



© Gendarmerie maritime

En 2010, le ver informatique *Stuxnet* est découvert. S'attaquant aux centrifugeuses d'enrichissement d'uranium iraniennes, il alimente alors la polémique sur ses auteurs au détriment de la question fondamentale : qui peut être impacté par cette attaque en dehors du programme iranien ? En effet, ce malware s'attaque au logiciel de contrôle de SCADA[1] WinCC, développé par Siemens et présent sur de nombreux navires. Le monde maritime n'étant pas touché, cette première mise en alerte se noie alors dans l'océan des attaques informatiques « *qui touchent les autres* ».

(1) Système d'acquisition et de contrôle de données (Supervisory Control And Data Acquisition)

Toutefois, quelques événements plus confidentiels montrent que le secteur n'est pas exempt d'intérêt en la matière. En 2011, le système de gestion des conteneurs du port d'Anvers est piraté par des cybertrafiquants. Cette intrusion leur permet de choisir l'emplacement de la cargaison dans le port afin de faire sortir de grosses quantités de stupéfiants sans risque de contrôle. Dans le même temps, des pirates en océan Indien ou dans le golfe de Guinée choisissent leurs proies grâce à la géolocalisation des navires de commerce accessible à tous sur internet.

Dans les années suivantes, quelques cas intéressants, bien que peu médiatisés, voient le jour. Un pétrolier iranien modifie les données de son système de positionnement et d'identification pour contourner l'embargo américain. Des étudiants d'une

université texane parviennent à détourner le signal GPS d'un navire en mer. Plusieurs systèmes d'information portuaires français sont victimes d'attaques par déni de service. Un hacker parvient à modifier l'assiette d'une plate-forme pétrolière au large de l'Afrique tandis qu'un autre pirate interfère avec une hydrolienne immergée au large d'Ouessant. Plus récemment, la compagnie danoise de MAERSK, leader mondial du shipping, est victime du *ransomware Petya*.

Branle-bas de combat !

Compte tenu de ces événements, on peut se demander quelles actions ont été entreprises en la matière, d'autant que dès 2011, l'agence européenne chargée de la sécurité des réseaux et de l'information publie un rapport[2] alarmiste : « *La sensibilisation à la cybersécurité maritime est actuellement faible, voire inexistante* ».

(2) https://www.enisa.europa.eu/news/enisa-news/prs-in-french/premier-rapport-europeen-sur-la-cyber-securite-maritime/at_download/file

Le cadre européen est particulièrement propice à l'harmonisation des activités portuaires. À cet égard, la directive européenne 2010/65 vise à simplifier la transmission des formalités déclaratives applicables aux navires à l'entrée et à la sortie des ports des États membres. La dématérialisation des procédures implique l'interconnexion des systèmes d'information au sein d'un guichet unique portuaire (GUP). Un tel système attise inévitablement les convoitises des cybercriminels. La sécurisation de ces systèmes d'information est par conséquent un enjeu majeur d'autant que l'Union européenne prévoit d'ici 2020 le déploiement de CISE (*Common Information Sharing Environment*). Cet outil intégrera les systèmes de surveillance maritime existants et permettra à toutes les autorités concernées d'accéder aux informations dont elles ont besoin pour effectuer leurs missions en mer (contrôle des frontières, sécurité et sûreté, contrôle des zones de pêche, douanes, environnement, défense…).

En parallèle, la France s'est mise en ordre de bataille pour répondre au défi de la cybersécurité maritime. La stratégie nationale de sûreté des espaces maritimes[3] de 2015 a clairement pris en compte les cybermenaces, au même titre que la piraterie et le terrorisme, comme un axe de travail majeur pour les années à venir. Le comité interministériel de la mer de la même année a lancé plusieurs actions, avec les armateurs français, pour améliorer la cybersécurité des navires. La direction des affaires maritimes et l'ANSSI ont ainsi procédé à un certain nombre d'audits et d'enquêtes au sein de compagnies maritimes. Ces travaux ont conduit à la publication de trois guides concrets[4] à destination des opérateurs maritimes. Dans le même temps, les services de l'État, des

(3) http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2015/11/strategie_nationale_de_surete_des_espaces_maritimes.pdf

(4) https://omi.delegfrance.org/Cybersecurite-maritime

La gendarmerie maritime contribue à la lutte contre les cybermenaces dans son spectre d'expertise.

© Gendarmerie maritime

élus locaux ou nationaux, les acteurs du secteur et des industriels ont développé leurs échanges et provoqué des réunions d'information pour partager leurs expériences ou leurs préoccupations et développer une culture cyber au sein du monde maritime.

L'ensemble des acteurs français a par ailleurs effectué un véritable travail de lobbying auprès de l'Organisation maritime internationale (OMI) afin qu'elle se saisisse pleinement de la problématique, en partenariat avec d'autres organisations internationales comme l'Organisation hydrographique internationale (qui a défini une norme de sécurité pour la cartographie électronique) ou la Commission électrotechnique internationale (qui recommande la mise en place d'un pare-feu entre le navire et l'extérieur pour 2018). En effet, pour l'heure, la Convention SOLAS[5] ne fait aucune mention explicite à la cybersécurité, même si le code ISPS[6] comporte des dispositions générales dans sa partie facultative. Après quelques sessions plénières effleurant le sujet, l'OMI a émis des directives intérimaires sur la gestion des cyber-risques maritimes[7] en juin 2016. Le sujet est d'autant plus d'actualité sur le plan international, que l'OMI travaille sur un projet de *Maritime Cloud*, l'équivalent au niveau mondial du GUP et du CISE réunis !

(5) Convention sur la sauvegarde de la vie humaine en mer

(6) Code international pour la sûreté des navires et des installations portuaires

(7) http://www.imo.org/fr/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

La gendarmerie maritime embarque pour le cyberespace

Dans ce contexte de développement accéléré de la sphère cyber dans le monde maritime et portuaire, la gendarmerie maritime s'organise pour, d'une part, tirer profit de cette évolution et, d'autre part, prévenir ou traiter à une attaque cyber qui toucherait ce secteur.

En effet, si l'évolution de la marétique[8] présente une face anxiogène au regard des cybermenaces, elle n'en demeure pas moins une révolution bénéfique dans le travail quotidien des gendarmes maritimes. En effet, l'accès dématérialisé à l'ensemble des documents liés à un navire facilite grandement le travail de ciblage et de criblage réalisé par les nouvelles cellules d'évaluation de la menace et de l'analyse de sûreté des groupements. Il permet l'orientation des contrôles de sûreté des navires de commerce faisant escale en France ou la programmation de déploiement d'équipes de protection des navires à passagers. Bon nombre de ces informations sont d'ailleurs partagées avec nos partenaires étrangers via la base MARSEC Web du réseau Aquapol[9]. La finalisation du GUP, de CISE ou la mise en place future du PNR[10] maritime permettra assurément d'accroître l'efficacité de la gendarmerie maritime en la matière. En outre, l'accès aux positions des navires, à l'aide des outils grand public ou plus restreints[11], facilite le suivi des cibles ou éclaire les enquêteurs lors de la survenance d'un accident en mer ou d'une pollution avec des capacités de consultation d'historiques allant jusqu'à 6 mois.

(8) Néologisme associant la mer et le monde numérique

(9) Réseau européen des polices maritimes et fluviales

(10) Passenger Name Record : base de données de réservation des passagers déjà existante dans l'aérien

(11) Avec le système SPATIONAV de la défense, le système IMDatE de l'agence européenne de sécurité maritime ou le système Aquatrack d'Aquapol

Sur le plan des cybermenaces, la gendarmerie maritime s'est pleinement investie dans la prévention. En partenariat avec le ministère de la Transition Écologique et Solidaire, la Marine nationale, le Cluster maritime français, Armateurs de France, l'ENSM[12] et le GICAN[13], la section de recherches de la gendarmerie maritime a ainsi édité un guide sur la préservation des traces et indices en cas d'acte cybermalveillant sur un navire à destination des opérateurs maritimes.

Pour répondre sur le plan judiciaire à un événement cyber, la gendarmerie maritime a formé 3 enquêteurs spécialisés dans les technologies numériques (NTECH) et 15 correspondants NTECH (C-NTECH). Le défi est désormais d'adapter les méthodes de travail utilisées dans ce type d'investigations en mettant en place des protocoles d'analyse propres au monde maritime (SCADA, outils de navigation ou de communication particu-

(12) Avec le système SPATIONAV de la défense, le système IMDatE de l'agence européenne de sécurité maritime ou le système Aquatrack d'Aquapol

(13) École nationale supérieure maritime

(14) Groupement des industries de construction et activités navales

liers…) ou en développant une capacité d'investigation crédible dans des conditions dégradées, notamment en projetant ces enquêteurs en mer.

Prévoir, c'est anticiper

Décembre 2007[14] : une loi de 1825[15] traitant de la piraterie est abrogée. Ce phénomène semble être alors relégué au passé, du moins pour la flotte française. Moins de 4 mois après, le voilier Ponant est attaqué par des pirates au large de la Somalie. En janvier 2011[16], la France réintroduit dans son droit interne la notion de piraterie maritime. Si la loi pénale française n'a jamais été démunie pour réprimer de tels actes, il n'en demeure pas moins que la France a dû attendre le retour en force de la piraterie pour réadapter l'ensemble de son dispositif à cette menace.

(14) Loi n° 2007-1787 du 20 décembre 2007 relative à la simplification du droit

(15) Loi du 10 avril 1825 pour la sûreté de la navigation et du commerce maritime

(16) Loi n° 2011-13 du 5 janvier 2011 relative à la lutte contre la piraterie et à l'exercice des pouvoirs de police de l'État en mer

Gageons que la prise de conscience par les acteurs du monde maritime des enjeux de cybersécurité leur permettra de se préparer à réagir à une attaque lorsqu'elle surviendra. Dans le même temps, espérons que la normalisation internationale dans le domaine cyber prendra moins de temps que pour les mers et les océans : presque quatre siècles séparent le premier traité sur la liberté des mers de Grotius de la Convention de Montego Bay !

L'AUTEUR

Le colonel Barnabé Watin-Augouard, ancien élève de l'école navale, a rejoint la gendarmerie en 2004 après huit années passées dans la Marine nationale. Chargé de mission auprès du Secrétaire général de la Mer depuis sa sortie de l'école de Guerre en 2012, il était notamment chargé des travaux d'élaboration de la stratégie nationale de sûreté des espaces maritimes. Il est maintenant commandant du groupement de gendarmerie maritime de la Manche et de la Mer du Nord.

Analyse économique
des monnaies virtuelles

Par JEAN-LUC DELANGLE

Si le concept des monnaies virtuelles est déjà ancien, il a fallu attendre 2013 pour que le grand public commence à s'y intéresser, avec l'envolée du bitcoin, leur parangon. Conçues pour l'internet, elles symbolisent la modernité d'autant qu'elles reposent sur une innovation majeure, la chaîne de blocs. Cependant, ces monnaies ne sont pas exemptes de risques de toute nature. Il leur faudra ainsi démontrer leur aptitude à établir et à conserver ce qui fonde la valeur d'une monnaie : la confiance.

JEAN-LUC DELANGLE

Contrôleur - Banque de France - Lieutenant-colonel de la réserve citoyenne de la gendarmerie

Quelques préalables sur la monnaie

Définir la monnaie semble trivial tant elle fait partie du quotidien. Comme l'écrivait, voilà quelques décennies, l'économiste américain John Kenneth Galbraith, l'argent concerne tout le monde, celui qui en a comme celui qui n'en a pas. Cependant, il est inutile de feuilleter le Code monétaire et financier : le droit français n'en donne aucune définition.

Tout au plus, le Traité de Maastricht réserve le monopole[1] de l'émission des seuls billets à avoir cours légal[2] à la Banque Centrale Européenne. Ces billets ne peuvent donc être refusés en règlement de dettes libellées en euros. Quoique… il existe des dispositions juridiques stipulant l'obligation de régler par un moyen traçable au-delà d'un seuil déterminé. Le Code monétaire et financier se limite à préciser quel est le pouvoir libératoire[3] des formes monétaires expri-

(1) Article 106 du Traité de Maastricht

(2) Cours légal : les billets ou pièces ayant cours légal ne peuvent être refusés par un créancier ; toutefois, les montants pouvant être réglés de cette façon sont limités par la loi (art L 112-6, D 112-3 et D 112-4 du Code monétaire et financier) ; d'une façon générale, un paiement libellé en euros ne peut être refusé au sein de la zone euro du fait du cours légal.

(3) Pouvoir libératoire : qui éteint une dette.

mées en euros. Pour les économistes, les choses sont mieux cernées et ce, depuis longtemps. En effet, dès le IVe siècle avant notre ère, Aristote dans son « Éthique à Nicomaque » avançait que la monnaie était un instrument d'échange, un étalon de valeur et une réserve. Cette vision a certes suscité de nombreux débats sans véritable remise en cause. Le prix Nobel d'économie Milton Friedman[4] rappelait qu'au final « *n'importe quel bien susceptible de fournir une garantie provisoire sur le pouvoir d'achat général peut faire office de monnaie* ». Il donne de la monnaie la définition suivante[5] : « *est monnaie tout ce qui est accepté de manière constante et générale en échanges de biens et de services, et accepté non pas pour être consommé*[6] *mais en tant que constituant un réservoir temporaire de pouvoir d'achat qui servira à l'acquisition d'autres biens et services* ». Aristote est toujours en filigrane.

(4) Prix Nobel d'économie en 1976

(5) FRIEDMAN M. 1992 « La monnaie et ses pièges » Dunod

(6) La consommation correspond à une destruction ou à un réemploi sous une forme différente ; ainsi une pièce en métal est une monnaie si elle est conservée et réutilisée sous cette même forme, mais cesse de l'être si elle est fondue et réemployée dans un processus productif.

L'histoire de la monnaie est aussi celle de l'innovation pour une plus grande simplification. A l'origine, les échanges fonctionnent sous forme de troc : celui qui a besoin d'un bien l'échange en remettant un autre bien dont il dispose et dont son interlocuteur a besoin, du sel contre des poissons par exemple. On devine ainsi que le troc restreint les échanges. Il repose sur une multiplicité de coïncidences car chaque interlocuteur doit disposer à l'instant de l'échange de ce dont l'autre a besoin : celui qui veut du poisson et dispose de sel doit trouver quelqu'un qui a les poissons et veut du sel. Très vite, est donc apparu le besoin de rompre cette simultanéité, en introduisant une réserve de valeur utilisable ultérieurement. Ainsi, celui qui a du sel peut le céder contre cette réserve de valeur pour la remettre ultérieurement à une 3e personne prête à se défaire de poissons. L'invention de la monnaie, qui n'est rien d'autre que cette réserve de valeur, a grandement facilité le commerce et l'amélioration du niveau de vie.

Dans un premier temps, on a pu se servir de troupeaux. Ainsi le mot « pécuniaire » qui désigne ce qui est relatif à l'argent vient-il du latin « *pecus* » signifiant bétail et le nom de la monnaie indienne, la roupie, provient d'un mot sanskrit ayant la même acception.

On leur a préféré rapidement les métaux, notamment précieux, qui offrent l'avantage d'être pérennes et divisibles. Ces métaux étaient toutefois lourds et présentaient des risques à être conservés. Aussi, l'habitude s'est prise de confier les avoirs monétaires à des orfèvres, lesquels disposaient des équipements de sécurité adaptés de leur profession. Cette remise s'effectuait contre délivrance de bons. Puis, plutôt que de retirer l'or et l'argent déposés pour effectuer

des transactions, il est devenu beaucoup plus simple d'échanger ces bons représentatifs de dépôts et donc garantis par de l'or et l'argent. C'est ainsi que sont apparus les billets de banque en lesquels la confiance initiale repose sur la certitude de pouvoir les convertir en métaux précieux si nécessaire. Il est à noter qu'à partir du moment où la confiance existe, peu de gens cherchent à user de cette faculté de conversion[7].

Il est à souligner que les métaux précieux ont une valeur intrinsèque et s'échangent en tant que tels. De ce fait, jusqu'à la fin du système de Bretton Woods le 15 aout 1971, le système monétaire défini par rapport à l'or n'était rien d'autre qu'un dispositif de troc très élaboré[8], mais au final de plus en plus illusoire car de moins en moins assis sur l'or[9].

La détention de billets de banque a très vite présenté le même risque de sécurité que celui de l'or. Il est apparu que les confier à une banque – ou établissement de crédit, en droit français – était un moindre mal.

(7) La Banque générale, de l'Ecossais John Law illustre l'exemple d'une perte de confiance dans les billets de banque. Créée en 1716 notamment pour financer le déficit de l'Etat, cette banque a émis des billets garantis sur l'or et l'argent. Cependant à partir de 1720, des mouvements de panique bancaire ont conduit un grand nombre de détenteurs de billets à demander la conversion… pour découvrir que les émissions de billets avaient été supérieurs à la masse de métaux précieux, conduisant à la faillite de la banque en 1721. Sous la Révolution Française, les assignats gagés sur les biens nationaux (principalement du patrimoine immobilier confisqué à l'Eglise et aux émigrés) perdront toute valeur à la suite d'émissions bien au-delà de ce qui pouvait être garanti.

(8) Les accords de Bretton Woods ont régi le système monétaire international de 1944 à 1971, en posant la définition stable des monnaies par rapport au dollar (change fixe) et du dollar par rapport à l'or. La fin de ce système a notamment été causée par le trop grand écart de valeur apparu entre l'or « marchandise » sur les marchés de matière première et la valeur officielle de l'or monétaire.

(9) En février 2008, les clients qui se sont précipités aux guichets de la vénérable banque britannique Northern Rock pour retirer leurs économies voulaient des billets et effectuer des virements vers d'autres établissements ; personne n'a cherché à obtenir de l'or.

(10) Le chèque, qui a été longtemps le moyen de paiement préféré des Français, n'est qu'un moyen de faire circuler la monnaie de compte à compte.

Un dépôt bancaire s'est très vite résumé à une ligne d'écriture dans les livres comptables d'une banque : le XXe siècle a connu l'essor de la monnaie scripturale. Les règlements se sont effectués le plus souvent par mouvements d'écritures comptables, par virements de compte à compte[10]. La dématérialisation est allée jusqu'à la monnaie électronique[11], des impulsions numériques, détenues sur des supports *ad hoc* : cartes, clés USB ou disques d'ordinateur.

La monnaie, entre pouvoir régalien et acteurs privés

Les monnaies – et ce très tôt dans l'histoire – ont acquis une spécificité forte : elles sont devenues la marque, le symbole du souverain. Battre monnaie est la caractéristique du pouvoir régalien. Il semble que les premières pièces frappées à l'effigie d'un souverain l'aient été par le roi Alyatte II, qui régna sur la Lydie entre 610 et 560 av. J.-C. Outre l'aspect publicitaire, la marque du souverain apporte également la garantie de la valeur des pièces, en garantissant le poids et la

pureté du métal. A cet égard, soulignons que Philippe le Bel fut considéré comme un roi faux-monnayeur pour avoir rogné les pièces à son effigie afin d'en augmenter artificiellement le nombre.

Soulignons à cet égard que la Banque de France qui a obtenu progressivement au cours du XIXe siècle le privilège de l'émission des billets de banque en France a été une banque privée jusqu'en 1945. Aujourd'hui, tout en étant une institution publique, la loi de 1993 lui assure une large autonomie et une indépendance vis-à-vis du pouvoir politique dans le cadre du système européen des banques centrales (SEBC)[12].

Ce principe régalien suscite toujours d'importants débats chez les économistes. Il a toujours été disputé et, dans les faits, la création monétaire est largement privée. En effet, pour l'essentiel, la monnaie naît à l'occasion de l'octroi d'un crédit bancaire[13], principalement par les banques commerciales, le plus souvent privées[14]. De même, l'or et l'argent n'ont jamais été créés par un État, le souverain se limitant à apporter sa marque.

Le pouvoir régalien s'exprime en fait au travers des actions de contrôle, de réglementation et de régulation de l'activité monétaire. L'estampille du souverain sur les pièces en métal garantissait le poids et la qualité du métal. L'activité bancaire aujourd'hui s'effectue sous la surveillance de la Banque Centrale Européenne. Icelle exécute une mission définie par la loi[15], avec des moyens définis par la loi. Elle est ainsi fort proche d'une autorité administrative indépendante. Cette réglementation garantit des droits aux utilisateurs de la monnaie souveraine.

Cependant fleurissent depuis quelques années[16] des monnaies privées appelées alternatives ou parallèles. Limitées à une aire géographique donnée, rejetant le système financier et la mondialisation chargés de tous les maux, elles ont pour vocation de favoriser la consommation locale, au risque d'ailleurs d'un repli sur soi. Les formes en sont multiples mais elles se caractérisent par une convertibilité[17] limitée :

(11) La directive européenne 2009/110/CE du 16 septembre 2009 définit la monnaie électronique comme une « valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique ».

(12) Le SEBC détermine la politique monétaire de la zone euro, la BCE exécute les décisions du SEBC relayée au niveau national par les banques centrales.

(13) La création monétaire résulte d'un simple jeu d'écriture : lorsqu'un client bénéficie d'un crédit, ses disponibilités sur son compte, comptabilisé au passif du bilan de la banque - et donc son pouvoir d'achat - augmentent ; la contrepartie figure à l'actif dans la rubrique « prêts accordés à la clientèle ».

(14) L'article 101 du Traité de Maastricht et sa transcription dans l'article L 141-3 du CMF interdisent respectivement à la BCE et à la Banque de France de prêter à une entité publique.

(15) Article 108 du Traité de Maastricht et L 141-1 du CMF (pour la Banque de France) ; l'objectif assigné à la BCE par la loi est prioritairement la maîtrise de l'inflation

(16) La plus ancienne encore utilisée est le wir suisse, qui date des années 1930. Le phénomène des monnaies alternatives en France semble démarrer dans les années 90.

(17) La convertibilité est la possibilité donnée à une monnaie d'être changée dans une autre monnaie.

(18) Les entreprises peuvent avoir la possibilité de la convertir en monnaie souveraine moyennant le règlement d'une commission.

(19) Les entreprises peuvent avoir la possibilité de la convertir en monnaie souveraine moyennant le règlement d'une commission.

les particuliers peuvent acheter la devise locale contre euro à un cours fixe mais, devenant « *captifs* », ne peuvent s'en défaire qu'en la dépensant chez les commerçants qui l'acceptent[18]. Fonctionnant de façon proche des monnaies scripturales ou fiduciaires, ces monnaies locales restent émises sous le contrôle des autorités monétaires publiques, des dispositions législatives les régissant[19]. Elles ne sont, au final, qu'un avatar de l'euro et n'entrent pas dans le cadre du présent document.

En revanche, les monnaies virtuelles, appelées encore cryptomonnaies ou cybermonnaies, tout autant privées, relèvent à la fois d'une philosophie et d'un fonctionnement radicalement différents.

Monnaies virtuelles, cryptomonnaies et cybermonnaies

En préalable, il est nécessaire de définir la terminologie, les termes employés mettant l'accent sur des aspects précis du phénomène :

– « *cybermonnaie* » insiste sur son caractère numérique, consubstantiel à l'Internet ; c'est le terme le plus récemment employé, proposé en mai 2017 par le comité d'enrichissement de la langue française,

– « *cryptomonnaie* » met en évidence le procédé informatique reposant sur la cryptographie ; le parangon de ce type de monnaie est le *bitcoin*, historiquement la première créée et aujourd'hui utilisée pour 90 % des échanges utilisant ce type de monnaie,

– « *monnaie virtuelle* » repose sur une vision économique. Cette expression a été utilisée, semble-t-il, pour la première fois par la Banque Centrale Européenne en 2012
pour désigner un instrument numérique utilisé comme une monnaie mais dont les instigateurs - gestionnaires du dispositif voire régulateurs[20]- sont des agents purement privés et dont les utilisateurs constituent *de facto* une communauté.

(20) Dans le présent article, nous adoptons l'acception française du terme « régulation », c'est-à-dire « ce qui permet l'ajustement vers un équilibre » ; à son acception anglo-saxonne, nous préférerons le terme « règlementation ».

Nous retiendrons ici cette dernière expression « *monnaie virtuelle* » en raison du choix fait d'éclairer plus particulièrement les mécanismes économiques induits par les cybermonnaies.

A l'origine, elle désigne les simulacres de monnaie utilisés au sein des métavers, ces sites à la fois jeux de rôles multi-joueurs et réseaux sociaux, dont l'archétype est le *Linden dollar* du site « Second Life ». Les monnaies virtuelles sont cependant très

vite sorties de l'univers ludique. Ainsi, le *Linden dollar* s'achète aujourd'hui contre des devises souveraines.

La seconde vague a été constituée par des dispositifs alliant système de paiement centralisé et monnaie. Par centralisé, il faut entendre l'existence d'un agent, gestionnaire de l'ensemble des comptes ou des portefeuilles, à qui est transmise la totalité des demandes de paiements qu'il effectue en réalisant des virements de comptes à comptes. C'est ainsi qu'ont fonctionné *e-gold*, de 1996 à 2006, et *liberty reserve* de 2006 jusqu'à son démantèlement par les polices de 17 pays en mai 2013. Les sociétés gérant les systèmes de paiement, domiciliées respectivement à St Christophe-et-Nieves et au Costa-Rica, étaient séparées des clients par un ou deux intermédiaires assurant le change. Il y a eu très manifestement la volonté de ne pas tomber sous le coup d'obligations réglementaires. N'étant pas très regardantes sur l'exactitude des identités des détenteurs de portefeuille, leur intérêt pour les blanchisseurs a été rapidement avéré. Si les avocats de *e-gold* ont fait valoir que le droit US est inapplicable à ce type d'instruments privés, la justice en a décidé autrement et a retenu la qualification pénale de blanchiment.

La troisième vague a été celle de la décentralisation, avec le *bitcoin*, inventé en 2009 par un Japonais, Satoshi Nakamoto, vraisemblablement le pseudonyme d'un groupe d'informaticiens sur lequel on sait peu de chose[21]. Ses promoteurs se réclament très ouvertement d'une philosophie libertarienne et ne cachent pas leur méfiance, voire leur

(21) Le microcosme du bitcoin s'agite régulièrement quand quelqu'un croit avoir percé l'identité réelle de Satoshi Nakamoto, sans résultat probant à ce jour.

Nombre de transactions quotidiennes en bitcoin, dans le monte. (L'échelle va de 0 à 400 000).

© blockchain.info

hostilité, envers l'État à qui il est reproché de manipuler la monnaie et de surveiller les citoyens au travers des flux financiers. Son univers est le cyberespace, il ne connaît donc pas de frontières et circule librement sur l'ensemble de la planète.

Il fonctionne en *peer to peer*, c'est à dire en échange direct et décentralisé entre internautes. Autrement dit, le dispositif *bitcoin* est aussi système de paiement (appelé *Bitcoin* avec un B majuscule.) Les transactions financières se dispensent de banques ou de plateformes de compensation, ce qui, selon ses partisans réduit très fortement les coûts de fonctionnement. Afin de vérifier l'existence des bitcoins utilisés lors d'une transaction et de justifier les soldes des porte-monnaies, l'ensemble des participants au système *Bitcoin* dispose du grand livre comptable recensant l'ensemble des transactions depuis la création du bitcoin. Ces transactions restent traçables, mais demeurent anonymes... du moins tant que le détenteur du portefeuille n'est pas identifié.

(22) Sur le plan économique, s'entend ; il existe une communauté gérant l'aspect technique (Cf. infra).

(23) Une banque centrale a pour mission de mettre en œuvre la politique monétaire d'un pays, dont la croissance de la masse monétaire ; elle est souvent également la banque des banques.

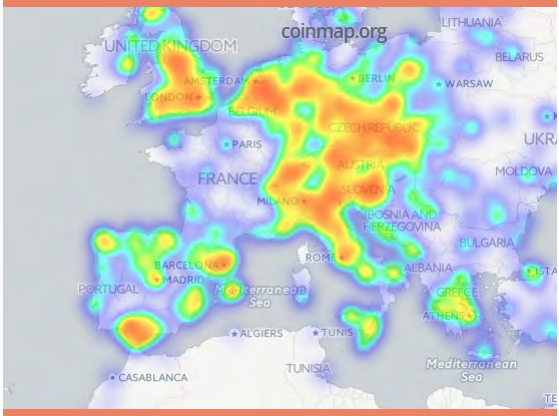
Il n'existe pas non plus d'autorité gérant le dispositif[22], l'équivalent d'une banque centrale[23]. Cette dernière est d'autant plus inutile que la création monétaire est programmée pour atteindre un nombre fini de bitcoins vers 2040 (environ 21 millions, sachant qu'à ce jour il y en a 16,4 millions qui ont été créés). Les *bitcoins* naissent *ex nihilo* selon un rythme décroissant par l'exécution d'un algorithme complexe conduit par des participants au système appelés mineur[24]. Le minage valide les *blockchains* et « *fait jaillir* » de nouveaux bitcoins.

(24) Le minage est donc l'action conduite par les mineurs.

(25) L'assouplissement quantitatif (appelé également « quantitative easing ») consiste à faciliter la création monétaire par la Banque Centrale Européenne ; cette politique mise en place depuis janvier 2015 vise à soutenir l'économie de la zone euro mais a suscité un tollé chez les puristes qui craignent un retour de l'inflation.

Une masse monétaire indépendante de l'action des États est supposée leur éviter la tentation de jouer avec sa valeur. En clair, le *bitcoin* a été pensé comme un instrument apolitique, échappant aux décisions du souverain. Pour exemple, il ne peut ainsi être utilisé, en l'état actuel des choses, pour une politique d'assouplissement quantitatif[25]. Cerise sur le gâteau, le bitcoin est convertible en monnaies souveraines. Des plates-formes fonctionnent tels des marchés financiers pour l'achat ou la vente, le taux de change se formant selon l'offre et la demande (*Cf. infra*). Après des débuts discrets, le bitcoin a connu un réel succès :

Le *bitcoin* est sorti du cercle des initiés à partir de 2012, année au cours de laquelle le nombre de transactions quotidiennes connaît une hausse brutale en atteignant les 25 000. Le cap des 100 000 transactions quotidiennes a été durablement



Carte représentant la densité de commerces acceptant le bitcoin. Plus la densité est importante, plus la teinte tend vers l'orangé.

© https://bitcoin.fr/depenser-ses-bitcoins/

franchi en janvier 2015 pour tendre en 2017 vers 300 000 transactions quotidiennes. Sans être négligeable, la liste des entreprises qui acceptent le *bitcoin* demeure encore restreinte, voire confidentielle[26], au moins en France.

(26) On trouvera à l'adresse https://bitcoin.fr/depenser-ses-bitcoins/ une liste d'entreprises acceptant les règlements en bitcoin.

La carte ci-dessus montre que le phénomène *bitcoin* touche, en Europe, plutôt la Grande Bretagne et les pays de l'Est. A l'inverse, la France est peu concernée. On y trouve des pionniers de la monnaie virtuelle dans tous les secteurs d'activité, mais peu nombreux. Des instruments de paiement existent toutefois. Ainsi, la société Visa propose des cartes de paiement en bitcoins fonctionnant à l'identique de n'importe quelle carte de paiement. Aussi, le succès de cette monnaie virtuelle a attiré de nouvelles offres similaires. Plusieurs centaines de monnaies ont été créées sur ce modèle depuis 2009, dont un bon nombre a déjà disparu ! La suprématie du bitcoin n'a jamais été remise en cause à ce jour.

Avers et revers économiques de la monnaie virtuelle

Les promoteurs du bitcoin mettent en avant deux avantages majeurs :

– le faible coût, la rapidité des transactions et la possibilité de joindre les paiements à la réalisation de conditions ;

(27) L'inflation se définit comme la hausse généralisée et continue des prix.

– l'absence d'inflation[27].

Ces avantages avancés sont contrebalancés par des risques de nature économique ou par la facilitation de comportements déviants qui, à terme, obéreront la confiance que l'on peut placer dans le bitcoin, la pire des choses qui puisse arriver à une monnaie. Les banques centrales n'ont d'ailleurs pas manqué d'alerter à ce sujet.

Certes, une transaction effectuée en *bitcoin* a l'avantage d'être rapide, en quelques minutes, les délais exigés par les banques[28] se chiffrant en heures ou en jours. Le coût de la transaction est lui-même très modeste, l'équivalent de quelques centimes d'euros, quelle que soit la

(28) Les banques s'intéressent désormais à la technologie des chaines de bloc, entre autre pour améliorer la rapidité des flux.

destination. En revanche, les coûts de change du bitcoin en une monnaie souveraine et réciproquement sont souvent élevés, jusqu'à plus de 10 % du montant de l'opération[29] et réduisent l'intérêt économique de l'opération.

(29) Le spectre des frais de change est dans les faits extrêmement variables, de 1 % à 15 %, sans certitude d'exhaustivité.

Ceci dit, la rapidité des paiements en bitcoin n'est plus ce qu'elle était… Le système *Bitcoin* rencontre désormais une difficulté. Il ne peut gérer qu'une dizaine d'opérations à la seconde ce qui s'avère désormais très insuffisant.Un débat existe depuis des années au sein de la communauté *Bitcoin* et une partie de ladite communauté a adopté, le 1er aout 2017, une solution technique – l'agrandissant des blocks – en provoquant un « *fork* » - un embranchement – qui a conduit à la création d'une nouvelle monnaie numérique, le *bitcoin cash* (qui conserve néanmoins en mémoire toutes les opérations passées). Au cours des 2 premiers mois de sa vie, le cours du *bitcoin cash* a fluctué entre 200 et 700 $.

Des monnaies virtuelles, comme l'*éthereum*, permettent d'associer un paiement à la réalisation de conditions. Ainsi, A peut s'engager à verser 100 *ethereums* à B s'il fait beau. Il suffit que A et B s'entendent sur le référent qui déterminera s'il fait beau ou non. D'une façon générale, une telle fonctionnalité trouvera aisément des applications, comme le déclenchement du paiement à la réalisation d'une livraison, le référent pouvant être le livreur.

Un *bitcoin* considéré comme un rempart face à l'inflation repose par ailleurs sur une conception très angélique de la monnaie. D'une part, la stabilité des prix n'est pas garantie par une masse monétaire fixée. Les promoteurs du bitcoin procèdent en effet à une lecture intégriste de la loi de Fisher[30]. Pour que les prix restent stables, il faut, au moins en première approximation, non pas que la quantité de monnaie soit stable mais qu'elle croisse au même rythme que l'offre de biens et services ce que la conception d'une cryptomonnaie exclut – en tout cas aujourd'hui – puisque la création de *bitcoins* obéit à ses propres règles (Elle est générée par l'utilisation de la monnaie). D'autre part, la notion même d'inflation n'a guère de sens pour des monnaies virtuelles. Elles ne sont assises sur aucune économie et aucun prix n'est exprimé originellement en *bitcoin*. Ces prix le sont en monnaies souveraines et ensuite convertis. Aussi, les variations de prix en *bitcoins* reflètent avant tout les fluctuations du taux de change[31].

(30) Irving Fisher (1867-1947) est un économiste américain qui a expliqué que l'inflation était notamment causée par une création excessive de monnaie.

(31) Le taux de change est la valeur d'une monnaie exprimée dans une autre monnaie.

Le *bitcoin* offre en effet l'avantage d'être convertible en devises, à partir notamment de plateformes qui effectuent ces opérations de change. La contrevaleur en monnaies officielles du *bitcoin* obéit plei-

© blockchain.info

Cours du bitcoin contre dollars depuis 2009. Echelle de 0 à 4000$ pour un bitcoin

nement à la très classique règle de l'offre et de la demande : s'il y a plus de *bitcoins* à vendre contre une monnaie donnée que de *bitcoins* demandés dans cette monnaie, le cours du *bitcoin* baisse ; à l'inverse, s'il y a plus de *bitcoins* demandés que de bitcoins à vendre, le cours dans la monnaie donnée augmente. Les plateformes de change publient les cours en temps réels. Ces cours – sauf accident – ne diffèrent pas trop d'une plateforme à une autre, les opérateurs effectuant des arbitrages[32].

(32) L'arbitrage consiste à acheter sur une place pour vendre sur une autre en profitant des écarts de cours ; cette activité permet de lisser les cours.

(33) Le risque de change est le risque de perte liée aux variations de valeur d'une devise.

Le cours du *bitcoin* exprimé en dollars (et c'est vrai aussi en euros) apparaît comme très instable, avec une tendance à la hausse. D'aucuns affirment qu'il s'agit là d'un défaut de jeunesse, qui passera avec le temps. C'est peu probable, l'instabilité étant inhérente par construction. Le *bitcoin* fait courir un fort risque de change[33] à ceux qui le détiennent :

– il ne possède pas de valeur intrinsèque, qui jouerait le rôle d'un garde-fou. Les métaux précieux, par exemple, ont une valeur *a minima* qui est celle fixée sur un marché par l'offre et la demande industrielles et c'est cette valeur de marché qui sert de référence sur le long terme aux opérateurs pour déterminer s'il faut vendre ou acheter. A cet égard, il sera intéressant de suivre l'évolution du *Bilur*, monnaie virtuelle récente dont les promoteurs ont adossé la valeur à celle d'un stock de pétrole ;

– aucune banque centrale n'intervient pour maintenir sa valeur de change ; en effet, lorsque le taux de change d'une devise est éloigné de ce qui semble souhaitable aux autorités monétaires d'un pays, la banque centrale procède à des achats ou des ventes sur la marché des changes, qui agissent sur le cours de la monnaie ; même dans un système de change fixe[34], la stabilité requiert des interventions d'un organisme central comme le Fonds monétaire international (FMI), créé par les accords de Bretton Woods à cette fin ;

– il n'est pas adossé à une économie et, de ce fait, la masse monétaire de *bitcoins* n'est pas garantie par une production de biens et de services[35] ; en effet, s'il advient que le taux de change d'une monnaie souveraine se dégrade de façon excessive, le commerce extérieur du pays concerné s'en trouve favorisé par une amélioration apparente de sa compétitivité, ce qui tend à redresser la valeur de la monnaie ;

(34) Un système de change est dit « fixe » quand les valeurs des différentes monnaies sont définies les unes par rapport aux autres par convention ; le système de Bretton Woods est un système de change fixe, les monnaies étant toutes définies par rapport au dollar (et l'or) ; quand le change n'est pas fixe, il est dit « flottant ».

(35) La valeur de l'euro, par exemple, est d'abord déterminée par la quantité de biens et de services produits au sein de l'UE et qui donc peuvent être acquis en euro.

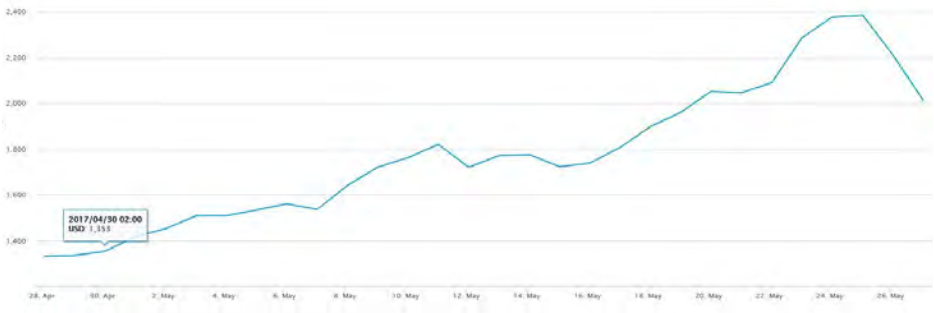
– il est en concurrence permanente avec les monnaies officielles et avec les autres cyber-monnaies, ces dernières offrant les mêmes services – voire encore plus de services ; un simple effet de mode, un engouement même passager pour une monnaie virtuelle concurrente se feraient alors sentir sur le cours du *bitcoin* ; ainsi le *monero* dont les promoteurs affirment qu'il est des plus anonymes a vu son cours doubler au cours de l'été 2016 et veut se poser en rival ; il en est de même pour l'*ethereum* passé de 8 $ l'unité en janvier 2017 à près de 400 en juin 2017 ; la compétition entre monnaies virtuelles peut devenir intense et jouer sur leur taux de change, avec de forts phénomènes spéculatifs ;

– la détention des *bitcoins* apparaît très concentrée : moins de 50 personnes possèdent 30 % des *bitcoins*, moins de 1000 en conservent la moitié ; l'étroitesse du marché fait que des variations de volumes échangés même réduites entraînent des variations de cours importantes, voire facilitent des manipulations de cours qu'on ne peut exclure dans l'actuelle envolée du *bitcoin*.

Du coup, le *bitcoin* est d'une nature très volatile. Alors qu'il se voulait apolitique, Il se montre très sensible au contexte politique. Sa première envolée, celle qui l'a fait connaître, date du printemps 2013, avec la crise chypriote et ses conséquences, notamment le blocage des comptes bancaires de l'île. De même, la crise grecque de l'été 2015 et le Brexit au début de l'été 2016 ont provoqué des sursauts. Le rôle de la Chine, devenue acteur majeur du *bitcoin*[36], est aujourd'hui mis en avant pour expliquer l'envolée des cours : le *bitcoin* est un moyen de contourner le contrôle des capitaux mis en place dans ce pays.

(36) La Chine représenterait 90 % de l'activité sur le bitcoin.

A l'inverse, des prises de bénéfice après de fortes envolées, des interdictions ici ou là, ou le piratage de plateformes ont fait chuter les cours. Pour illustrer ces variations, il suffit de constater une chute de l'équivalent de 110 € (par *bitcoin* …) en 3 jours, fin juillet 2016, à la suite du vol de 119 756 bitcoins sur la plateforme BIFINEX. Dans



Evolution du bitcoin contre dollar du 28 avril au 28 mai 2017.
L'échelle va de 1500 à 2400 dollars pour 1 bitcoin

© blockchain.info

l'autre sens, le cours du bitcoin a pris 10 % entre le 4 et le 11 septembre 2016 et même 3 % en une heure le 11 octobre 2016 … L'activité économique s'accorde mal avec une monnaie dont, au final, on ne sait trop comment va évoluer son pouvoir d'achat, même à court terme.

Ce qui donne du crédit au *bitcoin* aujourd'hui, c'est la croyance des utilisateurs en l'idée qu'en échappant à l'action publique, cette monnaie virtuelle échappe à l'inflation et protège l'épargne. L'idée est également solidement ancrée qu'avec le temps, le *bitcoin* ne peut que prendre de la valeur, en raison d'une offre limitée alors que la demande est présumée croissante. C'est oublier qu'il est en concurrence permanente avec d'autres monnaies virtuelles au risque de se faire supplanter. A cet égard, l'exemple du sucre en 1974 est instructif : sur la base de rumeurs annonçant une possible pénurie, le prix du sucre s'est envolé sur les marchés, multiplié par 8. Au bout de quelques mois, d'aucuns ont commencé à douter du bien-fondé de la pénurie annoncée et donc des prix. Ils ont pris leurs bénéfices, amorçant une chute des cours vers un niveau beaucoup plus normal mais laissant les derniers arrivés et les moins réactifs sur la paille !

Le graphe ci-dessus montre le change du bitcoin contre dollars s'apprécier de près de 70 % en un mois passant de 1400 à 2400 $ avant de perdre 20 % en deux jours. De telles fluctuations ne facilitent pas les échanges : la stabilité est l'une des qualités attendues d'une monnaie. Dans le cas présent, l'évolution récompense les détenteurs anciens de *bitcoin* (qui « *s'enrichissent en dormant* » selon l'expression d'un ancien président de la République) et pénalise les derniers entrants.

Le bitcoin intéresse la finance

Depuis plusieurs années le *bitcoin* intéresse le monde de la finance, pour des raisons diverses, avec un début de reconnaissance par différentes autorités de surveillance.

L'aspect le plus basique de la finance consiste à mettre en relation des agents ayant des disponibilités à placer et des emprunteurs. Des ressources disponibles sont une manne pour les entreprises en quête de financement. Certes, les marchés financiers (actions et surtout obligations) et les banques sont censés permettre la rencontre de l'offre et de la demande de capitaux. Malheureusement, il n'est pas toujours facile pour une entreprise de faire appel à l'un ou à l'autre. En effet, l'accès à l'épargne publique reste très largement l'affaire des structures de grandes dimensions tandis que les banques restreignent l'accès au crédit en période difficile.

Pourquoi alors ne pas emprunter directement auprès des détenteurs de *bitcoins*, c'est-à-dire faire appel à une ressource mondialisée ? On voit ainsi se multiplier les ICO, c'est-à-dire les « *initial coin offering* », des levées de fonds en monnaie numérique. Une entreprise a-t-elle besoin de capitaux ? Elle lance une ICO. En contrepartie des fonds reçus, elle donne des « jetons » aux investisseurs qui leur conféreront ultérieurement des droits : recevoir une action ou un accès prioritaire au produits élaboré grâce à ce financement… Les levées peuvent être substantielles : aux Etats-Unis, la société Civic, travaillant sur un développement de la *blockchain* pour vérifier l'identité a ainsi obtenu 33 millions de dollars en dehors de toute règle ! Rappelons que la législation encadrant l'appel à l'épargne est également là pour protéger l'épargnant. Des retours à la réalité pourraient s'avérer douloureux. La Suisse a d'ailleurs commencé à encadrer le phénomène.

La très forte volatilité[37] du bitcoin a suscité des produits spécifiques, sans doute encore marginaux mais en plein développement et calqués sur des produits similaires déjà disponibles pour les monnaies officielles. Il existe des produits de couverture[38] – qui ne demandent qu'à devenir purement spéculatifs – comme les contrats sur différence (« *contract for difference* » : CFD), les contrats à terme ou des swaps entre monnaies virtuelles[39]. Les très fortes variations du taux de change du bitcoin permettent de prendre des paris sur les évolutions à venir, avec un côté « jeux de casino » non négligeable.

(37) La volatilité mesure l'importance des fluctuations du prix d'un actif.

(38) La couverture est un moyen de protection en cas de variation des cours ; à l'inverse, la spéculation consiste à miser sur une évolution de cours en espérant un gain … ou en prenant une perte en cas d'erreur.

(39) Le CFD consiste à miser sur une valeur du bitcoin pour une date donnée et à encaisser ou payer à la dite date la variation du cours ; le contrat à terme consiste à acheter ou vendre des bitcoins à une date et pour une valeur convenues à l'avance ; le swap consiste en un échange temporaire de portefeuilles en monnaies différentes.

(40) Le sous-jacent est l'actif sur lequel porte le produit financier.

(41) L'effet de levier permet d'investir dans des contrats pour un montant supérieur à la mise de départ ; ainsi, des CFD permettent un effet de levier de 20, c'est-à-dire qu'il suffit de disposer d'1 € pour investir dans un contrat de 20 € et ainsi d'amplifier les gains … ou les pertes ; certains sites de trading offrent des effets de leviers de 400 !

(42) L'Autorité des Marchés Financiers a attiré l'attention sur l'impossibilité parfois de retirer ses gains … et sur le très grand nombre de perdants !

(43) Fonds domiciliés à Singapour, à Jersey ou aux Etats-Unis, la liste n'étant pas exhaustive.

Des courtiers proposent ainsi des options binaires qui consistent, moyennant le paiement d'une prime, à miser sur l'évolution du cours du *bitcoin* : si l'évolution est favorable, l'acheteur de l'option binaire perçoit la valeur du sous-jacent[40] augmentée d'une fraction de l'écart avec le cours constaté ; à l'inverse, une évolution défavorable se traduit par la perte du capital. Ces produits sont complexes, très risqués car avec de forts effets de levier[41] et évoluent trop souvent dans un univers opaque aux règles floues, quand ils ne relèvent pas de l'arnaque[42]. En fait, l'instabilité permet de gagner – ou de perdre – beaucoup d'argent en prenant des paris sur l'évolution des cours. Trop ressemblant à des jeux de casino, ces produits financiers sont à déconseiller au commun des mortels !

Les investisseurs peuvent recourir à des fonds[43], qui ne sont pas forcément ouverts au grand public. Aux États-Unis – encore -, un organisme vient d'être accrédité pour la compensation des swaps et produits dérivés en bitcoins, ce qui marque un début de reconnaissance officielle.

Une règlementation quasi-inexistante

La réglementation régissant à ce jour le bitcoin est réduite, au moins en Europe[44]. Son statut légal est à ce jour parfaitement indéfini. Souvent, c'est le fisc qui s'y intéresse.

(44) La Russie a interdit l'usage des monnaies virtuelles puisque seul le rouble doit être utilisé comme monnaie de paiement.

De nombreuses banques centrales ont attiré l'attention sur les risques inhérents à cet « *objet monétaire non identifié* ». En France, TRACFIN publiait en 2014 une série de recommandations pour réduire l'opacité des transactions effectuées par monnaies virtuelles, en demandant la justification de l'identité lors d'ouverture de compte, en encadrant les possibilités de paiement et en favorisant la coopération internationale dans la surveillance des flux de telles monnaies. Ces préconisations se heurtent à l'essence même des principes fondateurs des monnaies virtuelles.

Les promoteurs des monnaies virtuelles utilisent des arguments à géométrie variable au gré de leurs intérêts. Ainsi, se sont-ils réjouis du début de reconnaissance du bitcoin comme monnaie au travers de la décision de la Cour de Justice Européenne d'exonérer de TVA « *les opérations d'échange de devises traditionnelles contre*

des unités de la devise virtuelle bitcoin *(et inversement)* » car elles « *constituent des prestations de services fournies à titre onéreux au sens de la directive, dès lors qu'elles consistent en l'échange de différents moyens de paiement* »[45]. Mais tout autant, ils se sont félicités qu'à l'inverse un juge de Floride ait arrêté, en juillet 2016, que le bitcoin n'était pas un instrument monétaire, relaxant ainsi un prévenu mis en cause pour infraction à la législation sur le blanchiment d'argent.

(45) CJUE, arrêt dans l'affaire C-264/14 Skatteverket/David Hedqvist ; 22 octobre 2015.

(46) Position 2014-P-01 du 29 janvier 2014 de l'Autorité de Contrôle Prudentiel et de Résolution (organisme en charge de la surveillance du secteur bancaire et des assurances)

En France, l'ACPR[46] exige depuis le début de l'année 2014 que les plateformes exerçant des activités de change « *bitcoins contre euros* » reçoivent un agrément en tant qu'établissements de paiement. Il ne s'agit pas pour autant d'une reconnaissance officielle du bitcoin en tant que devise. Simplement, la réception de fonds en euro pour le compte de la clientèle, nécessaire pour la gestion des opérations de change, « *relève de la fourniture de services de paiement* » et elle est réglementée à ce titre. L'octroi de cet agrément implique de la part de son bénéficiaire des obligations en matière de contrôle interne, de cyber-protection et de lutte contre le blanchiment.

Le bitcoin et le crime

Détenir des valeurs de paiements est une chose, savoir les protéger en est une autre. Les orfèvres du Moyen-âge conservaient les métaux précieux de leurs clients et les maisons de change ont inventé la lettre de change pour limiter leur transport. Plus tard, les banques ont généralisé l'usage du compte bancaire pour réduire la détention de billets.

Aujourd'hui, la question de la sécurité porte sur la protection des *bitcoins* - et autres monnaies virtuelles - détenus. Qu'ils soient sur un support informatique personnel ou confiés à une plateforme spécialisée, ils attirent la convoitise des pirates.

(47) Les circonstances de la disparition des fonds n'ont cependant pas été éclaircies.

Les chiffres sont éloquents : la plateforme MTGOX – qui fut jusqu'à sa disparition l'une des références du marché des *bitcoins* – a vu s'envoler[47] l'équivalent de 450 millions de dollars. Au début du mois d'août 2016, c'est BITFINEX qui s'est fait voler 36 % de bitcoins détenus, soit 64 millions de dollars. A côté, le piratage de BITSTAMPS en 2015 fait figure de gagne-petit, avec un vol de 4,3 millions de dollars. Au final, selon des données fournies par REUTER, ce serait 30 % des plateformes qui auraient été piratées depuis 2012, principalement en raison d'un manque de moyens – ou d'intérêt - pour

assurer une cyber-protection efficace. Les pertes ont été répercutées pour l'essentiel sur les clients. L'absence d'autorité de surveillance facilite les comportements à risque et les hackers ont compris que la rentabilité du piratage est forte pour des risques faibles. Par comparaison, le secteur bancaire a une obligation de protection[48] et rend des comptes à une autorité de contrôle.

(47) Articles 88 et 89 de l'arrêté du 3 novembre 2014 ; de telles dispositions ne suffisent certes pas à rendre impossibles les cyberattaques mais elles les réduisent.

(49) Voir : https://www.undernews.fr/malwares-virus-antivirus/un-pirate-mine-620-000-dollars-de-dodgecoin-via-botnet-nas.html

Enfin, on a vu apparaître les *botnets* de minage. Ce sont des ordinateurs piratés, appelés « *zombies* » qui échappent au contrôle de leurs propriétaires et se mettent à travailler en réseau pour capter les *bitcoins* nouvellement créés[49] grâce à ou à cause d'un logiciel malicieux.

Le *bitcoin* n'est pas qu'objet de délit, il en est aussi un moyen. Le monde criminel est un univers fort bien structuré, à l'affût de toute innovation permettant d'accroître sa performance et sa rentabilité. Et les crypto-monnaies offrent des atouts considérables : discrétion, anonymat, circulation de valeurs sous un volume inexistant, sans frontière et sans le contrôle d'un tiers. Elles facilitent donc les flux illicites sur la planète, avec un très faible risque de détection, et peuvent être partout – ou presque – changées en monnaies officielles.

Au début du mois d'octobre 2013, le FBI fermait SILK ROAD, site mettant en relation acheteurs et vendeurs et se rémunérant par commission, où les paiements ne s'effectuaient qu'en bitcoin. Ce cyber-courtier du produit criminel, ouvert en 2011, aurait généré en 2 ans un chiffre d'affaires de 9,5 millions de bitcoins, à comparer aux 12 millions à l'époque en circulation. Sa fermeture a facilité l'émergence de multiples sites fonctionnant de façon similaire. La cyber-extorsion – par menace d'attaque -, le cyber-chantage s'accommodent fort bien de versements de fonds en *bitcoins*.

En France, la gendarmerie a fermé en juillet 2014 une plateforme clandestine de change, dans la région toulousaine, pour avoir réalisé 2 750 opérations de change pour plus d'un million d'euros dans le cadre d'activités illicites de jeux en ligne et le blanchiment des fonds en découlant. Ces opérations étaient effectuées dans des conditions particulièrement opaques, sans que les bénéficiaires justifient de leur identité, moyennant des commissions de 40 à 50 %.

(50) Les bitcoins ayant fait l'objet d'une saisie ont fourni l'occasion à l'AGRASC de se familiariser avec les cybermonnaies.

La gendarmerie a saisi au passage 388 bitcoins[50], l'équivalent de 200 000 €. De façon régulière, des affaires mettent en cause l'usage du *bitcoin* dans les mécanismes du blanchiment.

L'utilisation des bitcoins apparaît aussi avec les rançongiciels qui bloquent les systèmes informatiques tant qu'un paiement n'a pas été effectué, allant jusqu'à la destruction des données, comme l'a illustré la cyberattaque *Wanna Cry* du 14 mai 2017. Dans un premier temps, l'utilisateur de l'ordinateur a reçu un message contenant une pièce jointe. En ouvrant cette dernière, il a libéré le logiciel malicieux, lequel a immédiatement crypté les données du disque dur.

La rançon demandée était comprise entre 300 et 600 bitcoins. Selon le GUARDIAN[51], des banques anglaises stockeraient même des bitcoins pour faire face à d'éventuelles attaques de ce type. Précisons que le *bitcoin* n'est en rien responsable de l'agression, mais sa conception facilite la circulation de l'argent du crime.

(51) https://www.theguardian.com/technology/2016/oct/22/city-banks-plan-to-hoard-bitcoins-to-help-them-pay-cyber-ransoms

Le *bitcoin* est parfois comparé à l'argent liquide, ce qui demeure assez inexact. L'usage du numéraire est fortement encadré en raison de son absence de traçabilité, la plupart des paiements étant notamment limités à 1 000 €[52] . Le bitcoin, lui, s'il est anonyme, reste traçable : le « registre » de l'ensemble des opérations est à la disposition des participants au système.

(52) Art L.112-6 à L.112-8, art D.112-3 du Code monétaire et financier.

(53) Multiplication des mouvements entre quelques porte-monnaies pour nuire à la traçabilité des flux.

Toutefois, il existe des méthodes de blanchiment utilisées entre porte-monnaies de crypto-monnaies, comme le « *schtroumfage*[53] », afin de rendre le pistage impossible. De surcroît, dans ce domaine en plein évolution, l'adaptation aux « *besoins* » est rapide : d'une part, des procédés de cryptographie permettent de rendre les flux indétectables, d'autre part, sont apparues des monnaies virtuelles dont la spécificité est d'être intraçables, comme le *dash* (ex *darkcoin*) ou le *zerocoin*.

Conscientes que le premier garant de la valeur d'une monnaie est la confiance qu'on lui accorde, des plateformes de transactions ont entamé une réflexion, pour identifier et éliminer les flux malhonnêtes. L'idée est de repérer les portefeuilles à comportement suspect pour « marquer » les bitcoins, entre les « blancs » acceptables et les « noirs » à rejeter.

À l'instar d'Internet, le *bitcoin* et les crypto-monnaies constituent une formidable innovation. En revanche, le danger vient principalement de leur environnement. Elles ne pourront trouver leur place que si elles inspirent et méritent confiance. C'est une remise en cause de leurs fondements libertariens qui se dessine : elles ont besoin d'un tiers de confiance garant de leur bonne conduite.

L'AUTEUR

Jean-Luc Delangle est économiste et travaille depuis plusieurs années dans le contrôle du secteur financier. Après avoir exercé en qualité d'inspecteur général d'établissements de crédit, il a rejoint un organisme de surveillance.
Il est lieutenant-colonel de la réserve citoyenne de la gendarmerie, membre de la Réserve Citoyenne Cyberdéfense et chercheur associé au Centre de recherche de l'Ecole des Officiers de la Gendarmerie.

CyberEdu, parler
de sécurité numérique dans les cours

Par GÉRARD PELIKS

En 2013, le Livre blanc de la sécurité et de la défense nationale constate que trop rares sont les sensibilisations aux fondamentaux de la sécurité du numérique abordées dans les filières Bac+3 à Bac+5 qui forment aux métiers de l'Informatique. C'est un réel problème pour le pays, pour les données numériques et pour les citoyens alors que le passage vers le tout numérique progresse à grande vitesse dans les administrations, les services et l'industrie. Il est donc essentiel de convaincre les enseignants du supérieur de l'intérêt, en particulier pédagogique, de parler de sécurité dans leurs cours et de les accompagner dans cette démarche.

GÉRARD PELIKS
Président de CyberEDU

Il est des secteurs, comme celui de la gendarmerie nationale, de la Défense, des opérateurs de services essentiels (énergie, transports, aéronautique, banques)… où s'inquiéter pour la sécurité de ses données numériques va de soi. La sécurité n'est pas l'affaire que des experts, qui sont d'ailleurs aujourd'hui en nombre insuffisant, mais celle de tous. La solidité d'une chaîne est celle de son maillon le plus faible et pour le numérique il est crucial de renforcer l'utilisateur.

Le manque de spécialistes en sécurité pose un problème crucial alors que trop souvent les développements d'applications ne sont conduits ni avec les notions de « *sécurisé par conception* » ni avec celles de « *sécurisé par défaut* » comme le RGPD, règlement général pour la protection des données qui entrera en application dans les pays de l'Europe le 25 mai 2018, l'impose quand des traitements sur des données à caractère personnel sont pratiqués. Alors, par méconnaissance, on laisse dans des logiciels des failles qui conduisent à des attaques par dépassement de tampon, par requêtes volontairement mal formées… Et que dire de

Une fructueuse imprégnation aux impératifs de la sûreté numérique doit se faire dès les premiers apprentissages en école d'ingénieurs ou en faculté et lors de la formation continue.

l'absence de confidentialité et d'intégrité d'informations pourtant sensibles parce que l'utilisateur ne connaît pas les rudiments du chiffrement ? Que dire de l'absence de disponibilité et de résilience des fichiers parce que l'utilisateur ne les a pas sauvegardés. La sécurité de l'Information doit s'intégrer dans son vécu quotidien, devenir une seconde nature mais d'abord, elle s'apprend. Ainsi, nous diminuerons ensemble les risques des cyberattaques et leurs conséquences néfastes en local et pour les plus virulentes à l'échelle du pays.

La solution passe par un enseignement qui forme les futurs acteurs du numérique. Dès 2013, l'ANSSI, agence nationale de la sécurité des systèmes d'information, est chargée de trouver une solution. Elle lance la démarche CyberEdu et émet un appel d'offre pour que soient créés des éléments pédagogiques à destination des formateurs des filières d'enseignement de l'Informatique. L'université européenne de Bretagne, composée de 28 établissements d'enseignements supérieurs et de recherche, et Orange emportent ce projet. Aujourd'hui, de nombreuses fiches pédagogiques, de supports de cours, qui abordent différents aspects de la sécurité du numérique parmi lesquels : les systèmes d'exploitation, les réseaux, les bases de données, les langages, des notions de cryptologie, sont disponibles en licence Creative Commons et regroupées dans la « mallette pédagogique CyberEdu » :

https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/.

Bientôt ces documents et d'autres en développement migreront sur le site web de l'association CyberEdu, qui en est maintenant responsable et qui maintient et enrichit ces supports.

Proposer cette mallette pédagogique téléchargeable librement pour tous, à partir du web de l'ANSSI, ne suffisait pas. Pour que les enseignants s'approprient les différents éléments mis à leur disposition, et regroupés en deux catégories (Bac+3 et Bac+5), l'ANSSI a organisé des colloques gratuits à destination des personnels de l'enseignement supérieur susceptibles d'intégrer à leurs cours tout ou partie de ces modules ou de les adapter. Il est utile de préciser qu'il ne s'agit pas pour les enseignants d'ajouter simplement ces modules à leur enseignement existant, mais d'intégrer où et comme ils le souhaitent ces éléments pour enrichir leurs cours de notions de sécurité du numérique. De 2014 à 2016, quatre colloques ont ainsi été organisés par l'ANSSI à Paris. Plus d'une centaine d'universitaires, venus de Paris mais aussi des autres régions de France, ont bénéficié de ces colloques.

Mener ce type d'actions à destination des enseignants n'entre pas dans les missions à long terme de l'ANSSI et accompagner les universitaires dans les domaines de la sécurité du numérique est une tâche à confier à des universitaires. En conséquence, en mai 2016, l'ANSSI crée l'association CyberEdu qui a fait appel, pour constituer son bureau à des universitaires, experts ou non en sécurité du numérique, qui enseignent dans toutes les régions de France. La mission de cette association de bénévoles est de reprendre le flambeau, d'augmenter le volume des éléments pédagogiques fournis en diversifiant les thèmes de sensibilisation à la sécurité du numérique et en les adaptant à l'évolution des menaces et des contre-mesures disponibles.

L'association gère également un label qui distinguera les enseignements non dédiés spécifiquement à la sécurité de l'information mais qui intégreront ces éléments pédagogiques. L'ANSSI reste très intéressée par les actions de l'association. L'agence est représentée par le secrétaire général adjoint de l'association CyberEdu, Olivier Levillain, par ailleurs responsable du centre de formation de l'ANSSI qui a organisé un cinquième colloque en 2017. Maintenant, c'est à l'association CyberEdu que revient la mission de former les enseignants à la sécurité de l'Information pour qu'ils en tiennent compte dans leurs cours. Ainsi des enseignants parlent aux enseignants. Précisons ici que l'association CyberEdu n'est pas un organisme commercial de formation. Ses prestations sont gratuites, assurées par des bénévoles et réservées aux personnels de l'enseignement supérieur.

L'association CyberEdu est indépendante de l'ANSSI, mais cette dernière participe activement à ses groupes de travail. L'association se compose d'un bureau avec un président, des vice-présidents dans toutes les zones de l'hexagone et des secrétaires. Autour du bureau, chacun d'entre vous, chaque entité universitaire, chaque service administratif peut adhérer à cette association pour entrer dans les listes de distribution très actives et contribuer au travail commun qui, insistons bien, doit conduire à ce que la sécurité du numérique soit enseignée de base, dans toutes les filières de l'enseignement supérieur, et peut-être par la suite dans d'autres filières.

L'ambition de l'association CyberEdu ne se réduit pas, loin de là, à faire ajouter des modules de sécurité dans les filières qui forment ceux qui vont travailler dans le numérique. Elle souhaite dans un deuxième temps faire entrer naturellement les fondamentaux de la sécurité des données numériques dans les facultés de droit, de médecine et aussi dans d'autres filières comme par exemple les IUT qui sont très concernés. Par des concertations répétées auprès des directeurs d'IUT de notre vice-président en charge des outils, Philippe Werle (Université de Bordeaux), et de notre vice-président de la région Ouest, Xavier Roirand (université de Bretagne Sud), l'association a constaté qu'il convenait d'étendre son périmètre aux IUT qui nous demandent avec insistance de les aider.

La réputation des travaux de l'association CyberEdu a débordé nos frontières. Citons par exemple la Belgique, où le professeur Jean-Jacques Quisquater, éminent cryptologue, nous a contacté pour étudier les synergies que nous pouvons créer avec ce pays. Le vice-président de l'association de la zone Nord, Jean-Paul Pinte est chargé de concrétiser ces nouvelles relations que nous souhaitons bien sûr développer et grâce auxquelles nos capacités s'en trouveront renforcées.

Des membres du bureau de CyberEdu et d'autres experts dans leurs domaines mettent également leurs talents en commun pour ajouter ou renforcer d'autres modules dans la mallette pédagogique CyberEdu, en fonction de l'évolution rapide des technologies et des sciences humaines intéressant la sécurité du numérique. Citons par exemple le groupe « droit du numérique » animé par le secrétaire général de l'association CyberEdu, Patrick Erard, enseignant chercheur à l'IMT Atlantique à Rennes, et délégué général adjoint du Pôle d'excellence cyber, à qui l'on doit par ailleurs nombre de modules déjà présents dans la mallette pédagogique. Plusieurs avocats, des juristes, des ingénieurs se réunissent et agissent pour que la dimension juridique, pilier indispensable de la sécurité du numérique, ait la place qui lui convient dans l'ensemble des modules pédagogiques proposés. L'association a été récemment approchée par l'AFPA, association pour la formation professionnelle

des adultes. Des modalités pour des activités communes sont à l'étude, car bien sûr, les domaines de la cybersécurité offrent des postes de plus en plus nombreux et très intéressants d'autant plus que le pays manque cruellement de spécialistes.

Un label CyberEdu a été créé le 1er juin 2017, pour distinguer les enseignements qui, répétons-le, ne sont pas des enseignements spécifiques à la sécurité du numérique pour lesquels existe un autre label « SecNumEdu » géré directement par l'ANSSI. Déjà plusieurs dossiers ont été soumis à l'association. Le dossier à remplir est à récupérer sur le site http://www.cyberedu.fr/pages/labellisation/. Un groupe de travail « labellisation », présidé par Pascal Chour, responsable par ailleurs des labellisations à l'ANSSI, étudie les dossiers et l'association se donne environ deux mois pour valider les formations qui auront été jugées aptes à obtenir ce label CyberEdu. Les premières labellisations seront attribuées dès la fin de l'été 2018. L'association se chargera alors de publier largement sur les formations labellisées qui se distingueront des formations qui n'incluent pas la sécurité du numérique dans leur cursus.

Nombre de membres du bureau de l'association sont aussi impliqués dans d'autres associations, comme l'ARCSI (association des réservistes du chiffre et de la sécurité de l'information), la RCC (réserve citoyenne de cyberdéfense), le CECyF (centre expert contre la cybercriminalité français), et bien d'autres. Nous développerons ces synergies pour une efficacité accrue dans notre passion commune de faire entrer l'esprit et les notions de cybersécurité au plus près du citoyen.

L'Association CyberEdu organisera des rencontres et des échanges à Lille, à l'occasion du FIC 2018, marquant ainsi que son activité se situe dans toutes les régions de France.

La sensibilisation à la sécurité du numérique, qui comprend entre autres les domaines de la cybercriminalité, de la cyberdéfense, de la cybersécurité, abordés sous l'angle des sciences exactes mais aussi des sciences humaines, doit être l'affaire de chacun pour former et être formé. Le cyberespace, espace de tous les espoirs permis par beaucoup d'innovations disruptives, est aussi celui de tous les dangers. Tant qu'il existera dans le cyberespace des menaces et des cyberattaques, des

POUR EN SAVOIR PLUS

Sur le site www.cyberedu.fr, vous obtiendrez des informations sur l'identité et les missions de notre association. Allez voir la Foire Aux Questions (la FAQ) qui apporte des réponses aux questions qui nous sont les plus fréquemment posées. N'hésitez pas à nous contacter : cyberedu-contact@groupes.renater.fr

associations telles que CyberEdu pourront ne pas être inutiles. La cybersécurité est l'affaire de chacun d'entre nous, aussi chacun d'entre nous doit, sans forcément devenir expert de la sécurité du numérique, être formé. Nos libertés ne peuvent être garanties sans une nécessaire cybersécurité.

L'AUTEUR

Gérard Peliks travaille depuis plus de vingt ans dans le domaine de la sécurité de l'information. Ingénieur diplômé, son dernier employeur a été Airbus Defence & Space Cybersecurity. Il est lieutenant-colonel de la Réserve Citoyenne de Cyberdéfense (DGGN) et membre du Conseil d'administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI). Il préside l'atelier sécurité de l'association Forum Atena, et il est chargé de cours sur différentes facettes de la sécurité à l'Institut Mines-Télécom et au pôle Léonard de Vinci. Il est président de l'association CyberEdu, initiative de l'ANSSI pour que la sécurité du numérique soit évoquée dans les cours d'Informatique de l'enseignement supérieur.

Les enjeux de l'hyperconnexion : de la *smart* à la *safe cities*

Par MYRIAM QUÉMÉNER

Aujourd'hui, les villes intelligentes ou *smart cities*[1] sont un exemple parfait d'hyperconnexion puisqu'elles constituent une véritable concentration d'objets connectés qui occupent désormais une place centrale en tant qu'outils au service des utilisateurs. Equipées de capteurs collectant des données, s'appuyant sur des systèmes d'information pour optimiser leurs services, favorisant un usage croissant du digital, les smart cities bouleversent le fonctionnement de nos sociétés[2].

MYRIAM QUÉMÉNER

Magistrat, docteur en droit

Ces smart cities vont modifier la façon de vivre des citoyens, en raison d'une interconnexion entre les différents aspects de la ville, en intégrant des considérations socioculturelles mais aussi écologiques et environnementales. Selon les chiffres de Gartner[3], 8,4 milliards d'objets connectés sont dénombrés aujourd'hui dans le monde et, d'ici 2020, il devrait y en avoir environ 20 milliards[4]. Ils correspondent à l'ensemble des objets physiques, interagissant entre eux et/ou avec des individus *via* des réseaux de communication, qui collectent des données relatives à leur état et à celui de leur environnement. Du fait de sa capacité à recueillir massivement des données, l'Internet des objets[5] (IoT) accroît de façon très significative le volume de données générées sur le réseau. Il est donc l'une des sources

(1) www.cnil.fr/fr/definition/smart-city

(2) L'Internet des objets (IoT) est considéré comme la troisième évolution de l'Internet, baptisée Web 4.0. Il est en partie responsable de l'accroissement du volume de données générées sur le réseau, à l'origine du Big Data. L'IoT revêt un caractère universel pour désigner des objets connectés aux usages variés, dans le domaine par exemple de la e-santé , de la domotique ou du Quantified Self.

(3) Gartner, « Internet of Things. Endpoints and Associated Services, Worldwide », étude prévisionnelle de décembre 2015

(4) L'IDATE anticipe 80 milliards d'appareils connectés d'ici 2020, CISCO en envisage 50.

(5) Benhamou B., Internet des objets. Défis technologiques, économiques et politiques, Esprit, mars-avril 2009.

(6) L.Marino, l'Open data, une mine d'or pour les juristes, JCP G 2014, prat.438.

(7) Notion qui regroupe les outils, les principes et les méthodes permettant à chacun de mesurer ses données personnelles, de les analyser et de les partager. Les outils du quantified self peuvent être des objets connectés, des applications mobiles ou des applications Web.

du *Big data*[6]. L'internet des objets revêt un caractère universel et vise des usages variés par exemple dans le domaine de l'e-santé, de la domotique, des loisirs (drones, jouets), de la sécurité (surveillance et protection, armes, sauvetage…) ou du Quantified Self[7].

Les smart cities proposent des espaces plus écologiques, consommant 30 % d'énergie en moins que des villes comme Paris ou Londres. De plus, on se sert des données des citadins pour améliorer les transports ou les services publics. Rassemblées, les données collectées permettent par exemple de définir des itinéraires alternatifs afin de fluidifier le trafic routier et, par conséquent, de réduire les émissions de CO^2.

Les villes intelligentes doivent intégrer très en amont, dès la phase de la réflexion, les problématiques de protection des informations qui devront être à la fois en phase avec les besoins présents et futurs et faciliter (plutôt que freiner) le développement des services. Il est indispensable de bien définir les domaines d'intervention et de prendre les mesures essentielles pour favoriser l'essor de ces nouveaux services.

Ces projets peuvent être positifs pour la sécurité publique car les données recueillies peuvent permettre d'établir des statistiques sur le niveau de délinquance dans certaines zones urbaines.

Enjeux juridiques des smart et safe cities

Les smart cities brassent de multiples données et utilisent ainsi le Big data[8] pour tenter de mieux gérer les villes. Les infrastructures publiques ou privées, comme la domotique, les réseaux d'électricité, les télécommunications ainsi que les transports et les services administratifs sont concernées par ces traitements de données dans l'intérêt de la qualité de vie des usagers.

(8) T. Verbiest, Le « data », moteur des projets « smart cities », RLDI, N° 140, 1er août 2017

Une gouvernance urbaine encadrée

Les questions posées par cette nouvelle gouvernance urbaine se situent prioritairement au niveau de la protection des données personnelles car il existe une imbrication des sphères publique et privée, source de réelle complexité juridique.

Il faut rappeler qu'une obligation générale de sécurité incombe au responsable du traitement. En effet, l'article 34 de la loi Informatique et Libertés lui impose « *de*

L'interconnexion des objets et des infrastructures crée un univers numérique porteur de progrès et de risques pour les libertés individuelles.

prendre toutes précautions utiles (...) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Le non-respect de ces dispositions est puni par l'article 226-17 du code pénal de cinq ans d'emprisonnement et de 300 000 € d'amende, celle-ci pouvant atteindre 1 500 000 € pour les personnes morales.

La protection de la vie privée des personnes dont les données sont recueillies pour faire fonctionner une *smart city* est un enjeu majeur car le droit à la vie privée est un droit fondamental reconnu par les textes nationaux et internationaux. Il y a lieu de concilier le recueil, l'utilisation de données personnelles, le respect du droit à la vie privée car il existe un risque de surveillance de masse. L'exemple de la géolocalisation montre les avantages et les inconvénients d'une ville intelligente. Cette technique permet de suivre les déplacements d'une ou plusieurs personnes grâce à un téléphone. Les opérateurs de télécommunications, propriétaires des antennes, sont capables de localiser des personnes dont ils détiennent le numéro de téléphone.

La responsabilité des acteurs

Les véhicules autonomes sont des voitures intelligentes pouvant se déplacer toutes seules, sans que le conducteur ait quoi que ce soit à faire, grâce à leur connexion à un système central les aidant à faire des choix (changement de file, freinage, arrêt, *etc.*). Si un accident est causé par des dispositifs urbains interconnectés, à qui faudra-t-il imputer la faute ? De multiples intervenants seront susceptibles de voir leur responsabilité engagée (autorité publique locale qui est chargée de réguler la circulation, société ayant fabriqué le système intelligent…).

Le statut des données

Les données personnelles caractérisent un individu et sont détenues par des personnes morales (opérateurs de télécommunications, services publics sociaux, hôpitaux…). La question de leur propriété n'est pas tranchée. La ville intelligente étant bâtie sur une multitude de données, il convient de déterminer qui en est le propriétaire afin de cadrer leur utilisation et leur éventuelle réutilisation. Si l'on identifie le propriétaire d'une donnée, lui seul pourra par la suite, sans contestation possible, utiliser cette donnée comme bon lui semble.

(9) Rapport, Le numérique et les droits fondamentaux www.conseil-etat.fr/.../Rapports.../Etude-annuelle-2014

Le Conseil d'État, dans son rapport sur le numérique et les droits fondamentaux[9], a pris position pour ne pas reconnaître un droit de propriété sur ces données. Il prône la reconnaissance d'autres droits, comme un droit de regard sur l'utilisation des données concernant les citoyens.

Hyperconnections et cyberrisques

Si les *smart cities* présentent des aspects positifs pouvant les transformer en safe cities[10], il convient de ne pas négliger les vulnérabilités des systèmes d'information, les menaces générées par un ou des agents malveillants et les impacts potentiels de la sécurité des systèmes d'information[11]. Elles concernent aussi bien les collectivités que les opérateurs d'importance vitale du pays et les futurs opérateurs d'importance essentielle (définis par la directive européenne de juillet 2016 sur la sécurité des réseaux et de l'information) dont les dysfonctionnements sont susceptibles d'impacter fortement l'économie française.

(10) Harari David, Trink Claude, « L'amélioration de la sécurité des villes », Annales des Mines - Responsabilité et environnement, 2016/4 (N° 84), p. 15-21. URL : https://www.cairn.info/revue-responsabilite-et-environnement-2016-4-page-15.htm

(11) Misc N) 91 , Quelles sont les vulnérabilités des smart cities ?

Dans une *smart city*, la présence d'objets connectés, piliers des services innovants proposés par la ville, « *fait potentiellement peser un risque sur la sûreté des personnes, accru par l'interconnexion des services. Les services sont en effet portés par des systèmes d'information distincts mais interconnectés pour mettre en relation*

les feux de signalisation, l'éclairage, la distribution d'énergie, etc. ». Le risque cyber peut se maîtriser, « *il est particulièrement complexe à appréhender pour la smart city et il est nécessaire qu'une gouvernance soit mise en place pour traiter ce sujet, y compris par les collectivités* » mais les villes n'ont pas toujours les compétences ou les moyens financiers pour faire avancer ce sujet. L'ANSSI n'a d'ailleurs pas connaissance aujourd'hui qu'un projet smart city « *ait entamé une prise en compte du risque cyber à son juste niveau* ». Loin d'être fataliste face à cette situation, l'institution a commencé à déployer des agents sur le terrain pour sensibiliser les collectivités à ces questions. La CNIL accompagne aussi les communes de plus de 3 500 habitants sur l'anonymisation des données, une initiative inscrite dans le cadre des démarches *Open Data* qui leur seront obligatoires en 2018.

Solutions et perspectives

On constate la présence d'une multiplicité d'acteurs autour de la *smart city* et chacun d'entre eux doit avoir un rôle à jouer en tant que partie prenante de la cybersécurité

Les objectifs du législateur européen, exprimés à travers le Règlement général pour la protection des données (RGPD), vise à créer un cadre renforcé et harmonisé de la protection des données tenant compte des récentes évolutions technologiques comme les smart et safe cities, le Big data, les objets connectés associés à l'Intelligence Artificielle.

Le règlement (UE) n° 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, adopté par le Conseil le 27 avril 2016 et abrogeant la directive 95/46/CE du 24 octobre 1995 sur la protection des données, met à la charge du responsable du traitement une obligation de sa sécurité. Ce dernier doit ainsi garantir un niveau de sécurité adapté aux risques avec des mesures techniques et organisationnelles adaptées.

En matière de protection des données à caractère personnel, les obligations pesant sur le responsable du traitement ont été étendues. L'individu, placé au cœur du dispositif légal, voit ainsi ses droits renforcés : consolidation des obligations d'information, restrictions en termes de recueil de consentement, nouveau droit à la portabilité des données, à l'effacement, *etc*. La mise en place de ces villes intelligentes, afin de devenir de véritables *safe cities*, impose donc l'intégration et la mise en œuvre par les collectivités des dispositions du règlement européen sur la protection des données personnelles.

© Vichie81 - Fotolia.com

La multiplicité des acteurs au sein d'une *safe city* impose une gouvernance du régime d'utilisation des données personnelles.

État des lieux
de la sécurité des objets connectés

Par CYRIL NALPAS

L'Internet des objets se développe à une vitesse fulgurante. Il concerne aujourd'hui l'ensemble des secteurs d'activité et s'invite dans tous les environnements : le lieu de travail, la maison, les transports, sur terre ou sur mer... Comme le définit la Commission Européenne, il s'agit du mariage du monde physique et du monde virtuel en vue de produire des environnements intelligents par l'ajout aux objets traditionnels de composants électroniques, logiciels et dans certains cas de capteurs de diverses natures. L'engouement pour cette transformation numérique est à la hauteur des enjeux tant l'Internet des objets est créateur de valeur, notamment par l'optimisation des flux et des processus.

CYRIL NALPAS

Consultant Cybersécurité - Compagnie européenne d'intelligence stratégique (EIS)

Le cercle de réflexion McKinsey Global Institute évalue l'impact économique de l'IoT, d'ici à 2025, entre 3,9 et 11,1 billions de dollars par an. De son côté, IHS prédit plus de 30 milliards d'objets connectés en 2020 et plus de 75 milliards en 2025.

En élargissant le numérique à un nombre d'objets physiques et d'activités humaines toujours plus important, les objets connectés augmentent non seulement la surface de vulnérabilité aux menaces informatiques mais également les conséquences matérielles des risques associés. Pourtant, dans cette course à l'environnement intelligent, l'innovation et la rapidité de mise sur le marché prennent généralement le pas sur la maîtrise des risques cyber.

Un panel de vulnérabilités à l'image de l'hétérogénéité des acteurs de l'IoT

Un objet connecté possède plusieurs dimensions, toutes potentiellement porteuses de vulnérabilités : une base matérielle (proces-

seur, mémoire, capteurs, actuateurs, *etc.)*, logicielle, un vecteur de communication et une dimension applicative. Cette dernière dimension correspond à la plateforme qui collecte et traite les données, qu'elles soient locales (réseau interne du particulier ou de l'entreprise) ou distantes (de plus en plus souvent directement dans le *Cloud* de l'entreprise qui propose une solution unifiée).

Les socles matériels et logiciels n'échappent pas à la règle du recours toujours plus courant aux composants sur étagères, que ces derniers soient adaptés ou non à la finalité de l'objet connecté, afin de réduire les coûts de développement et d'accroître l'interopérabilité. L'utilisation de composants sur étagère et l'éclatement du processus de conception, qui comprend généralement une succession d'acteurs indépendants et parfois sans aucun lien, implique une faible maîtrise de la sécurité de la solution finale.

Les mauvaises pratiques dans la conception de ces systèmes comprennent notamment l'absence de chiffrement, le défaut ou la mauvaise implémentation de mesures de sécurité ou encore la présence de mots de passe par défaut. Bien souvent, ces derniers ne sont pas supprimés par l'utilisateur final, d'autant que certains systèmes ne le permettent pas. Les mauvaises implémentations[1] peuvent également concerner la couche réseau, à l'image des vulnérabilités baptisées BlueBorne découvertes par la société Armis en septembre dernier. Celles-ci affectent des implémentations du protocole *Bluetooth* présentes au sein de systèmes d'exploitation majeurs (Android, Linux, Windows).

(1) Installation d'un logiciel en réalisant les adaptations nécessaires à son fonctionnement.

(2) L'appairage (peering en anglais) désigne, en informatique, l'échange de trafic Internet avec des pairs. l'appairage implique trois éléments : une interconnexion physique entre les réseaux, une liaison virtuelle entre les réseaux pour permettre l'échange des routes via un protocole de routage et des accords commerciaux et contractuels entre les deux parties.

Ces failles particulièrement critiques ne nécessitent aucun appairage[2] ni aucune action de l'utilisateur pour être exploitées. Elles affecteraient plusieurs milliards d'appareils dont elles permettent de prendre le contrôle.

Aux vulnérabilités propres aux couches matérielles et logicielles s'ajoutent celles affectant directement les protocoles de télécommunications (et non leurs implémentations). L'actualité récente a ainsi fait émerger des vulnérabilités critiques concernant le protocole WPA2, celui-là même qui sécurise la quasi-totalité des réseaux Wifi modernes. Il s'agit des vulnérabilités Krack (pour Key Reinstallation AttaCK), qui permettent notamment de déchiffrer les paquets transmis sur le réseau et dans certains cas d'injecter des données malicieuses au sein des paquets.

Ces failles affectant les protocoles de communication réseau sans fil ou leurs implémentations sont d'autant plus drama-

Des contraintes économiques poussent les constructeurs à ne pas mettre en œuvre des maintenances de produits considérés comme obsolètes.

tiques que de très nombreux dispositifs ne sont jamais mis à jour. En effet, l'innovation, un faible coût unitaire ou encore la course aux performances contribuent à une prolifération d'objets connectés dont le cycle de vie est relativement court. Rapidement considérés comme étant obsolètes par leurs fabricants, la maintenance corrective est abandonnée par ces derniers. Sauf obligation contractuelle spécifique, aucune mise à jour ne sera ainsi produite afin de corriger les failles de sécurité découvertes ultérieurement.

Enfin, les objets connectés se distinguent du parc informatique traditionnel par l'absence de solutions de sécurité intégrées de type antivirus (*endpoint security*). Cette absence se justifie généralement par l'insuffisance des ressources (capacité de calcul, mémoire) disponibles sur ces dispositifs. Ces ressources sont effectivement généralement à l'échelle des besoins nécessaires pour remplir les fonctions premières de ces appareils, parfois très basiques. Il est évident qu'une solution de détection des menaces nécessite plus de ressources computationnelles que les menaces elles-mêmes en ont besoin, donnant un avantage indéniable à ces dernières. *A contrario*, les fonctionnalités des *malwares* peuvent être limitées par les faibles ressources des objets ciblés.

Un panel de risques extrêmement large

Le périmètre des risques associés aux objets connectés est à l'image de leur champ d'application : vaste et divers. Parmi les risques qu'impliquent leur usage, on retient notamment :

- des risques de fuite d'information par interception du flux réseau ou compromission de l'appareil. Les panoplies de cap-

teurs équipant les objets connectés en font des sources d'information directe sur le monde physique. A ceci s'ajoute le risque de collecte, non consentie par les utilisateurs, d'informations par les créateurs de la solution IoT, un cas qui concerne aussi bien des jouets que des sextoys connectés comme l'actualité a pu le démontrer.

Des risques de compromission du système d'information auquel l'objet est connecté : les objets connectés peuvent effectivement constituer des cibles en tant que vecteur initial d'une attaque informatique, permettant par mouvement latéral d'infecter les cibles véritables.

Des risques d'attaques par déni de service sur des cibles externes. Les objets connectés ne sont pas seulement une menace pour leurs utilisateurs, mais également pour les tiers. L'apparition en septembre 2016 du premier botnet[3] visant spécifiquement les objets connectés, Mirai, a concrétisé cette menace. En s'attaquant au potentiel jusqu'alors inexploité par les botnets des objets connectés grand public, le ou les auteurs de ce botnet ont pu lancer des attaques en déni de service d'une ampleur jusqu'alors inédite. Comme une piqûre de rappel, des chercheurs de *Check Point® Software Technologies Ltd*. mettent en garde aujourd'hui sur la formation d'un nouveau botnet appelé *IOTroop/Reaper* qui pourrait infecter plusieurs millions d'objets connectés, sans qu'il ne soit encore possible de déterminer les intentions exactes des acteurs à l'origine de cette nouvelle menace. Ce botnet en formation se distingue des précédents par sa méthode de propagation, qui ne repose pas sur une simple base de mots de passe par défaut mais sur des failles au sein des *firmware*[4] des objets connectés ciblés. Ainsi, à considérer que les principaux fabricants implémentent des mécanismes de changement obligatoire de mots de passe par défaut à la mise en service des appareils, il reste la problématique d'absence de mise à jour logicielle.

(3) Réseaux de machines zombies, utilisés pour des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS).

(4) Le firmware permet à un matériel informatique d'évoluer (via des mises à jour), d'intégrer de nouvelles fonctionnalités, sans avoir besoin de revoir complètement le design du hardware.

(5) Dispositifs destinés à effectuer une action, qui généralement influence le milieu matériel dans lequel ils se trouvent, sur commande d'un organe décisionnel.

Des risques de compromission des objets connectés dans un objectif d'action physique dans le monde réel. Au-delà des capteurs, nombreux sont les objets connectés dotés d'actuateurs[5], apportant ainsi une menace potentielle sur les personnes. Dans ce domaine, certains dispositifs médicaux critiques tels que des pacemakers ou des pompes à insuline ont à de nombreuses reprises été montrés du doigt pour leurs insuffisances flagrantes en termes de sécurité qui mettent en danger physique leurs utilisateurs. Notons à ce sujet que le danger ne se limite pas aux at-

taques ciblées sur les personnes : à l'heure du développement de *malware* ciblant les objets connectés, les porteurs de ces dispositifs pourraient être les victimes collatérales de pirates qui n'envisageaient pas les risques de leur création. Les risques ne se limitent cependant pas au domaine médical mais comprennent bien entendu l'ensemble des objets connectés dotés de capacité cinétique, dans le domaine de l'internet des objets industriels (transport, énergie, *etc.*) comme dans celui de la domotique (serrures connectées, fours, *etc.*).

Quelles réponses aux dangers de l'IoT à l'horizon ?

En août, quatre sénateurs américains ont déposé un projet de loi appelé « *IoT Cybersecurity Improvement Act* » visant à améliorer la sécurité des objets connectés. La stratégie consiste à imposer des obligations sur la commande publique plutôt que sur les constructeurs. Le Congrès américain est généralement très réticent à imposer des régulations qui auraient pour conséquence d'entraver le développement économique des entreprises. Le texte déposé proposait ainsi d'intégrer des clauses d'exigence de fonctionnalités de sécurité aux contrats de commandes publiques. Celles-ci imposeraient l'utilisation systématique de chiffrement pour le transfert de données collectées, l'intégration d'un mécanisme obligeant le changement de mots de passe et l'absence de mot de passe par défaut et notamment aux vendeurs de certifier l'absence de vulnérabilité connue au sein de leurs dispositifs. Plus important encore, tous les composants devraient être capables de recevoir des mises à jour du constructeur. Enfin, le texte prévoyait également d'assouplir le *Computer Fraud and Abuse Act*, en permettant aux chercheurs agissant de bonne foi de tester la sécurité des objets connectés sans craindre de poursuites.

Pour Bruce Schneier, directeur technique d'IBM Resilient, qui a participé à la rédaction des exigences de sécurité de la proposition de loi, elle n'a aucune chance d'être votée. Elle n'a d'ailleurs pas refait parler d'elle depuis la révélation de son existence à la fin du mois de juillet. Bruce Schneier place ses espoirs dans l'entrée en application du Règlement général sur la protection des données (RGPD), qui pourrait ouvrir la voie à l'adoption quelques années plus tard d'une loi similaire à celle proposée aux États-Unis. La taille du marché de l'Union européenne pourrait effectivement faire une différence si une telle loi venait à être adoptée en Europe.

En attendant l'adoption de lois de cette envergure, plusieurs pistes sont envisageables pour accroître la sécurité des produits. La première est le développement des labels sécurité. L'ENISA, l'agence de sécurité informatique européenne, s'est associée en mai dernier à plusieurs acteurs industriels européens pour lancer auprès de la Commission un appel à la création d'un label européen de sécurité. Le rapport

de l'ENISA proposait par ailleurs d'intégrer des exigences de sécurité au sein des marchés publics.

On trouve des initiatives plus concrètes dans le secteur privé. Dans le secteur médical, par exemple, les labels DMD et mHealth s'intéressent à la sécurité des applications mobiles médicales en sus des questions juridiques et de la pertinence médicale des solutions. De façon plus large, probablement plus poussée, Digital Security développe un programme de labellisation qui s'adresse aux acteurs de l'IoT désireux de faire vérifier par un tiers indépendant la sécurité de leurs solutions. Actuellement, en phase de test, ce programme nommé IoT Qualified Security (IQS) devrait voir le jour en début d'année 2018.

Du côté des acheteurs, il peut être judicieux d'avoir recours, lorsque c'est possible, au regroupement des achats entre structures ayant des besoins similaires. Il s'agit de peser davantage dans la négociation, non pas seulement pour réaliser des économies d'échelle, mais pour faire intégrer dans les contrats des exigences de sécurité concernant les produits et leur maintenance. Cela peut concerner, par exemple, les établissements de santé qui peuvent être tributaires des pratiques de fournisseurs incontournables de produits de niche.La question de la sécurité des objets connectés concerne l'ensemble des dispositifs. La position qui consiste à considérer qu'il faut approcher les questions de cybersécurité en fonction des usages, c'est-à-dire que l'on n'a pas à se soucier de la sécurité d'une caméra IP comme on se soucie de celle d'une pompe à insuline, semble aujourd'hui inadaptée face à l'évolution de la menace et de l'ubiquité de ces dispositifs. Si elle a du sens au niveau d'une organisation qui se penche sur la gestion de ses risques propres, cette vision est insatisfaisante à l'échelle globale. Dans cette optique, la voie normative est la plus à même d'opérer un compromis judicieux entre innovation et sécurité. Il faut aujourd'hui saluer et encourager les efforts réalisés en ce sens.

L'AUTEUR

Après une double formation en droit et en programmation, puis une première expérience dans le développement logiciel, Cyril Nalpas obtient un MBA de Risk Management et rejoint en 2014 le pôle cybersécurité de CEIS. En tant que consultant cybersécurité, il travaille notamment sur les études prospectives et stratégiques concernant l'espace numérique à destination du ministère des Armées.

Cybermalveillance.gouv.fr

C'est parti !

Par JÉRÔME NOTIN

Après une expérimentation dans la région des Hauts-de-France, le programme gouvernemental « Cybermalveillance.gouv.fr » a été lancé au niveau national le 17 octobre 2017. C'est l'occasion de revenir sur les objectifs de ce dispositif et son articulation avec les autres services de l'État dont les forces de l'ordre et en particulier la gendarmerie nationale.

De quoi s'agit-il ?

Le dispositif Cybermalveillance.gouv.fr est issu de la stratégie numérique du gouvernement, présentée le 18 juin 2015. Ses objectifs ont été ensuite détaillés dans la Stratégie nationale pour la sécurité numérique publiée le 16 octobre 2015.

JÉRÔME NOTIN

Directeur général du GIP ACYMA

Ses missions visent à apporter le meilleur soutien à l'ensemble de nos concitoyens, qu'ils soient des particuliers, des entreprises ou des collectivités, face à la cybermalveillance et s'articulent autour de 3 axes : la prévention, l'assistance et la prospective. Ces missions sont réalisées en synergie, dans une volonté de complémentarité, avec les autres services de l'État impliqués dans la lutte contre la cybermalveillance, telle que l'Agence nationale pour la sécurité des systèmes d'informations (ANSSI) principalement centrée sur la défense des Opérateurs d'importance vitale (OIV).

Pour porter ces missions d'intérêt général, le gouvernement a souhaité la création d'une entité juridique spécifique. L'ANSSI et le ministère de l'Intérieur, qui ont co-piloté ce projet, ont retenu la forme d'un Groupement d'intérêt public (GIP). Cette formule permet de réunir les talents des acteurs publics et privés, de disposer d'une autonomie de gestion sur le plan opérationnel tout en restant sous le contrôle de l'État. C'est ainsi qu'est né le GIP ACYMA (actions contre la cybermalveillance) le 3 mars 2017.

Ce groupement est composé pour partie de services de l'État : les services du Premier ministre (SGDSN-ANSSI), le ministère de l'Intérieur, le ministère de la Justice, le ministère de l'Économie et des Finances et le Secrétariat d'État au Numérique. Ils sont majoritaires au conseil d'administration et à l'assemblée générale en termes de voix. Le groupement est également composé de représentants du secteur privé avec des associations de consommateurs, des fédérations d'entreprises des secteurs du numérique ou de l'assurance, des représentants de chambres de commerce et d'industrie, des entreprises, des services d'assistance aux victimes et des entreprises du secteur du numérique comme des opérateurs de télécommunications, des éditeurs de logiciels, des sociétés spécialisées dans la cybersécurité...

Le GIP ACYMA a créé la plateforme Cybermalveillance.gouv.fr. Après une expérimentation de mai à octobre 2017, dans la région des Hauts-de France qui avait été choisie comme région pilote, la plateforme a généralisé l'accès à ses services sur l'ensemble du territoire national le 17 octobre 2017. Ce lancement national a été réalisé en présence du Secrétaire d'État chargé du numérique, M. Mounir Mahjoubi, du Secrétaire général de la défense nationale, M. Louis Gautier, du directeur général de l'ANSSI, M. Guillaume Poupard, du président de la Fédération française de l'assurance, M.Bernard Spitz et de M. Jérôme NOTIN, directeur général du GIP ACYMA ainsi que de nombreux représentants du ministère de l'Intérieur, dont M. Thierry Delville, Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces.

Dès mai 2017, le ministère de l'Intérieur a mis à la disposition du GIP ACYMA un officier de liaison, matérialisant la forte relation partenariale et transverse avec ses services, en la personne du capitaine de gendarmerie Dominique Bogé, expert en cybercriminalité, qui dispose également d'une parfaite connaissance du fonctionnement et de la structure du ministère.

L'assistance aux victimes

En ayant recours à la plateforme Cybermalveillance.gouv.fr, les victimes peuvent décrire leur problème en répondant à des questions types qui permettent d'établir un diagnostic. A l'issue, les premiers conseils leur sont donnés puis elles sont orientées au besoin vers les structures existantes pour les assister (par exemple : internet-signalement.gouv.fr). A ce titre, pour les victimes, le site Cybermalveillance.gouv.fr est un point d'entrée privilégié vers les différents services de l'État.

La plateforme propose également aux victimes des prestataires privés de proximité, susceptibles de les accompagner pour remédier au problème qu'elles rencontrent, si une intervention technique s'avère nécessaire. Après plusieurs vérifications, ces prestataires sont référencés sur la plate-

forme Cybermalveillance.gouv.fr. Ceux-ci se sont engagés au travers d'une charte qui encadre leur pratique. Ils peuvent faire l'objet d'une « notation » de leur intervention par les victimes. Au 15 novembre 2017, soit 1 mois après l'ouverture nationale du service, près de 1500 prestataires étaient référencés pour l'ensemble du territoire national.

Enfin, toujours dans l'esprit d'assister les victimes, la plateforme les accompagne dans leur démarche juridique. Elle propose pour certains types de cybermalveillance des fiches réflexes qui, entre autres éléments sur les bonnes pratiques préventionnelles à adopter et les actions à mener quand on en est victime, indique les incriminations pénales susceptibles de pouvoir être retenues lors du dépôt de plainte.

La prévention

La seconde mission du dispositif Cybermalveillance.gouv.fr est la sensibilisation du public aux bonnes pratiques en matière de sécurité et de protection de la vie privée numériques.

Des contenus de sensibilisation, réalisés par le dispositif avec le soutien de ses membres, sont d'ores et déjà disponibles sur son site Internet. Ce dernier met également en valeur des guides et supports pédagogiques réalisés par les tiers sélectionnés pour leur complétude et la qualité du message délivré.

Le dispositif réalise de surcroît des actions ponctuelles de sensibilisation dans différents cercles professionnels de son cœur de cible. Ces actions et contenus sont relayés sur les réseaux sociaux (Twitter-Facebook : @cybervictimes) afin de toucher le plus grand nombre de personnes. Ces comptes relayent également l'activité générale du dispositif.

A terme, le dispositif a pour mission de réaliser des campagnes nationales de prévention sur les sujets liés à la sécurité du numérique sur le modèle de celles de la sécurité routière.

La prospective

La troisième mission du dispositif Cybermalveillance.gouv.fr est la mise en place d'un observatoire de la menace numérique.

Celui-ci vise à apporter une vue sur la réalité de la cybermenace au-delà des statistiques des infractions relevées qui ne représentent parfois qu'une partie infime de phénomènes pas ou peu signalés aux forces de l'ordre. Cette vision offrira au pouvoir politique, aux services de sécurité et aux acteurs de la société civile une cartographie des risques et une analyse des tendances leur permettant une meilleure prise de décisions sur les axes d'effort nécessaires. Cet observatoire ne pourra être mis en place que lorsque le dispositif disposera de suffisamment d'éléments remontés et consolidés avec les sources

tierces, mais les premiers mois de fonctionnement ont déjà permis de confirmer certaines tendances et d'identifier l'émergence ou la recrudescence de certaines menaces.

A titre d'exemple, l'arnaque au « faux support technique » (*Tech Support Scam* en anglais) apparaît être une menace ascendante. Les victimes se font piéger durant une navigation sur Internet par des messages alarmistes leur demandant de rappeler sans délai un faux support technique pour « décontaminer » ou « réparer » leur ordinateur au prix de plusieurs centaines d'euros pour cette prestation réglée par carte de crédit. Les cybercriminels incitent souvent la victime à installer sur sa machine des logiciels de prise de contrôle à distance. Parfois, elle est également menacée de destruction de ses fichiers ou de la divulgation de ses données personnelles si elle refuse de payer une nouvelle fois. En nombre de cas référencés par Cybermalveillance.gouv.fr, cette menace touche à ce jour plus de victimes que celles de rançongiciels et il apparaît que la démarche, visant à la circonscrire, va devoir être assortie d'une forte priorité.

Une complémentarité forte avec le ministère de l'Intérieur

Co-pilote avec l'ANSSI, le ministère de l'Intérieur est un des principaux partenaires du dispositif Cybermalveillance.gouv.fr. Dès mai 2017, le ministère de l'Intérieur a mis à disposition du GIP ACYMA un officier de liaison chargé d'assurer la relation forte et indispensable avec ses services en la personne du capitaine de gendarmerie Dominique Bogé, expert en cybercriminalité. Durant la phase d'expérimentation, des contenus de sensibilisation ont été fournies aux 5 groupements des Hauts-de-France pour diffusion dans les brigades territoriales.

Les services de police et de gendarmerie sont en première ligne vis à vis des citoyens lorsque ceux-ci sont victimes d'une malveillance. Le monde cyber n'échappe pas à ce phénomène. Pour autant, la problématique soumise par la victime ne relève pas toujours de la plainte au pénal et la victime peine parfois à décrire le problème auquel elle est confrontée, en particulier dans les cas de cybermalveillance. Le dispositif Cybermalveillance.gouv.fr peut alors agir en permettant de mieux identifier le problème. Les fiches « réflexe » rappellent les infractions qui peuvent être retenues et servir de support pour la qualification d'une plainte. En complément de celles-ci, Cybermalveillance.gouv.fr peut proposer des moyens de remédier aux problèmes rencontrés au travers des conseils dispensés à la victime ou en l'orientant vers des prestataires techniques de proximité référencés pour leurs compétences afin de « réparer » les conséquences de l'incident subi. Si Cybermalveillance.gouv.fr a donc vocation à orienter naturellement les victimes vers les services de police et de gendarmerie lorsqu'un dépôt de plainte

apparaît nécessaire, ces derniers doivent pouvoir tout aussi naturellement orienter les victimes vers Cybermalveillance.gouv.fr quand le sujet ne leur semble pas relever du pénal ou pour permettre à la victime d'obtenir les moyens d'en réparer les dommages.

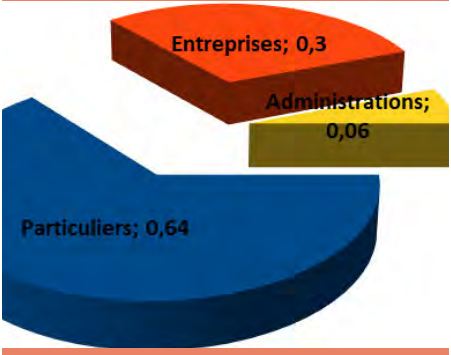
Enfin, Cybermalveillance.gouv.fr coopère avec les services spécialisés en cybercriminalité de la police et de la gendarmerie tel le centre de lutte contre les criminalités numériques (C3N) avec lesquels elle échange régulièrement que ce soit pour la réalisation des supports de sensibilisation ou pour la qualification des menaces émergentes.

Retour sur l'expérimentation sur les Hauts-de-France

Comme prévu durant la phase d'incubation au sein l'ANSSI, le dispositif Cybermalveillance.gouv.fr a d'abord été expérimenté dans la région des Hauts-de-France.

Cette région a été sélectionnée pour sa représentativité du territoire national avec de grosses agglomérations et des zones moins urbanisées. Par ailleurs, les acteurs locaux, en particulier les acteurs publics, y sont très sensibilisés aux problématiques de sécurité du numérique. L'organisation tous les ans du Forum International de la Cybersécurité en janvier à Lille ou la distribution d'affiches de présentation de cybermalveillance.gouv.fr dans les brigades de gendarmerie lors de l'expérimentation illustrent cet engagement particulier.

Durant cette phase d'expérimentation 724 victimes ont effectué un signalement d'incident.



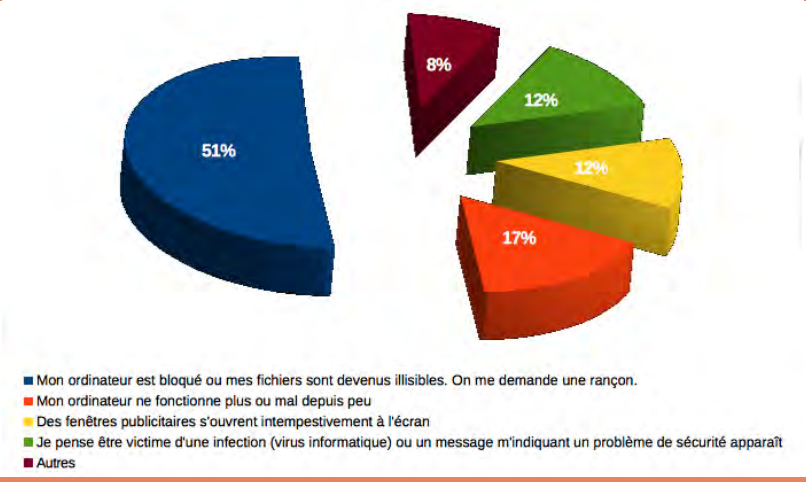
© Adobe Stock

Incidents par catégories de victimes.

64 % d'entre-elles étaient des particuliers, 30 % par des entreprises et 6 % par des administrations.

Ces signalements ont permis de confirmer que la menace principale concernant les particuliers était sur cette période les rançongiciels. Ils ont été 202 à déclarer avoir été victime de ce type de programme malveillant (soit 51 % des incidents qui ont touché les postes de travail).

La phase d'expérimentation a également permis de référencer un nombre important de prestataires afin de préparer le lancement national. La veille de celui-ci, le



Menaces touchant les ordinateurs des particuliers.

dispositif avait en effet validé l'inscription de 1120 sociétés sur 1300 demandes (180 étant rejetées ou en cours de complément d'instruction), offrant une couverture nationale très complète de la population pour l'ensemble des incidents de sécurité identifiés.

Et maintenant ?

Moins d'un mois après le lancement national, plus de 2500 nouveaux signalements ont été effectués, démontrant le besoin réel d'accompagnement des victimes et l'utilité de ce dispositif. Le retour d'expérience obtenu, tant sur l'expérimentation des Hauts-de-France que depuis le lancement national, laisse entrevoir toutes les optimisations et les développements de services que la plateforme Cybermalveillance.gouv.fr devra pouvoir offrir à ses usagers. De nouveaux partenaires arrivent dans le dispositif pour y apporter leur contribution. Ce partenariat actif des services de l'État avec les acteurs du secteur privé permettra, par leur complémentarité et leur engagement, de développer l'action de service public entreprise pour lutter ensemble contre les menaces qui pèsent dans le cyberespace et renforcer ainsi la confiance numérique de nos concitoyens à l'heure où le digital n'a jamais été aussi présent dans leur vie quotidienne.

L'AUTEUR

Impliqué dans la sécurité digitale depuis de nombreuses années Jérôme Notin dispose d'expériences dans la création et la direction d'entreprises. Il a rejoint l'ANSSI en mai 2016 en qualité de préfigurateur du dispositif et a été nommé en mars 2017 directeur général du GIP ACYMA. Il est par ailleurs ancien gendarme auxiliaire (94/10 PSIG de Blois) et chef d'escadron de la réserve citoyenne cyberdéfense de la gendarmerie.

La donnée, nouvelle préoccupation du comité exécutif

Par GÉRARD HATABIAN

Cet article est l'occasion d'esquisser la méthodologie à mettre en œuvre pour sensibiliser un Comité Exécutif, l'alerter sur le tsunami des données qui va déferler sur l'entreprise et l'amener à se saisir du sujet Donnée pour favoriser les initiatives terrain des métiers tout en préservant une logique d'entreprise préparant et préservant l'avenir.

De longue date, les données sont au cœur des processus « métier » d'un Groupe comme EDF

GÉRARD HATABIAN

EDF - Direction des Systèmes d'Information Groupe -Directeur Donnée Groupe.

La donnée n'est pas une histoire récente pour EDF. Quelques cas d'usage de la donnée « historique », au cœur des préoccupations des équipes opérationnelles depuis des décennies sont là pour nous le rappeler :
– Prévision de consommation ;
– Compréhension des comportements sociétaux vis-à-vis de l'énergie ;
– Détection de signaux faibles pour ajuster la maintenance des installations ;
– Utilisation des données comportementales des opérateurs en salle de conduite pour valider les nouveaux systèmes de conduite informatisés.

(1) La gestion du cycle de vie des produits, ou GCVP (en anglais product lifecycle management, ou PLM), est un cadre organisationnel et un ensemble de concepts, méthodes et outils logiciels visant à créer et à entretenir les produits industriels tout au long de leur cycle de vie, depuis l'établissement du cahier des charges du produit et des services associés jusqu'à la fin de vie, en passant par le maintien en conditions opérationnelles

Pourtant nous avons acquis la certitude que nous sommes aujourd'hui confrontés à un changement de paradigme sur la donnée :

– Les conditions d'acquisition, de transmission, de traitement, de stockage sont profondément modifiées.

– La variété des sources d'approvisionnement est devenue une réalité

industrielle : Internet des Objets dans les centres de production mais également chez nos clients, description des installations dans des systèmes de *Plant Lifecycle Management*[1], mais aussi données issues des scanérisations 3D de nos installations, données issues des réseaux sociaux….

(2) Compteur connecté d'Erdf.

– Le volume de nos données va croître régulièrement (Données Linky[2] par exemple). Enfin, la vitesse de traitement, y compris dans les approches analytiques, va se rapprocher du temps réel.

Les finalités d'usage évoluent aussi : au-delà de l'usage de la donnée pour la classique amélioration de la performance opérationnelle des processus, nous utilisons maintenant la donnée pour créer de nouveaux services… voire des nouveaux modèles d'affaires.

S'agissant de la relation client, il y a ce que l'on fait depuis longtemps :

– Mener à bien les opérations : je facture,
– Faire du reporting : je fais mon bilan,
– Prendre des décisions : je décide d'investir pour couvrir des besoins croissants de mes clients).

Il y a aussi ce que l'on commence à faire :

– Améliorer les processus opérationnels : je dispose en ligne des informations sur mon client au moment où il appelle,
– Proposer de nouveaux services : je réponds aux questions les plus simples par un automate sans attente,
– Imaginer de nouveaux modèles d'affaires : je vends un budget énergie et non plus de l'électricité avec l'offre Sowee).
– La donnée : une importance stratégique visible au plus haut niveau du Groupe

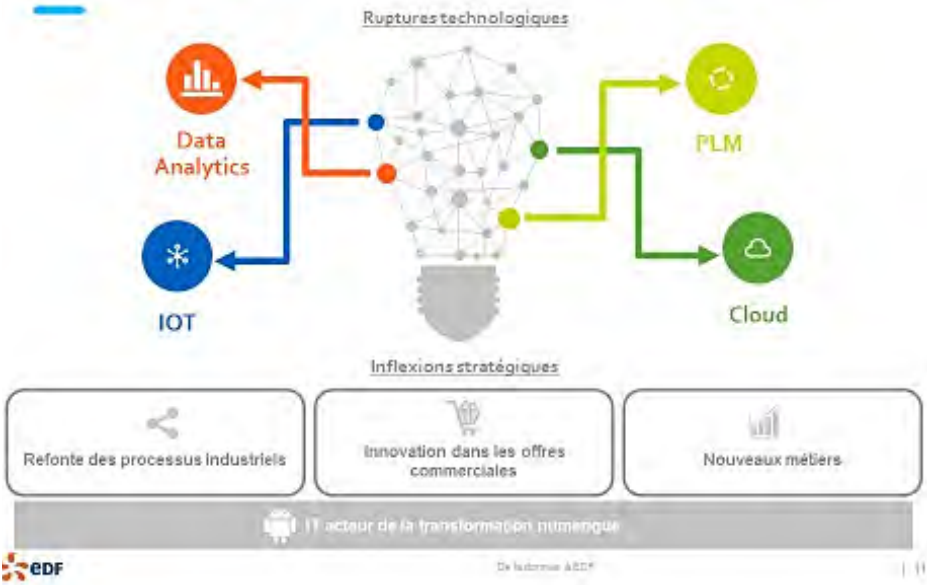
Face à cette nouvelle réalité de terrain, la donnée s'est invitée, sûrement pour la première fois, dans les préoccupations du Comité exécutif du Groupe.

Ainsi, CAP2030, le projet d'entreprise d'EDF à horizon 2030, contient un chantier transverse sur l'« *Accélération de la transformation numérique du Groupe* » où une des 5 orientations s'intitule tout simplement « *Valoriser les données* ».

CAP2030 s'attelle de même, dans la cadre d'un chantier similaire, à la simplification des politiques Groupe visant à réduire drastiquement le nombre d'exigences s'imposant aux managers. Malgré ce contexte de disette, une division par 5 du nombre de ces politiques, le COMEX a décidé d'en ajouter une nouvelle, uniquement consacrée à la Donnée : une Politique de Gestion de la Donnée, détaillée plus loin.

Deux autres initiatives illustrent l'importance prise par la donnée au sein du COMEX.

C'est ainsi qu'une campagne de communication « Corporate » a été engagée, centrée sur 12 engagements personnels



pris, *intuite personae*, par les 12 membres du COMEX pour accélérer la transformation numérique du groupe…De son coté, le directeur exécutif du pôle Commerce s'engage sur la donnée.

Dans le même esprit, un séminaire COMEX « Ruptures Technologiques SI et Inflexions Stratégiques métier » a porté un éclairage sur 4 technologies majeures ayant modifié la stratégie métier de plusieurs grands Groupes où le rôle de la donnée s'est révélé être omniprésent et central.

D'une politique Groupe de gestion de la donnée…. à une stratégie « données » du Groupe

Politique Groupe de Gestion de la Donnée

La politique Groupe de gestion de la donnée adoptée en COMEX est porteuse d'un véritable changement de posture. Elle est tournée vers l'ouverture, le désîlotage, la gouvernance et la valorisation des données.

Cette politique rétablit un équilibre entre des orientations défensives de protection (sécurité du SI, patrimoine à protéger contre la malveillance), des orientations (protection des données à caractère personnel) répondant à des contraintes réglementaires ou légales et une démarche offensive de création de valeur, davantage portée vers l'ouverture et la valorisation des données, favorisant le partage, la transversalité, le rapprochement des données pour produire de nouvelles connaissances.

Beaucoup plus que les spécialistes de la donnée, cette politique cherche à mobiliser un management sensibilisé par le biais de 10 questions clefs auxquels tout manager doit avoir réfléchi.

Cette politique va ainsi permettre à chaque

salarié du Groupe de savoir comment classer les données qu'il produit ou importe, à qui s'adresser pour avoir accès aux données dont il a besoin, quel usage il peut faire de ces données, comment se conformer aux exigences réglementaires ou légales, combien de temps et comment les conserver, comment les publier…

A titre d'illustration, donnons quelques exemples de principes directeurs ou d'exigences portées par la Politique de la Donnée.

Un principe fondateur de la politique de gestion de la donnée est d'assurer la transversalité et le décloisonnement des données produites par une entité ou importées par elle de l'externe. Il faut pour cela parler un langage unique au sein du Groupe (EDF SA et à tout le moins ses filiales non régulées).

L'élaboration de ce langage repose sur deux principes : le premier est de classer les données en domaines pertinents (météo, clientèle, installations…). Le deuxième est d'accompagner chaque ensemble de données de critères qui le caractérisent : confidentialité, qualité, durée de conservation, ouverture à l'externe…

L'ensemble constitue le catalogue des données potentiellement accessibles au sein du groupe EDF. Ce catalogue permettra aux projets d'identifier pour chaque ensemble de données l'entité qui en est le gestionnaire, les modalités d'accès et les règles qui s'y appliquent.

La liste des différents domaines de données et sa gestion dans le temps sont de la responsabilité du « Directeur Donnée du Groupe », localisé à la DSI Groupe.

De son côté, chaque entité du Groupe désigne un « Responsable Donnée d'Entité » qui a en charge de proposer au Directeur Donnée Groupe des domaines métier dont il souhaite que son entité prenne la responsabilité. Le domaine de données ainsi reconnu se voit désigner un « Responsable de Domaine de Données » appartenant à l'entité.

Ce dernier est responsable de la définition précise des données de son domaine, de leurs caractéristiques, des entités qui les produisent ou les importent et des règles d'utilisation de ces données. Ce travail est réalisé de manière collaborative avec l'ensemble des entités du Groupe.

L'un des objectifs de la politique de gestion de la Donnée est de faciliter le ré-usage des données produites par une entité ou importées par elle. Les données sont par défaut caractérisées dans le catalogue comme « accessibles » ou « ouvertes » aux projets qui en ont le besoin tout en affectant des contraintes de manipulation lorsque c'est nécessaire (telles celles qui sont relatives à la protection des données personnelles ou aux données clients).

Afin de faciliter le ré-usage des données produites par une entité ou importées par elle, l'usage des données se fait sous la responsabilité de celui qui les consomme et non de celui qui les produit. Chaque entité consommatrice des données s'engage à prendre connaissance des règles et exigences du domaine concerné de données, les applique et contribue à les améliorer.

A ces règles, élaborées et entretenues par les responsables de domaine de données s'ajoutent celles, plus générales, s'appliquant au groupe EDF, comme celles relatives à la protection des données personnelles, à la sécurité informatique, à la protection du patrimoine face à la malveillance ou à l'éthique.

Une stratégie Donnée

La stratégie Donnée du Groupe est en cours de construction, dans le cadre défini par la Politique, avec deux finalités.

Il s'agit d'abord de disposer d'une démarche méthodologique permettant d'associer au plus haut niveau d'une Direction « métier » les enjeux de la Direction et le rôle de la donnée dans l'atteinte de ses enjeux. Cette méthode a pour vocation d'être appliquée de manière systématique dans toutes les Directions et toutes les filiales.

Le second objectif est de gérer au niveau Tête de Groupe et dans la durée les aspects transverses liés à la donnée : compétences, infrastructures, architecture, politique industrielle, politique de partage et d'accès aux données en interne, services autour de la donnée (catalogue de données, dispositif Open Data vers l'externe,…).

Une DSI groupe au carrefour des enjeux autour de la donnée

Ces nouvelles orientations mettent la DSI Groupe au carrefour des enjeux antagonistes portés par la donnée. En effet, on l'a dit, la politique Groupe de gestion de la donnée rétablit un équilibre entre des orientations défensives de protection (sécurité du SI, patrimoine à protéger contre la malveillance), des orientations (protection des données à caractère personnel) répondant à des contraintes réglementaires ou légales, et une démarche offensive de création de valeur, davantage portée vers l'ouverture et la valorisation des données, favorisant le partage, la transversalité, le rapprochement des données pour produire de nouvelles connaissances.

La DSI du Groupe est une Direction fonctionnelle, composée d'une trentaine de personnes, en charge de définir et d'impulser les orientations, les politiques, les stratégies. Elle vient donc de prendre à son compte la dimension Donnée et plus particulièrement la dimension Valorisation de la Donnée, en localisant en son sein le tout nouveau Directeur Donnée Groupe ; il y trouve sa place à côté du Correspondant Informatique et Liberté, placé de longue date au sein de cette direction fonction-

Une DSI groupe au carrefour des enjeux autour de la donnée.

nelle. Ces 2 fonctions, à la marge du Système d'Information, cohabitent avec une troisième fonction essentielle pour la donnée, mais qui a toute sa place dans une Direction des Système d'Information classique, à savoir la fonction de Responsable Sécurité du Système d'Information.

Ces 3 fonctions sont donc pilotées sous la responsabilité directe du même dirigeant, assurant par là-même cohérence, complémentarité et résolution des enjeux multiples et parfois contradictoires.

Quelques belles histoires sur la donnée

Ces considérations générales d'ordre politique ou stratégique sont indispensables mais il est utile de les compléter par quelques « belles » histoires sur la donnée, illustrant de manière concrète leur mise en œuvre.

1/ Le traitement analytique des données de masse via des infrastructures BigData :

• une infrastructure homogène et à la pointe de la technique est imaginée par le R&D pour nos équipes Commerciales, puis

mise en exploitation industrielle au sein de nos services partagés,

• cette même infrastructure imaginée pour les métiers de l'aval trouve maintenant un usage pour les données de la Production Nucléaire, et se trouve à l'origine d'une démarche globale de « Data Analytic pour la Production »

2/ Les données issues des scan 3D TQC (Tel que Construit) des installations

Une démarche R&D initiée des années 1990 dont le seul usage opérationnel à l'époque était centré sur le mécénat technologique trouve dans les années 2010 (et comme imaginé à l'origine mais sans succès) un aboutissement dans une démarche industrielle (Scan des Bâtiments Réacteurs des têtes de série, opérations de maintenance dans le but de simuler les déplacements des opérateurs sur site).

3/ Une gestion des compétences sur le traitement des données en langage naturel

Une co embauche Commerce/R&D à la R&D d'un premier chercheur conduit à la création d'une équipe spécialisée à Commerce sur le traitement des mails, des réactions sur le net, avec en appui des équipes de recherche.

La donnée a pris une place majeure au sein d'une Direction des Système d'Information du Groupe, dont la mission est maintenant à la fois de créer les conditions d'une meilleure valorisation de ces données, dans le respect des contraintes de sécurité et de protection des données personnelles, et de démontrer *in fine* aux parties prenantes du Group, et en premier lieu le COMEX, que les gains apportés par les données sont à la hauteur des attentes.

L'AUTEUR

Diplômé de l'Ecole Nationale de la Statistique et de l'Administration Économique (ENSAE), Gérard Hatabian a fait toute sa carrière à EDF. Il entre comme Ingénieur-Chercheur à EDF R&D où il applique très tôt les techniques d'analyse des données aux domaines alors en récente expansion dans l'entreprise que sont la sociologie, les facteurs humains, les études de marché, les enquêtes d'opinion,…
Après avoir dirigé pendant 5 ans un Département de Recherche sur le Traitement de l'information, il quitte la R&D pour travailler auprès du Directeur des Systèmes d'Information de la Production et de l'Ingénierie qu'il seconde pendant une dizaine d'années. Il dirige ensuite pendant 4 ans l'Observatoire Statistique d'EDF SA.
En novembre 2014, il rejoint le Directeur des Systèmes d'Information Groupe, pour piloter le chantier de transformation numérique interne du Groupe, où il définit les contours de la mission d'Animation et de Gouvernance de la Donnée pour le Groupe. En juillet 2017, il devient le premier Directeur Donnée Groupe.

@tatomm AdobeStock

PRÉDIRE POUR UNE COUVERTURE TERRITORIALE INTELLIGENTE

Les hommes qui commandent ou qui exécutent les missions de surveillance connaissent leur circonscription. Ils orientent leur activité de manière intuitive, en s'appuyant sur leur expérience et l'examen de statistiques. C'est le cas pour le traitement des vols de véhicules. Toutefois, il est difficile de saisir, au seul regard de la criminalité légale, les fils directeur d'une délinquance d'appropriation qui peut être itinérante, endogène ou centrée sur une délinquance spécifique (braquage, convoyage de stupéfiants).

L'idée a été d'appliquer des algorithmes à une base de données agrégeant des informations puisées légalement en sources open, issues du service de la gendarmerie ou calculées à partir d'informations complémentaires. Le logiciel qui en résulte, baptisé « PredVol », fournit les résultats des prédictions journalières aux opérationnels de terrain. Globalement, il permet de visualiser les quartiers les plus risqués, d'afficher une typologie des quartiers en fonction des modes de vols et de visualiser les faits passés sur une carte. C'est une aide à la décision qui s'inscrit dans la police de proximité et dans une démarche évolutive. La pratique du terrain entraînera des inflexions du développement du logiciel et de son algorithmie par une interaction avec les concepteurs de ce remarquable outil.

Prédire les vols de voitures ?

Par FLORIAN GAUTHIER

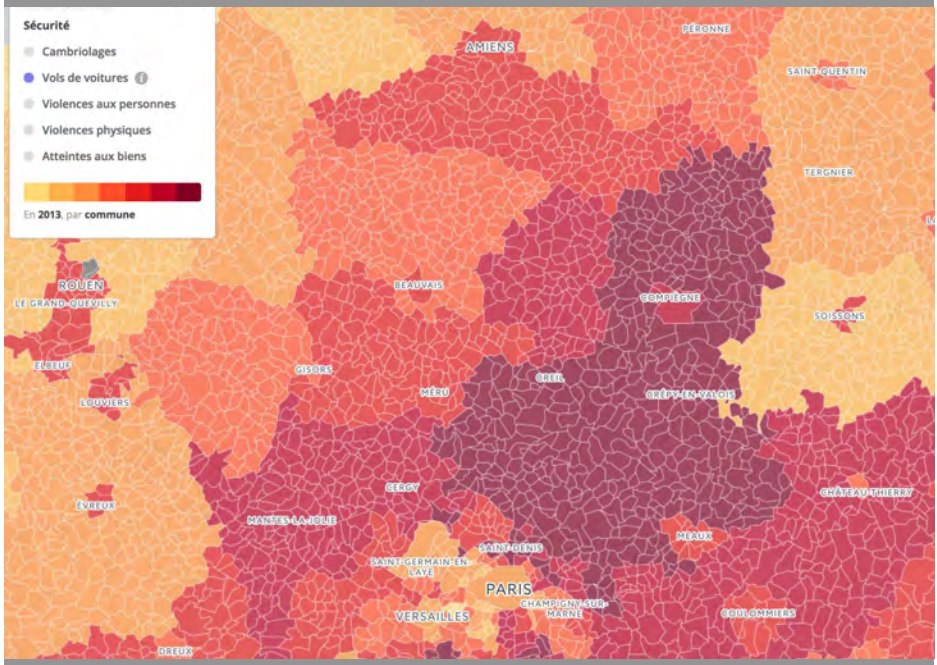
En 2015, l'équipe de l'Administrateur général des données au sein de la DINSIC a développé, en collaboration avec le Service des technologies et des systèmes d'information de la Sécurité intérieure (ST(SI)²), un modèle de prédiction des vols liés aux véhicules. Cette collaboration a permis de développer Predvol, un outil d'aide à la décision pour les policiers et les gendarmes, comprenant une prédiction quotidienne du risque de vol, une carte de l'historique des vols et une typologie des quartiers en fonction de la nature des infractions qui y sont réalisées.

FLORIAN GAUTHIER

Data-scientist - administrateur général des données. Secrétariat général pour la modernisation de l'action publique

Dès sa nomination au poste d'Administrateur général des gonnées (AGD) en septembre 2014, Henri Verdier a entrepris de constituer une équipe de *data-scientists* pour moderniser l'action publique en diffusant l'usage de la science de la donnée dans l'administration. Cette équipe, composée de quatre personnes, est elle-même intégrée à Etalab, au sein de Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC).

Dans ce cadre, un des premiers projets de l'AGD vit le jour lors d'une rencontre entre Etalab[1] et le service des technologies et des systèmes d'information de la sécurité intérieure -ST(SI)[2]. Les responsables de ce dernier, soucieux de tirer partie des avancées en matière de data-sciences, cherchaient un appui scientifique pour expérimenter des techniques d'apprentissage automatique (*machine learning)* sur un département. L'Oise, particulièrement exposée aux vols de voitures, réunissait les conditions pour lancer un projet.



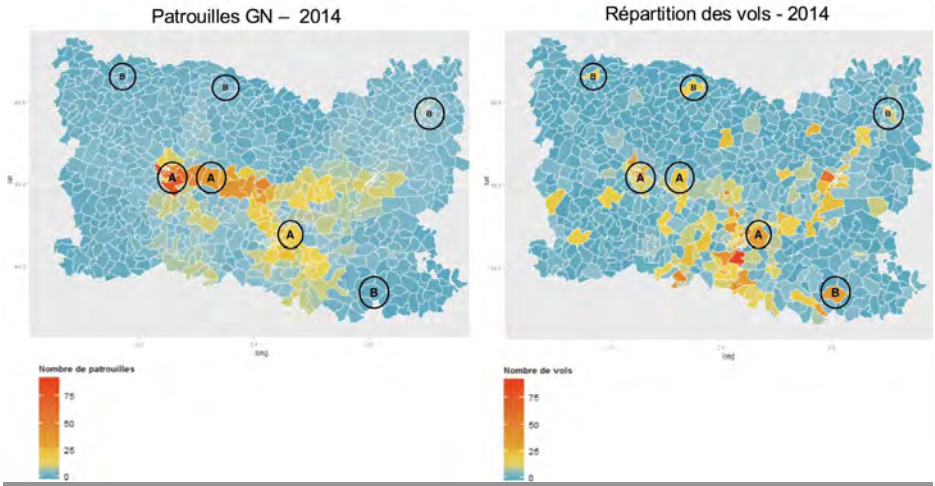
Datafrance

Carte des vols de véhicules dans l'Oise en 2015.

Définir une problématique claire est indispensable au démarrage d'un projet de datasciences. S'agissant des vols de voitures, nous sommes partis du constat suivant : un simple coup d'œil permet de s'apercevoir que certaines zones très surveillées par les forces de l'ordre montrent de nombreux vols de véhicules (zones A), tandis que d'autres, très touchées par les vols de véhicules, sont très peu empruntées par les patrouilles (zones B).

Dans quelle mesure serait-il possible d'anticiper les vols de voitures afin d'aboutir à une meilleure orientation des patrouilles de police et de gendarme ?

Afin de répondre à cette problématique, le ST(SI)^2 nous a transmis des données provenant directement des bases de dépôts de plaintes auprès de la police et de la gendarmerie : LRPPN et LRPGN. En tout, 3 ans d'historique de vols liés aux véhicules en ont été extraits. Chaque ligne



DataFrance

Une vision de l'adéquation des patrouilles aux zones de vols de voitures.

correspondait à une infraction définie par un lieu (coordonnées XY), une date ainsi que quelques informations - souvent manquantes - sur le véhicule volé.

Par ailleurs, un contact régulier avec les utilisateurs finaux s'est très vite imposé afin d'identifier précisément les problématiques des acteurs de terrain et leurs façons de travailler. Deux besoins très distincts ont tout de suite émergé :
1) Cibler les zones les plus à risques en amont de la patrouille,
2) Disposer d'un outil d'aide à la décision pendant la patrouille.

Sur le premier point, il convenait tout d'abord de définir un découpage géographique optimal afin d'entraîner nos algorithmes. Le découpage IRIS, proposé par l'INSEE et apportant le meilleur arbitrage taille/quantité de données disponibles, s'imposa comme le meilleur candidat. Ce dernier permit en effet d'enrichir notre base de données d'apprentissage avec plus de 600 variables socio-démographiques sur ces zones : taux de chômage, scolarisation des jeunes, nombre de commerces à proximité, âges moyens… Nous avons calculé d'autres indicateurs sur les circonstances temporelles des vols que nous avons ajouté à la base de données : Y-avait-il eu un vol la veille ? L'avant-veille ? Dans les quartiers voisins ? Quelle était la météo du jour ? …

Le principe est en effet d'amener, sans *a priori*, le maximum de variables dans notre base de données (ici plus de 650 variables) puis de laisser les algorithmes de *machine learning* sélectionner les meilleures prédicteurs pour anticiper les vols de voitures. Nous avons alors testé 3 grandes familles d'algorithmes afin d'anticiper au mieux, chaque jour, les vols liés aux véhicules dans les 799 quartiers de l'Oise :

Des algorithmes fondés sur une grande quantité de variables

Ces algorithmes figurent parmi les plus classiques de la littérature en matière de machine learning : régression logistique, forêts aléatoires, boosting, forêts aléatoires extrêmement randomisées, XGBoost… Ces algorithmes qui utilisent une très grande quantité de variables, sélectionnent les meilleurs prédicteurs en leur associant des poids et les utilisent pour tenter d'anticiper la variable d'intérêt.

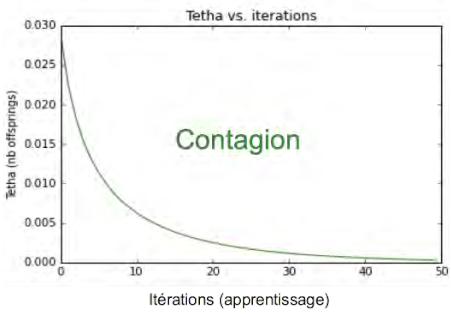
Les algorithmes de PredPol, une entreprise américaine connue dans ce domaine

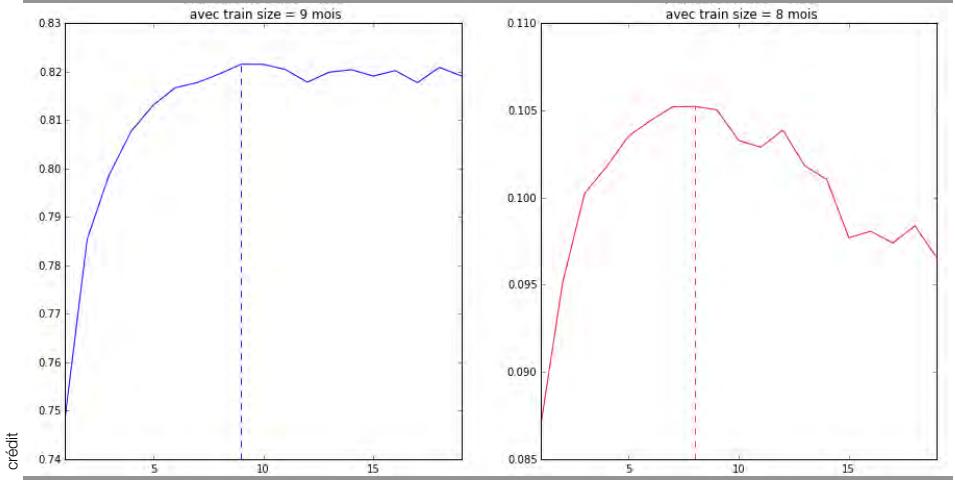
Revendiquant la première place en matière de predictive policing, la société PredPol utilise des algorithmes initialement développés par un sismologue français, David Marsan, afin de prédire les répliques des séismes. PredPol a fait l'hypothèse que les crimes se comportent comme les séismes :
- il existe un risque-terrain : des zones plus sujettes au crime (calculée en fonction de leur passé).
- les crimes entraînent des répliques (on parle d'effet de « contagion ») c'est-à-dire que lorsqu'il y a un crime dans une zone, la probabilité qu'il en survienne un autre dans une zone géographique proche est plus grande et décroît avec le temps.

Nous avons implémenté leurs algorithmes et les avons testés sur les vols liés aux véhicules, voici les résultats :

Deux constats :
Les vols de véhicules dans l'Oise n'ont pas de mémoire. Sur 1 000 vols, seuls 5 seraient issus d'une contagion.
Seuls le « risque terrain » du quartier est important.

Ce deuxième constat nous a alors conduits à tester notre troisième algorithme.





Cartes de chaleurs évolutives.

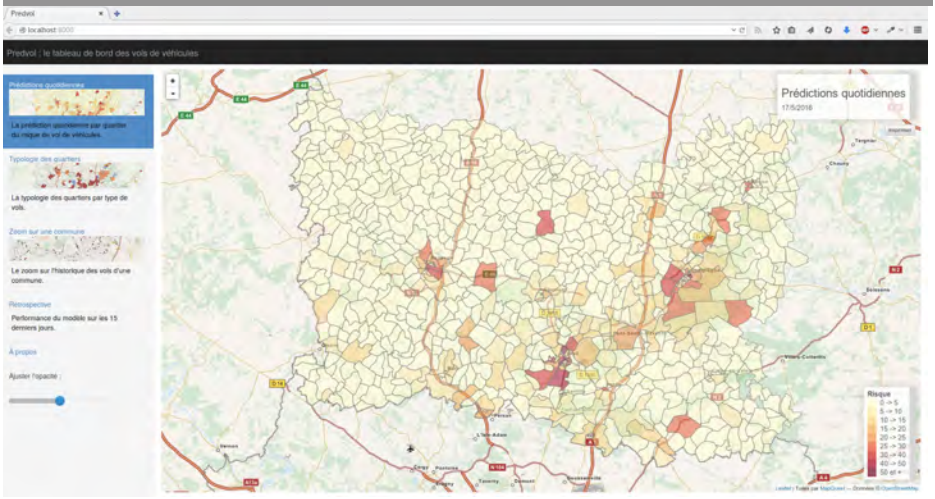
Les cartes de chaleurs évolutives

Une carte de chaleur est finalement exactement comme le modèle de PredPol sauf qu'on enlève la complexité du facteur de contagion. On prédira comme zone la plus risquée demain, celle dans laquelle ont été observés le plus de vols dans le passé. Il convient désormais de définir ce fameux « passé ». En effet, la technique des « punaises apposées sur la carte « infractions du dernier mois » est toujours couramment utilisée par la police et la gendarmerie. Notre idée ici était de tester l'historique optimal à utiliser afin d'obtenir la carte de chaleur prédictive la plus pertinente.

Nous avons comparé les différents historiques utilisés selon les deux facteurs clés d'un modèle prédictif : la capacité prédictive et la précision du modèle. Un historique trop petit (les fameuses punaises) pénalise grandement la capacité prédictive du modèle, tandis qu'un historique trop grand pénalise sa précision. Afin d'obtenir le meilleur ratio capacité prédictive / précision, la construction d'une carte de chaleur sur neuf mois serait le seuil optimal.

Une fois nos modèles construits, il s'agissait ensuite de les comparer. La méthodologie est très classique : les algorithmes ont été entraînés sur une partie de la base de données (la première année d'infractions) puis testés sur une seconde partie que les algorithmes n'avaient jamais vue (les deux dernières années). Les résultats furent sans appel.

Les modèles prédictifs donnaient tous d'excellents résultats : cibler en moyenne 10 % des quartiers prédits les plus risqués par le modèle permettait de couvrir 50 % des vols.
De plus, le modèle le plus simple (carte de



crédit

PredVol - Prédictions quotidiennes.

chaleur prédictive) permettait d'obtenir des résultats quasiment identiques aux modèles les plus complexes (celui de PredPol, notamment)

Simple is Beautiful. Cet adage bien connu prit alors tout son sens. Pourquoi ajouter un coût en complexité important lorsqu'on peut faire presque aussi bien avec un modèle simplissime ? Cela est d'autant plus vrai dès lors qu'on envisage d'intégrer nos travaux lors de la mise en production dans les systèmes d'information de l'État dont les environnements ne sont pas toujours prêts à recevoir des calculs complexes.

Une fois le modèle choisi, nous avons construit un outil baptisé « PredVol », optimisé pour un usage en mobilité (sur tablette), afin de rendre disponibles les résultats des prédictions journalières aux opérationnels de terrain. Nous avons doté « PredVol » de 3 onglets, l'un permettant de visualiser les quartiers prédits les plus risqués par le modèle, le second affichant une typologie des quartiers en fonctions des types de vols les plus présents et un troisième permettant de visualiser les faits passés sur une carte.

Côté Gendarmerie, l'outil a été intégré aux outils décisionnels et testé au sein de la compagnie de Compiègne à partir de mai 2016. Côté Police nationale, l'outil a été testé par les agents de la Direction départementale de la sécurité publique (DDSP)

de Beauvais et notamment par la Brigade anti-criminalité (BAC).
Pendant 6 mois d'expérimentation, nous avons eu l'occasion d'améliorer l'outil PredVol afin qu'il convienne au mieux aux usages opérationnels. Cette étape cruciale nous a par exemple permis, en patrouillant avec la BAC de Beauvais, de réaliser que les boutons de sélection étaient trop petits pour être utilisés dans les virages.
Après 6 mois d'expérimentation, nous avons réalisé que l'essentiel de l'attention des patrouilles se dirigeait non pas sur les prédictions quotidiennes, mais sur la simple visualisation des faits passés. En effet, si les prédictions - bien que toujours très performantes - ne permettaient que de confirmer les zones à risques connues par les opérationnels, la simple visualisation des faits (onglet 3) représentait un très net progrès dans leur usage quotidien.
Enfin, permettre aux agents du terrain de visualiser les faits qu'ils renseignent au moment des plaintes amorce un cercle vertueux : cela les encourage à recueillir des données de qualité, condition nécessaire - datascience ou pas - à l'obtention de résultats pertinents.

Différents tests sont encore à mener autour de ces sujets, notamment sur un visualiseur des découvertes de véhicules qui permettrait aux brigades d'orienter leurs recherches lorsqu'un véhicule est volé, en fonction de sa marque et de son modèle.

L'AUTEUR

Expert en approche de *machine learning*, Florian Gauthier travaille depuis 3 ans en tant que data-scientist auprès de l'Administrateur général des données sur des thématiques comme l'emploi et la sécurité intérieure. Il est diplômé de l'ENSAI en Big Data

kasdesign - Fotolia.com

UNE INTELLIGENCE ARTIFICIELLE POUR HAUSSER LE POTENTIEL DES FORCES DE SÉCURITÉ

L'Intelligence artificielle (IA) peut se concevoir comme une ingénierie de structuration, de transformation et d'exploitation des données, dédiée à une aide à la décision. L'exploitation par des algorithmes mathématiques d'informations multimodales permet de déceler des comportements illégaux et de mettre en évidence des signaux faibles, précurseurs d'événements graves. Cela entre dans une stratégie de compréhension et d'anticipation préventive ou judiciaire de la criminalité. En matière de sécurité publique générale, une célérité d'analyse et une réduction des tâches chronophages liées au traitement de l'information, renforce le contact humain entre les forces de sécurité et la population tout en accroissant la qualité de la réponse opérationnelle en matière de lutte contre une criminalité transverse et diffuse. En matière d'intervention comme d'ordre public, l'IA accroit la perception de l'environnement de l'événement et permet d'augmenter, lors de la conduite des actions, la sécurité des personnels et du public. De même, il est évident que son application aux transports intelligents devrait à court terme modifier les méthodes de lutte contre l'insécurité routière.

Il est toutefois indispensable que le législateur définisse son cadre légal et éthique. Le contrôle par des magistrats spécialisés, garants des libertés individuelles, et une transparence des modèles mathématiques utilisés lèveraient les préventions émises quant au développement de l'intelligence artificielle dans un domaine régalien.

L'intelligence artificielle
au service de la sécurité : enjeux et perspectives

Par PATRICK PERROT

Qui aujourd'hui peut négliger l'intelligence artificielle (IA) tant elle est présente dans de nombreux domaines d'application. Marketing, finance, médecine, industrie, grande distribution, il n'est pas un secteur d'activité qui échappe à ce nouvel engouement. Stephen Hawkins, Bill Gates, Elon Musk, Mark Zuckerberg se prononcent sur l'irrémédiable imprégnation de l'IA dans nos vies quotidiennes au risque même de la voir transgresser notre humanité.

PATRICK PERROT

Colonel de gendarmerie - commandant le groupement de gendarmerie départementale de la Haute Marne

Nombreuses sont les questions qui se posent, mais tout autant les perspectives ouvertes par une discipline dont nous ne pouvons garantir le devenir.

Quoiqu'il en soit, ce sont bien les germes d'une nouvelle révolution qui apparaissent : industrielle pour les uns, sociétale pour les autres. Mais, comme le souligne Cédric Villani, « l'*intelligence artificielle est l'affaire de tout le monde* ». Les forces de sécurité intérieure peuvent-elles alors ignorer l'émergence de l'IA dans la lutte contre une délinquance en évolution croissante ? Parce que l'anticipation est aujourd'hui essentielle dans la lutte contre la criminalité, il est indispensable de s'interroger sur les principes de l'IA, ses applications dans le domaine de la sécurité comme son impact sur la législation.

L'IA : du principe aux perspectives

Souvent présenté comme le décodeur d'Enigma, le code de chiffrement exploité par les Allemands durant la Seconde Guerre mondiale, le mathématicien Alan Turing propose, en 1950, un article qui tend à évaluer si une machine est capable d'intelligence et de rivaliser avec l'humain à travers « *le test de Turing* ». Simple d'apparence, il a longtemps posé les bases du

concept de l'IA dont le nom n'apparaîtra qu'en 1956 à la suite d'une université d'été organisée par les scientifiques John Mc Carthy et Marvin Lee Minsky. Ils ignoraient alors que ce nouveau concept allait perdurer et bouleverserait le siècle à venir. Aujourd'hui, l'objectif de l'IA n'est plus seulement de rivaliser avec l'homme. Ce challenge est déjà largement relevé dans de nombreux domaines, notamment la mémorisation et le traitement (distribution et parallélisation des calculs) des données mais aussi la célérité de restitution des résultats. La rencontre de l'afflux des données, des capacités de stockage et de calcul et l'apport de nouvelles méthodes algorithmiques démultiplient les perspectives et les champs d'application.

Le socle de l'IA repose sur le principe de l'apprentissage. La norme ISO 2382-28 définit l'IA comme « *la capacité d'une unité fonctionnelle à exécuter des fonctions généralement associées à l'intelligence humaine, telles que le raisonnement et l'apprentissage* ». L'homme développe au cours de sa croissance de nombreux apprentissages qui génèrent des capacités de raisonnement déductif, inductif ou abductif : apprentissage de la langue, de la marche et des codes comportementaux. L'apprentissage du point de vue de l'IA est automatique et regroupe de nombreuses méthodes mathématiques cherchant à inférer de la connaissance sur les données. Il se décline en général sous trois formes :

- Apprentissage supervisé : il consiste à apprendre des modèles à partir d'une base étiquetée préalablement. Une nouvelle entrée sera affectée au modèle le plus proche par une règle probabiliste.

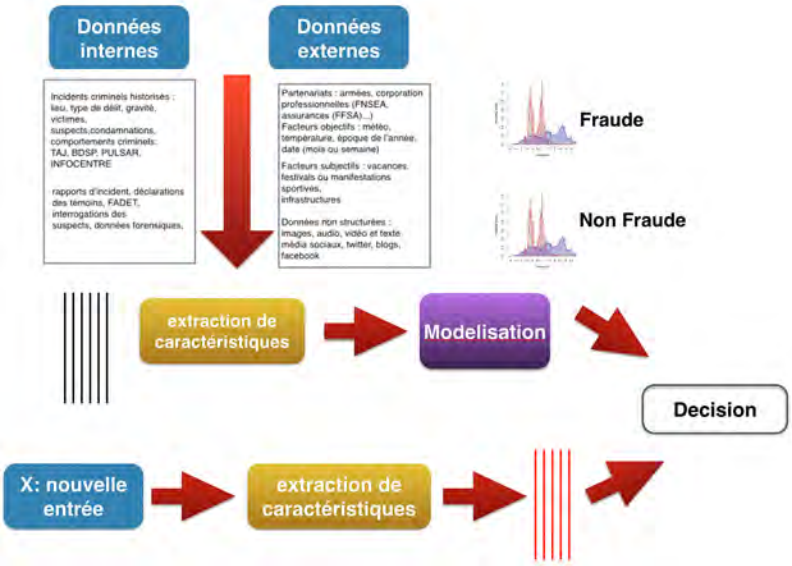
- Apprentissage non supervisé : il consiste à regrouper sans a priori les données les plus similaires au sein d'un même groupe tandis que des données différentes (au sens d'une métrique établie) rejoignent des groupes distincts. Ainsi, à partir d'une nouvelle entrée, la distance minimale d'un des groupes permettra de l'affecter et donc de la caractériser.

- Apprentissage par renforcement : cette technique s'appuie sur le principe global de l'apprentissage en rajoutant une fonction d'optimisation d'une récompense quantitative au cours du temps.

Synoptique d'apprentissage automatique

Les méthodes mathématiques, au travers notamment des réseaux neuronaux (qui ne sont pas récents puisque le premier perceptron[1] est apparu à la fin des années cinquante) mais aussi de l'apprentissage profond (*Deep Learning*) actuellement très en vogue et

(1) Le perceptron est un algorithme d'apprentissage supervisé de classifieurs binaires, c'est-à-dire séparant deux classes.



crédit

Synoptique d'apprentissage automatique

demain de l'apprentissage quantique (*Quantum Learning*), témoignent de belles performances. L'IA doit se voir comme une ingénierie de la connaissance comprenant des étapes de collecte, de structuration, d'exploitation et de transformation des données, préalables à la mise en œuvre d'une aide à la décision. Certes, elle demeure, même par ses concepteurs, encore bien difficile à appréhender. Les raisons qui expliquent par exemple les performances en terme de généralisation des réseaux de neurones profonds (*Deep Learning*) sont encore en partie à élucider. Par ailleurs, ces techniques révèlent de très bonnes aptitudes d'identification et de reconnaissance mais montrent aussi des faiblesses de compréhension. Nul doute que les travaux actuels en apprentissage quantique démultiplieront encore les possibles en accélérant considérablement la vitesse de calcul mais aussi en permettant la multiplication des états pour une même tâche, se rapprochant ainsi de plus en plus des capacités cognitives humaines. Nous ne pouvons, dans les années à venir,

occulter la potentialité de l'IA au risque d'être totalement incapables de traiter objectivement et de la manière la plus complète possible la donnée.

L'IA dans la lutte contre la délinquance

Face à la diversité des formes de délinquance, à la multiplication des déterminants expliquant l'insécurité, l'IA offre des capacités indéniables d'optimisation de l'efficacité des forces de sécurité. Que la délinquance soit commune ou organisée, l'explosion du numérique modifie considérablement la cartographie criminelle en termes de protection des biens matériels, virtuels ou des personnes. Les forces de sécurité intérieure doivent adopter une approche proactive pour exploiter des informations multimodales caractérisant des comportements prédéfinis et mettre en évidence des signaux faibles, précurseurs d'occurrences plus graves. Les données sont aujourd'hui disponibles au travers de formats très hétérogènes : données de géolocalisation, tweet, SMS, communications sur les réseaux sociaux, données d'environnement physique, analyses de faits précédents, contextes socio-économiques, images, vidéos. Dès lors, il serait opportun d'exploiter ce patrimoine à des fins de compréhension et d'anticipation préventive ou judiciaire de la criminalité.

En matière de sécurité publique générale, l'IA s'inscrit parfaitement dans la volonté d'accroître le contact humain entre les forces de sécurité et la population. Capable de proposer une exploitation massive des données, une célérité d'analyse et l'exécution de tâches consommatrices de temps, elle libère des plages horaires pour renforcer le contact humain et la proximité. Les travaux déployés dans le domaine de l'analyse prédictive participent à une meilleure prévention en permettant d'estimer le risque d'infractions sur des périodes et des espaces géographiques probables et donc en orientant l'action de contact. L'objectif n'est en aucune façon, comme une vulgarisation excessive tend à le faire accroire, d'envisager une quelconque préemption ciblée sur les individus par rapport à l'exploitation d'antécédents mais bien d'exploiter l'observation de faits antérieurs.

Dans le domaine du renseignement, qui repose essentiellement sur la fonction « connaissance - anticipation », l'IA offre des perspectives qui pourraient révolutionner les applications. L'analyste qui, au quotidien, lit les messages pour en effectuer une classification que nous qualifierons de manuelle ne peut plus faire face à l'afflux d'un déluge de données. L'exploitation automatique de données de masse, notamment en sources ouvertes, génère des possibilités jamais égalées d'enrichir les analyses. Exploiter des données de formats divers issues de drones, de la vidéosurveillance, de Tweet ou de comptes FaceBook est non seulement possible mais

réalisable dans un temps limité. La prise en compte d'informations périphériques ouvre ainsi de nouvelles hypothèses d'action par anticipation. L'IA permet d'analyser de nombreuses données en temps réels de façon parallèle et d'aider à la décision par la mise en place d'alertes sur des éléments déterminés au préalable, qualifiés généralement de signaux faibles.

En matière judiciaire, sous la direction d'un magistrat, les investigations peuvent par l'intelligence artificielle prendre de nouvelles formes. L'objectif est de matérialiser objectivement la commission d'infractions mais aussi d'anticiper l'activité criminelle et de la proscrire par des actions en flagrant délit. Il est par exemple possible de suivre l'évolution de criminels en temps réels en exploitant des sources de données structurées comme non structurées. Ainsi, le tissu relationnel de la personne soupçonnée, son environnement géographique, virtuel, ses zones et centres d'intérêt mais aussi le contexte dans lequel elle vit peuvent être analysés de manière globale et simultanée pour en extraire de l'information pertinente. On pourra alors faire appel à des méthodes d'apprentissage dans le domaine de la reconnaissance faciale à partir de vidéos ou d'images. Elles peuvent être étendues aux textes non structurés (Tweet, courriel, sms), aux documents audio en exploitant des enregistrements sonores à des fins de reconnaissance de la parole, à l'analyse des réseaux sociaux et à l'exploitation des données spatiales. En matière d'intervention comme d'ordre public, la capacité d'exploitation massive de données hétérogènes comme la célérité de l'analyse permettent d'accéder à des hypothèses en quasi temps réel et donc de conduire les actions en toute objectivité tout en améliorant la sécurité des personnels et du public. La perception de l'évolution d'une manifestation et la simulation d'actions entreprises pourront être combinées pour mieux anticiper les mouvements de l'adversaire. Par ailleurs, la détection des états émotifs, dont les performances peuvent encore s'accroître, pourra aider à la prise en compte des appels d'urgence mais aussi faciliter une négociation en affinant par exemple l'évaluation de l'état psychologique d'un forcené.

En matière de sécurité routière, l'IA permettra une analyse automatique de facteurs, dédiée à une meilleure compréhension des causes comme de la distribution des accidents, mais aussi de s'assurer de la pertinence et de l'influence des mesures de prévention ou de répression. Le futur des transports, autour du véhicule connecté comme des transports intelligents, devrait à court terme modifier les méthodes actuelles de lutte contre l'insécurité routière.

La question éthique et juridique

Nombre de questions se posent dès lors que le terme d'intelligence artificielle est prononcé et de surcroît associé à une

activité de sécurité. Il convient néanmoins de garder raison et d'examiner les impacts possibles sur les libertés individuelles.

Les risques d'une exploitation détournée de l'IA existent et le nier serait une erreur fondamentale. C'est d'ailleurs pour cela qu'il est indispensable que les organes étatiques comprennent le sujet et s'en emparent pour l'exploiter en toute légalité et dans un cadre éthique. Se détourner des méthodes d'IA laisserait le champ libre à des utilisations malveillantes et sans contrôle.

Parmi les risques exposés, l'un des principaux réside dans la collecte et le traitement des données à caractère personnel. Pourtant cette question ne devrait pas en être une tant les processus de protection des libertés individuelles sont ancrés dans la culture policière et tant sont traçables les étapes algorithmiques. Dès lors que l'exploitation s'effectue dans un cadre judiciaire, c'est-à-dire sous le contrôle d'un magistrat, la garantie du respect des libertés individuelles est peu contestable, l'article 66 de la constitution du 4 octobre 1958 posant l'autorité judiciaire comme gardienne de la liberté individuelle.

Dans le cadre des activités de renseignement comme de sécurité publique, l'intérêt de l'IA est d'anticiper des faits et des phénomènes. A titre d'exemple, il est possible de modéliser les caractéristiques des distributeurs automatiques de billets et d'estimer le risque pour un nouvel automate d'être l'objet d'une tentative d'arrachement ou d'attaque à l'explosif. Il est possible de modéliser sans les nommer les entreprises victimes de faux ordres de virement et d'estimer celles qui pourraient le devenir. Il est possible encore d'estimer des zones propres au développement de certaines formes de délinquance sans s'intéresser aux délinquants eux-mêmes. Les exemples d'applications qui n'exploitent en aucune façon des données à caractères personnels ne manquent pas.

La notion de transparence est régulièrement soulevée par ceux qui craignent une exploitation peu scrupuleuse de l'IA par les services de l'État. D'une façon générale, les méthodes mathématiques utilisées à ce jour dans le domaine de l'IA ne sont en aucune façon secrètes. Elles font l'objet de publications scientifiques qui ne sont certes pas à la portée de tous mais qui sont parfaitement analysables par des experts. Dès lors, la question est plus à orienter vers les données exploitées. Il s'agit d'une problématique déterminante qui renvoie à la nécessité de disposer, à l'instar des entreprises, d'un cadre en charge des données, le *chief data officer* et d'un référent « libertés individuelles » comme c'est déjà le cas dans nombre d'unités de gendarmerie.

Du point de vue sociétal, l'IA, en dépit des débats qu'elle suscite, ne devrait pas s'arrêter et les développements en cours, qui combinent la physique quantique aux méthodes d'apprentissage, apporteront des capacités démultipliées. En matière de sécurité, elle doit être utilisée à des fins de renforcement et de complémentarité des actions entreprises. Elle est créatrice de valeur, de qualité, d'efficacité opérationnelle et accroît considérablement les capacités décisionnelles dès lors qu'elle est exploitée à bon escient au sein d'un cadre juridique précis.

L'AUTEUR

Colonel de gendarmerie, Patrick Perrot dirige le groupement de gendarmerie départementale de la Haute Marne. Il a alterné des postes opérationnels et des fonctions de nature scientifique au sein du PJGN. Auteur de nombreuses publications dans le domaine des sciences forensiques et du renseignement, il est ingénieur de formation et titulaire d'un doctorat de Télécoms Paris Tech.

Blueby2014 - Adobe Stock

LE DANGER DU PASSAGE D'UNE ALGORTHMIE PRÉDICTIVE À UNE FORME PRESCRIPTIVE

La psychométrie est une branche de la psychologie consacrée aux tests, à leur construction et à leur utilisation. Elle peut s'appliquer, *via* une algorithmie convenable, à l'accumulation de données personnelles liée à l'utilisation des objets réels ou virtuels qui laisse une empreinte de nos habitudes, de nos choix culturels, esthétiques et de valeurs sur la toile. Des déductions fiables peuvent être faites de ces simples actions en ligne. L'examen des choix que nous faisons lors de nos interventions sur les réseaux sociaux est une mine d'informations. Des algorithmes spécialisés permettent d'évaluer le profil psychologique d'une personne, de prédire son comportement et de lui conférer un poids dans un traitement. Ils donnent la possibilité de sérier une population en segments homogènes qui constituent autant de cibles commerciales, électorales ou susceptibles d'être approchées par des groupes d'intérêts. Un moteur de recherche d'individus pourrait-il servir de vecteur à une manipulation généralisée avec des algorithmes qui passeraient inéluctablement du prédictif au prescriptif ?

Algorithmes prédictifs :
au cœur de la politique ?

Par JEAN-PAUL CRENN

Le psychologue Michal Kosinski[1] a développé une méthode pour prédire les comportements individuels à partir de Facebook. Aurait-il propulsé Donald Trump à la Présidence des Etats-Unis ?[2]

Le 9 novembre 2016, Michal Kosinski, 34 ans, apprend comme nous tous la nouvelle, encore incroyable quelques mois auparavant et en contradiction avec toutes les prévisions des instituts de sondage : Donald J Trump est devenu le 45e président des Etats-Unis. Mais lui, chercheur renommé en psychométrie, a le sentiment qu'il y est peut-être pour quelque chose.

JEAN-PAUL CRENN

Directeur de VUCA Strategy - Société de conseil spécialisée dans la transformation digitale et le e-commerce

Au même instant, une société britannique quasi-inconnue publie un communiqué de presse triomphal : « *Nous sommes heureux que notre approche révolutionnaire de la communication gérée par la donnée ait joué un tel rôle dans la victoire extraordinaire du président élu Trump* ». Une citation de son président, Alexander James Ashburner Nix.

De ces trois personnes, Kosinsky songeur, Nix triomphal et Trump souriant, l'un a permis la révolution des algorithmes prédictifs basée sur la psychométrie, l'autre sa mise en œuvre et le dernier en a sans doute tiré parti.

Si les algorithmes font partie de notre quotidien, la psychométrie l'est moins. Il s'agit d'une branche de la psychologie consacrée aux tests, à leur construction

(1) Site de Michal Kosinski avec son CV, ses publications, conférences : http://www.michalkosinski.com/

(2) Nos deux principales sources d'information sont : https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ et https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win pour lesquelles nous avons validé les sources d'information primaires.

et à leur utilisation. En 1961, Ernest Tupes et Raymond Christal[3] sont les premiers à avoir avancé un modèle théorique basé sur la description de cinq grands facteurs de personnalité (appelés Big Five) s'inspirant des travaux réalisés au sein du laboratoire du personnel de l'U.S. Air Force à la fin des années 50. Ce modèle évolue à partir de 1981 avec les travaux du psychologue Lewis Goldberg[4] et de ceux de John Digman[5] pour préciser un concept connu sous l'acronyme d'OCEAN. Ce modèle ne classe pas les individus selon 5 catégories mais les évalue cinq fois différemment, selon 5 dimensions :

O pour Ouverture : êtes-vous ouvert à de nouvelles expériences ? Appréciez-vous l'art, les idées originales, faites-vous preuve d'imagination, de curiosité… ?

C pour Conscienciosité : êtes-vous méthodique, fiable, ponctuel, respectez-vous facilement les obligations, faites-vous preuve de conscience professionnelle… ?

E pour Extraversion : recherchez-vous la stimulation et la compagnie d'autrui ? Êtes-vous une personne énergique… ?

A pour Agréabilité : avez-vous une propension à être compatissant et coopératif plutôt que soupçonneux et antagonique ?

N pour Névrosisme : (on parle également de stabilité émotionnelle) Avez-vous une tendance à éprouver facilement des émotions désagréables telles que la colère, l'inquiétude, la dépression… ?

Avec une évaluation de ces 5 dimensions vous décrivez le caractère d'une personne. Vous évaluez également ses besoins et son comportement probable. Les Big Five sont devenues l'un des standards techniques de la psychométrie et sont régulièrement utilisées par les professionnels du recrutement. La difficulté et la limite de cette approche ont été le recueil de données car il nécessite de renseigner des questionnaires détaillés, compliqués, posant des questions très personnelles.

Puis arriva le Web, Facebook et… Kosinski.

Michal Kosinsky est d'origine Polonaise. Etudiant en Psychologie à Varsovie, il est accepté en 2008 à l'Université de Cambridge pour réaliser un doctorat au Centre de Psychométrie, l'une des plus anciennes institutions dans ce domaine au niveau mondial[6]. Kosinski rejoint un autre doctorant, David Stillwell[7], qui avait lancé en juin 2007 une application Facebook,

(3) Tupes, E.C., Christal, R.E.; "Recurrent Personality Factors Based on Trait Ratings," Technical Report ASD-TR-61-97, Lackland Air Force Base, TX: Personnel Laboratory, Air Force Systems Command, 1961 : http://www.dtic.mil/dtic/tr/fulltext/u2/267778.pdf

(4) Goldberg, L.R. (1993). The structure of phenotypic personality traits. American Psychologist, 48, 26-34. http://psycnet.apa.org/doiLanding?doi=10.1037%2F0003-066X.48.1.26

(5) Digman, J.M., "Personality structure: Emergence of the five-factormodel," Annual Review of Psychology, 41, 417-440, 1990. http://www.annualreviews.org/doi/abs/10.1146/annurev.190.002221

(6) Site du Centre de Psychométrie de l'Université de Cambridge : https://www.psychometrics.cam.ac.uk/

(7) Site de David Stillwell avec son CV, ses publications, conférences : http://www.davidstillwell.co.uk/

(8) Page actuelle de myPersonality Project : http://mypersonality.org/wiki/doku.php

(9) 6 millions de tests pour plus de 4 millions de profils Facebook.

quand ce réseau social était balbutiant. Cette application, baptisée myPersonality[8], permettait aux utilisateurs de compléter différents questionnaires de psychométrie, dont des questions liées aux Big Five. Les répondants pouvaient partager leurs données personnelles Facebook avec les chercheurs puis recevoir gratuitement leur profil psychologique. Les doctorants s'attendaient à quelques dizaines de répondants mais ce sont des millions de personnes qui se sont prises au jeu de myPersonality[9], créant la plus grande base de données combinant des scores psychométriques avec des profils Facebook. Kosinsky et ses collègues travaillèrent alors sur cette base pour l'enrichir, au travers de questionnaires afin de détecter des corrélations entre les comptes Facebook et les traits du Big Five.

Des déductions fiables purent alors être déduites de ces simples actions en ligne. Par exemple, les hommes qui *likent* la marque de cosmétiques MAC étaient légèrement plus susceptibles d'être homosexuels. L'un des meilleurs indicateurs d'hétérosexualité étant le fait de *liker* le groupe de hip hop Wu-Tang Clan. Les *followers* de Lady Gaga étaient probablement des extravertis, tandis que ceux qui « *likaient* » la Philosophie tendaient à être des introvertis.

En 2012, Kosinski et ses collègues arrivent à prouver qu'avec l'analyse de 68 *likes* sur Facebook, il est possible de prédire la couleur de peau (avec un degré de confiance de 95 %), l'orientation sexuelle (88 % de confiance) et l'affiliation au parti républicain ou démocrate (85 % de confiance). religion, consommation d'alcool, de cigarettes, usage de drogues… peuvent également être déterminés.

Avec l'analyse de 300 de vos *Like* sur Facebook, l'algorithme vous connait mieux que votre conjoint

La force de ce modèle est illustrée par sa capacité à prédire les réponses du sujet. C'est là que les algorithmes prédictifs interviennent. Les algorithmes de Kosinski et de son équipe sont capables d'évaluer le profil psychologique d'une personne et ainsi de prédire son comportement, mieux que ses collègues de travail sur la base de l'analyse de 10 *Like* sur Facebook. 70 *Like* sont suffisants pour en savoir plus que les amis de la personne, 150 ses parents, 300 son conjoint. Plus de *Like* peuvent même surpasser ce qu'une personne pense savoir… d'elle-même.

Le 27 janvier 2015, Michal Kosinski et ses collègues David Stillwell et Wu Youyou publient les résultats de ces recherches dans les *Proceedings of the National Academy of Sciences of the United States*

(10) http://www.pnas.org/content/112/4/1036.full.pdf . Pour une synthèse : http://www.cam.ac.uk/research/news/computers-using-digital-footprints-are-better-judges-of-personality-than-friends-and-family

(11) https://apply-magicsauce.com/

of America[10] (PNAS). Ce jour-là Kosinski reçoit deux appels téléphoniques : l'un le menaçant d'une poursuite judiciaire, l'autre lui proposant un emploi, les deux provenant de Facebook.

Quelques semaines plus tard, les *likes* de Facebook, publics par défaut, devinrent privés par défaut... Mais cela n'empêche pas la collecte de données personnelles. Par exemple, pour obtenir un test de personnalité gratuit basé sur vos *likes* Facebook, un accès aux données personnelles est exigé. Vous pouvez d'ailleurs réaliser le test de Kosinsky encore aujourd'hui via une nouvelle application : Apply Magic Sauce[11].

Kosinsky et son équipe réalisèrent très rapidement qu'ils avaient ouvert la boîte de Pandore car ils pouvaient aller encore bien plus loin. Ils pouvaient attribuer des valeurs « Big Five » simplement à partir du nombre d'images de profils qu'une personne possède sur Facebook ou du nombre de ses contacts.

Ils constatèrent que nous révélons bien des aspects de notre personnalité quand nous ne sommes même pas en ligne, par exemple *via* le capteur de mouvement de notre smartphone. Ce dernier révèle notre vitesse et nos distances de déplacement, données corrélées à notre niveau d'instabilité émotionnelle, le « N » d'OCEAN. Pour Kosinsky notre smartphone est un questionnaire que nous remplissons constamment, consciemment et inconsciemment.

Ainsi les Big Five deviennent finalement réellement opérants grâce aux masses de données personnelles liées à l'utilisation des objets réels ou virtuels du Digital. Cela fonctionne également de façon inverse et c'est là que cela devient très intéressant. Non seulement un profil psychologique peut être créé à partir de nos données et ainsi permettre de déduire nos comportements probables mais nos données peuvent aussi être utilisées pour, à l'inverse, rechercher un profil spécifique. Les maris jaloux, les introvertis pétris de haine ou… des électeurs hésitants !

Kosinsky avait inventé un « moteur de recherche d'individus »…Et il devint inquiet.

Si le Web est un superbe espace pour créer de la connaissance c'est également un espace de manipulation. Son moteur de recherche d'individus servirait-il à les manipuler ? Il ajouta alors des avertissements à la plupart de ses publications. Son approche prévint-il « *pouvait être une menace au bien-être, à la liberté et même à la vie des individus* »[12].

C'est à cette époque, début 2014, que Kosinski est approché par un jeune professeur assistant du département de

psychologie, Aleksandr Kogan[13] qui lui dit qu'une société est intéressée par sa méthode et souhaite avoir accès à la base de données *myPersonality*. Kogan ne peut, pour des raisons de clauses de confidentialité, fournir ni l'objectif de la démarche, ni le nom de cette société. Dans un premier temps Kosinsky et ses collègues regardent cette demande avec intérêt car cela peut signifier un gros budget pour leur département. Ils hésitent car ils ne voulaient pas que leurs travaux tombent dans des mains mal intentionnées. Finalement, selon Kosinsky[14], Kogan révéla le nom de l'entreprise mandataire. Il s'agissait de SCL (*Strategic Communication Laboratories*)[15]. Kosinski se renseigne alors sur cette entreprise. SCL, fondée par Nigel Oakes[16], ex-patron de boîte de nuit passé par la publicité *via* Saatchi & Saatchi, s'avère être la société mère d'un groupe diffus d'entreprises et son actionnariat l'est encore plus. La mission de SCL : la gestion d'élection. SCL a été impliquée dans des élections de l'Ukraine, du Nigéria en passant par la lutte contre les rebelles par la monarchie népalaise. En 2013, SCL créait une société fille, Cambridge Analytica, pour proposer ses services lors des élections américaines.

Kosinski confie dans une interview au magazine suisse Dasmagasin : « *Tout cela commençait à sentir mauvais* » car au cours de ses recherches sur SCL, il se rend compte qu'Aleksandr Kogan avait créé une entreprise en affaire avec celle-ci et, selon un article de The Guardian publié en 2015[17], il apparaît que SCL aurait connu les méthodes de Kosinski au travers de Kogan. Kosinski fut amené à penser que l'entreprise de Kogan pourrait avoir reproduit l'outil de mesure des « Like » Facebook, basé sur les Big Five, pour le vendre à SCL. Il coupa immédiatement les contacts avec Kogan et en référa à sa hiérarchie au sein de l'Université, ce qui déclencha une crise inhabituelle dans l'univers feutré de Cambridge. Kogan alla à Singapour, se maria et changea de nom pour devenir le Docteur Spectre. Kosinski termina son doctorat, reçu une offre de l'université de Stanford puis alla s'installer aux USA.

En novembre 2015, le nom de Cambridge Analytica, la filiale de SCL, fut associé au camp des Pro-Brexit puis arriva le 19 septembre 2016, juste 1 mois avant les élections aux USA. Lors du Concordia Summit,

(13) Son CV, sous sa nouvelle identité (Kogan Spectre) : http://cpwlab.azurewebsites.net/CV/AleksandrKogan CV Website.pdf

(14) Sources : https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win et https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

(15) Site SCL : https://sclgroup.cc/home

(16) Article du Guardian sur Nigel Oakes avec un développement sur le rôle de SCL/Cambridge Analytica dans le Brexit et l'élection de Trump : https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump

(17) https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

(18) Vidéo de son intervention sur Youtube : https://www.youtube.com/watch?v=n8D-d5aVXLCc

à New York, apparaît le nouvel homme de la stratégie digitale de la campagne de Trump. Il s'agit d'Alexander Nix, le président de Cambridge Analytica[18].

« Nous avons un profil psychométrique pour chaque adulte aux Etats Unis d'Amérique »

Alexander Nix y explique comment, grâce à la psychométrie, aux Big Five et au modèle OCEAN, Cambridge Analytica a pu faire gagner à un candidat Républicain pratiquement inconnu, Ted Cruz, le caucus de l'Iowa[19] avant que ce dernier ne renonce. Nix y déclare : « *Nous avons un profil psychométrique pour chaque adulte aux Etats Unis d'Amérique – 220 millions de personnes* » et il présente comment il peut envoyer un message personnalisé à chaque citoyen américain afin d'influencer son vote. Il y explique pourquoi la méthode traditionnelle basée sur l'envoi de messages liés à des données socio-démographiques n'a plus d'avenir. Il y expose comment le fait d'avoir acheté une voiture *made in USA* anticipe un vote Trump, comment faire pour détecter les électeurs hésitants et les faire renoncer, *via* des publicités sur Facebook ou du démarchage à domicile, s'ils pourraient aller voter contre votre candidat. Dans une interview, Nix déclarera par la suite : « *Pratiquement chaque message de Trump était basé sur l'analyse de la donnée* ». Ceci viendrait corroborer ce que la mathématicienne Cathy O'Neil avait observé en août 2016[20] : Trump se comportait comme un algorithme parfaitement opportuniste. Les incohérences et contradictions de Trump auraient été « *gérées* » afin de lui permettre d'apporter une réponse à chacun des micro-segments de son électorat.

(19) Le caucus de l'Iowa est un événement électoral pendant lequel, au cours d'un caucus (réunion de sympathisants d'un parti) , les habitants de l'État américain de l'Iowa votent pour le parti politique qu'ils soutiennent, leurs délégués pour la convention de comté à laquelle leur circonscription appartient.

(20) https://mathbabe.org/2016/08/11/donald-trump-is-like-a-biased-machine-learning-algorithm/

Jusqu'à quel point les élections américaines ont-elles été gagnées *via* des algorithmes prédictifs basés sur la psychométrie ? Jusqu'à quel point Cambridge Analytica, étant du côté du vainqueur, s'en attribue les mérites ? Jusqu'où les théories du complot affectent-elles les sources des informations, les analyses des journalistes ? Ce qui est certain c'est que Cambridge Analytica ne souhaite pas fournir de preuves de l'efficacité de son action dans la campagne de Trump. Peut-être parce que c'est impossible. Il existe cependant un faisceau d'indices permettant de penser que les algorithmes prédictifs, basés sur la psychométrie, ont joué un rôle dans l'élection de Trump :

– la qualité prédictive des travaux de Kosinski et de ses collègues, qui n'est pas contestée dans le domaine de la recherche,

– l'investissement de l'équipe de cam-

pagne auprès de Cambridge Analytica utilisant des algorithmes proches de ceux de Kosinski,

– la progression surprenante de Ted Cruz pendant les primaires,

– le surinvestissements de Trump dans le digital plutôt que dans des campagnes télévisées, au contraire de Clinton,

– la sur et sous-représentation flagrante de certains types d'électorats lors de cette dernière élection, par rapport à l'ensemble des élections précédentes,

– le fait que, selon les membres de la campagne de Trump, Facebook ait été au cœur du succès de leur campagne.

Influencer l'opinion publique est l'objectif de toute campagne politique et celles qui réussissent sont sans doute celles qui utilisent le mieux les meilleurs outils à leur disposition. Ces outils s'avèrent de plus en plus basés sur des algorithmes et là où les campagnes politiques creusent le sillon, les entreprises suivent. Les équipes de Trump n'auraient-elles fait que mieux utiliser les dernières générations d'outils, c'est-à-dire les algorithmes prédictifs basés sur les données de la psychométrie, que celles de Clinton ? C'est probable. Déjà, les outils de demain se construisent. Les algorithmes prédictifs, alliés à la psychométrie, ont rendu opérants les Big Five et le modèle OCEAN grâce la multitude d'empreintes digitales laissées par les utilisateurs. Avec l'émergence inéluctable de l'Internet des Objets et de la croissance algorithmique du nombre et de la diversité de ces empreintes digitales, nous ne sommes clairement qu'au début d'une nouvelle ère du traitement des données, avec des algorithmes qui passeront inéluctablement du prédictif au prescriptif. Par ailleurs Kosinski vient de publier[21] une nouvelle étude qui fait grand bruit : la reconnaissance faciale permet de détecter nos préférences sexuelles, notre QI ou nos opinions politiques. Laissons-lui le dernier mot :

« *Face à des informations qui inquiètent, on peut choisir soit d'être inquiet soit de les rejeter. Et personne n'aime être inquiet*[22]… »

(21) https://techcrunch.com/2017/09/07/ai-that-can-determine-a-persons-sexuality-from-photos-shows-the-dark-side-of-the-data-age/

(23) https://twitter.com/michalkosinski

L'AUTEUR

Jean-Paul CRENN est le Fondateur-Dirigeant de la 1re société de conseil spécialisée dans la transformation digitale et le e-commerce, VUCA-Strategy. Conférencier international, il est l'auteur de nombreux ouvrages, le plus récent étant L'Internet des Objets : la 3ème révolution informatique aux Editions Kawa. Il enseigne à l'ESCP-Europe, à la Toulouse Business School et à l'IAE Toulouse-Capitole, la Stratégie et le Marketing Digital. Pour suivre ses conférences et ses publications : https://www.vuca-strategy.com/fr/actus.php

Scott Maxwell - Adobe Stock

OPEN DATA DES DÉCISIONS ASSOCIÉ AUX TRAITEMENTS DES ALGORITHMES : LA FIN DE D'UN TYPE DE JUSTICE

La généralisation d'un Opendata des décisions de justice conduira au développement de nouveaux logiciels analysant les jugements. L'irruption de nouveaux algorithmes, appliqués à une exploitation statistique et nominale des décisions de justice, peut fragiliser le mécanisme des décisions. Un traitement statistique des décisions par typologie de cas, par magistrats et selon un implantation géographique pose les questions fondamentales du rôle du juge et de l'anonymisation des décisions de justice. Cette dernière nécessite la mobilisation d'une forte ressource humaine et matérielle sans préjuger d'un contournement par le recoupement de données issues de bases différentes. La question d'un contrôle de la performance d'un juge au regard de sa singularité par rapport au traitement statistique moyen d'une typologie d'infractions laisse perplexe : l'appréciation personnelle du juge, fondée sur son impartialité et sa prise en compte de l'environnement juridique du cas traité, pourrait en conséquence être affectée par la puissance d'un raisonnement numérique.

Les algorithmes sont-ils
sont-ils une menace pour le juge ?

Par MARC CLÉMENT

La généralisation d'un *Opendata* des décisions de justice conduira au développement de nouveaux logiciels analysant les jugements. En prenant l'exemple de l'exploitation statistique des noms des magistrats de la formation de jugement, il est facile de montrer que l'irruption de ces nouveaux algorithmes pose dès aujourd'hui des questions fondamentales sur le rôle du juge.

La loi du 7 octobre 2016 pour une République numérique étend le principe de la mise à disposition gratuite de l'ensemble des jugements[1]. Le mouvement d'*Opendata* est déjà enclenché pour la justice administrative depuis 2015 avec la mise à disposition de l'ensemble des arrêts du Conseil d'État et des Cours administratives d'appel. Il a eu pour premier effet de mettre en cause l'impartialité des juges en examinant sur une base statistique le sens des décisions rendues. Il est clair que l'application de la loi de 2016 conduit à renforcer ce mouvement puisque la démarche statistique ne peut que se trouver confortée par un nombre plus important de décisions traitées et par des situations de contentieux de masse, notamment en première instance, qui sont favorables à de tels traitements[2].

MARC CLÉMENT
Conseil de l'Institut européen du droit

Se posent alors d'une part le problème de la protection de la vie privée, avec la mise sur la place publique des déboires de personnes ou d'entreprises ayant pour corollaire la persistance de l'information sur Internet, et d'autre part la question d'un contrôle de la performance des juges.

L'anonymisation des décisions de justice n'est pas limitée à l'effacement des références nominales dans un jugement. Il s'agit d'une première étape indispensable et

on ne trouvera pas sur legifrance les noms des personnes en cause mais des initiales. Observons que l'approche française fait plutôt figure d'exception car au Royaume-Uni par exemple, le requérant n'est pas protégé, le jugement étant public. La situation est la même pour la Cour de Justice de l'Union européenne où l'occultation des noms figurant dans la décision n'est pas automatique mais dépend d'une demande explicite[3]. Ce travail ne pose pas de difficultés considérables mais il suppose d'y allouer des ressources, en particulier dans le cadre d'une mise à disposition de décisions de première instance dont le nombre est conséquent.

Ce premier niveau d'anonymat ne signifie pas que l'identification d'une personne n'est pas possible : la description des faits et des lieux peut suffire dans certains cas. Il sera alors nécessaire de faire en sorte que la partie concernée puisse demander explicitement au juge que la décision ne soit pas versée dans la base de données en invoquant un intérêt à ce secret dont il appartient à la formation de jugement d'apprécier s'il peut s'opposer à celui que représente une base de données complète. On voit bien qu'à ce stade, selon que l'on adopte une attitude plus ou moins restrictive, on favorise la protection de la vie privée aux dépends de la mise à disposition de données publiques.

La deuxième difficulté de l'*Opendata* juridique est moins évidente du fait qu'elle n'est pas mentionnée par les articles 20 et 21 de la loi. L'anonymisation des noms de juges paraît à première vue un enjeu moins crucial que celle des justiciables. Pourtant, une des toutes premières applications - *Supralegem* - basée sur la mise à disposition des jugements a visé à évaluer la performance des juges dans certaines matières : il est en effet tentant de faire une statistique du sens des décisions rendues par les formations de jugement pour en tirer des conclusions sur les chances de succès d'une affaire. On peut émettre des doutes sur la fiabilité de telles statistiques notamment dans l'hypothèse de formations de jugement collégiales ou de bases statistiques trop réduites si on cherche à catégoriser de façon solide les affaires en fonction de leurs caractéristiques. Il n'en reste pas moins que l'*Opendata* pose la question de l'impartialité du juge d'une façon renouvelée.

La question n'est en effet pas nouvelle puisqu'elle est au cœur de l'office du juge : ce dernier doit être impartial pour que l'on puisse lui confier une affaire. Sans impartialité, la crédibilité du système institutionnel qui est en jeu. De ce fait, cette vertu fait depuis longtemps l'objet d'une attention particulière mais on peut constater que la sensibilité sur ce point est accrue depuis quelques années avec l'institution d'un collège de déontologie au sein de la juridiction administrative, et en 2017 la mise en place d'entretiens de

(1) L'article 20 de la loi du 7 octobre 2016 complète l'article L. 10 du code de justice administrative « Ces jugements sont mis à la disposition du public à titre gratuit dans le respect de la vie privée des personnes concernées. / Cette mise à disposition du public est précédée d'une analyse du risque de ré-identification des personnes. / Les articles L. 321-1 à L. 326-1 du code des relations entre le public et l'administration sont également applicables à la réutilisation des informations publiques figurant dans ces jugements. / Un décret en Conseil d'Etat fixe, pour les jugements de premier ressort, d'appel ou de cassation, les conditions d'application du présent article. ». L'article 21 fait de même s'agissant du code de l'organisation judiciaire même si la formulation autorise des exceptions au principe.

(2) V. La mémoire numérique des décisions judiciaires Recueil Dalloz / Eloi Buat-Ménard — Paolo Giambiasi — D. 2017. 1483 — 20 juillet 2017

déontologie et la publication d'une charte de déontologie[4].

Ce mouvement s'inscrit dans une nécessité de transparence qui touche toutes les fonctions d'autorité et il est normal que la fonction juridictionnelle soit concernée. Il est d'ailleurs clair que chacun a le droit de questionner l'action de tout fonctionnaire puisque l'article 15 de la déclaration des droits de l'homme et du citoyen dispose que « *La Société a le droit de demander compte à tout agent public de son administration* ». Mais doit-on pour autant mesurer en permanence la production d'un juge au regard de la moyenne des décisions rendues ? Certains systèmes judiciaires l'autorisent comme c'est le cas États-Unis où des sociétés vont proposer une analyse des décisions d'un juge dans un domaine particulier. Dans ce système, le juge est élu et il assume une part de subjectivité. Tel n'est pas le cas en France où la justice est rendue « *au nom du Peuple français* » et n'est donc pas le résultat d'une analyse personnelle du juge.

Or en mettant à disposition toutes les décisions des juges, y compris en première instance, dans des affaires répétitives ou urgentes où le juge siège seul, il devient possible de mesurer une performance individuelle. Les différences d'appréciation ou de sensibilité, qui pouvaient être supposées, sont alors explicitées par la puissance du raisonnement numérique[5]. Ce qui restait de l'ordre d'une appréciation vague et peu étayée devient vérité statistique.

Cette situation a par exemple été rencontrée s'agissant des ordonnances de référé prises dans le contexte de l'état d'urgence : les noms des juges pour ces décisions sont anonymisés afin d'éviter une mise en cause personnelle.

De fait, l'*Opendata* nous force à nous interroger : voulons-nous poser des limites à la transparence afin de préserver l'intérêt de l'institution ? Dans un mouvement de fond de l'évolution de nos sociétés où les institutions sont fragilisées et contestées, la remise en cause de l'autorité du juge conduit à la perte d'autorité de la loi elle-même. C'est bien dans le sens d'une préservation de cette autorité que les obligations déontologiques développées ces dernières années œuvrent. Mais il n'est pas certain que celles-ci soient suffisantes dans le contexte de l'*Opendata*.

On pourrait imaginer s'en remettre à la pédagogie et aux explications. Après tout, la possibilité de récusation d'un juge est ouverte à tout justiciable et la complexité des décisions rendues ne permet pas de considérer que les échantillons statistiques utilisés sont bien comparables. Par ailleurs, on peut légitimement s'interroger sur la notion de moyenne statistique : rien ne permet d'affirmer que les décisions les plus proches de la moyenne sont les meilleures. Enfin, les mécanismes d'appel et de cassation offrent une garantie d'examen par d'autres juges.

(3) Voir le document de la Cour de Justice de l'Union européenne Recommandations à l'attention des juridictions nationales, relatives à l'introduction de procédures préjudicielles 2012/C 338/01 (points 27 et 28)

(4) La loi du 20 avril 2016 relative à relative à la déontologie et aux droits et obligations des fonctionnaires a ajouté les articles L. 231-4-1 à L. 231-4-4 au code de justice administrative qui précise le régime des déclarations des intérêts et de gestion des conflits d'intérêts.

(5) Voir sur l'important problème du poids du raisonnement quantitatif dans nos sociétés, le cours du Collège de France d'Alain Supiot « La gouvernance par les nombres »

Adobe Stock

La notion de moyenne statistique ne recouvre pas le contexte particulier des affaires et peut favoriser une standardisation des décisions de justice.

L'institution prend donc déjà en compte, avec des procédures particulières, la question de l'impartialité.

Si la collégialité des décisions est une garantie permettant de fournir un écran suffisant à une exploitation statistique des bases de données de jugements, la situation est tout autre pour ce qui concerne les décisions rendues par un seul juge. Elles sont rendues en première instance de plus en plus souvent du fait de l'accroissement continu du contentieux qui a imposé ce mode dérogatoire de traitement pour les affaires les plus répétitives mais aussi du développement des procédures d'urgence. Nous sommes alors dans une situation proche de celle du juge américain qui doit assumer seul sa décision. Devra-t-il se plier à la loi de la moyenne pour éviter d'être mis en cause ? Ce serait alors une atteinte grave à son indépendance, deuxième vertu cardinale du juge. Qu'en penserait alors le justiciable qui verrait une décision rendue dans un sens pour faire en sorte que la moyenne des décisions reste acceptable ?

Doit-on alors envisager d'encadrer l'usage des algorithmes travaillant sur les bases de données de jugements ? Cela reviendrait à chercher à limiter l'innovation en fixant a priori des limites à ce que doivent faire les algorithmes. On pourrait d'abord objecter que l'idée est bien antinomique avec ce qui préside à l'*Opendata*. En effet, la raison d'être de la démarche d'ouverture des données publiques est bien de favoriser le développement d'outils numériques de tous ordres. Poser des limites à ces outils revient à retirer d'une main ce que l'on donne de l'autre. Cependant, si des raisons impératives liées à un intérêt supérieur l'exigent, l'objection doit être levée et un point d'équilibre doit être trouvé comme c'est le cas pour ce qui concerne la protection de la vie privée des parties. Or, il est moins évident que la protection de l'institution exige que l'on encadre le développement des algorithmes d'analyse jurisprudentielle puisque, comme nous l'avons indiqué, c'est seulement dans certaines situations (juge unique) que la question peut réellement devenir délicate. Plus encore la notion d'encadrement juridique de la production de logiciels d'analyse de jurisprudence

nous semble vouée à l'échec[6]. En effet, il s'agirait de fixer des limites à la production de certaines informations par ces logiciels : dans l'hypothèse d'une liste d'informations interdites, il conviendrait alors de définir *a priori* ces indicateurs sans que l'on soit certain que des moyens de contourner l'interdiction ne soient simples à mettre en œuvre. Par exemple, on peut imaginer des prestations de service fournies directement ou la fourniture d'éléments d'analyse permettant d'obtenir sans difficulté l'information interdite.

(6) Un projet de la Mission Droit et Justice est en cours sur ce thème de l'encadrement des algorithmes mais l'approche telle qu'elle est décrite dans la fiche disponible sur le site nous semble peut convaincante s'il s'agit d'examiner d'abord les approches mathématiques disponibles puis d'en proposer un encadrement : il est clair d'une part qu'il est impossible d'être exhaustif sur les techniques mathématiques appliquées et applicables et que d'autre part la notion d'encadrement de certaines techniques par le droit pose de redoutables problèmes.

Imaginer par ailleurs un contrôle du traitement de l'information par un organisme tel que la CNIL, qui délivrerait une autorisation, nous semble délicat à mettre en œuvre car les ressources nécessaires seraient conséquentes et le caractère bureaucratique du montage ridiculiserait les ambitions portées par la loi. Deux leçons nous semblent se dégager de ces quelques éléments d'analyse sur un problème en définitive simple à formuler et d'une portée circonscrite à un champ bien limité.

D'une part, il nous semble que les transformations profondes liées au numérique ne sont pas des développements réservés à un futur lointain mais que ces transformations sont déjà à l'œuvre. La mise à disposition des bases de données de jurisprudence pose aujourd'hui des questions redoutables qui ne sont pas tant liées à des techniques informatiques mystérieuses connexes de l'intelligence artificielle qu'à la possibilité de traitement d'un grand nombre d'informations jusqu'ici difficile d'accès.

(7) Voir pour plus d'information : http://lyon.cour-administrative-appel.fr/A-savoir/Communiques/Simulation-de-proces-2030-un-vehicule-automatique-detruit-un-lampadaire-place-Bellecour-a-Lyon

D'autre part, il convient, lorsque l'on évoque la question de l'encadrement juridique du développement d'algorithmes, de travailler concrètement sur des questions précises et de ne pas se contenter de généralités : chaque domaine pose des difficultés différentes avec des enjeux juridiques très précis. De ce fait, il nous semble indispensable de travailler à partir de situations réelles et d'analyser les impacts des innovations numériques dans une démarche d'expérimentation juridique. Nous avons engagé cet exercice dans le cadre d'un partenariat entre la Cour administrative de Lyon, la faculté de droit de l'université catholique de Lyon et le barreau de Lyon en développant un procès fictif pour traiter un accident d'un véhicule autonome[7]. Il faut multiplier ces expériences pour mieux comprendre les enjeux juridiques posés par le numérique.

L'AUTEUR

Marc Clément est rapporteur public à la Cour administrative d'appel de Lyon. Il est également membre de l'Autorité environnementale du Conseil général de l'environnement et du développement durable, du comité de déontologie de l'Institut de Radioprotection et de Sûreté Nucléaire et du conseil de l'Institut européen du droit.

L'ADAPTATION AU DÉFI DE LA CYBERCRIMINALITÉ PAR UNE ÉVOLUTION DES TEXTES ET UNE SPÉCIALISATION DES ACTEURS

Les cinq chantiers de modernisation de la justice, lancés par le Garde des Sceaux, Ministre de la Justice, soulignent la nécessité pour les magistrats de s'adapter aux nouveaux enjeux induits par la révolution numérique. Le droit et les procédures pénales de droit commun et d'exception sont adaptés en définissant des infractions spécifiques et en intégrant une maîtrise du numérique appliquée aux techniques d'enquêtes.

Une coordination nationale, couplée à la spécialisation de juridictions et relayée par des magistrats formés, illustre une organisation propre à animer et soutenir la lutte contre les cybercriminalités. Des plateformes, dédiées aux usagers et aux victimes de cybermalveillances, permettent de mieux accompagner les victimes et de cerner l'évolution de ce champ délictuel particulier.

Une réponse nationale et isolée n'est pas suffisante au regard de la transversalité de ce type de délinquance. Une coopération européenne constitue un enjeu majeur pour apporter une réponse à une cybercriminalité sans frontières.

L'action de la Justice
face à la cybercriminalité

Par SYLVIE SCHLANGER

La cybercriminalité par nature transfrontière est le nouveau défi auquel est confrontée la justice qui doit organiser l'identification des auteurs et leur répression. La coordination des acteurs est facilitée par :

- l'existence d'une mission placée auprès du directeur des affaires criminelles et des grâces,
- la spécialisation des parquets confrontés à la cybercriminalité et
- des services d'enquête dédiés.

SYLVIE SCHLANGER

Magistrate - Avocat général près la Cour d'appel de Paris

Le droit et les procédures pénales de droit commun et d'exception (Etat d'urgence, terrorisme) sont régulièrement adaptés pour répondre plus efficacement aux nouvelles formes de délinquance, intégrant la maîtrise du numérique appliqué aux techniques d'enquêtes (cyber-patrouilles, enquêtes sous pseudo, perquisitions numériques, *etc.*) , et la définition d'infractions spécifiques (atteintes aux STAD,) dans le contexte des cinq chantiers de modernisation de la justice lancés récemment par le Garde des Sceaux, ministre de la Justice, qui vise également la simplification de la procédure pénale.

La coopération européenne constitue un enjeu majeur : le parquet européen, en lien avec les parquets des Etats membres et Europol, pourrait apporter une réponse de poids aux défis de la cybercriminalité sans frontières.

Dans un monde en évolution constante où le transhumanisme[1] est aujourd'hui devenu une réalité, la Justice est confrontée à de nouveaux défis tant la cybercriminalité est protéiforme et sans frontières : il ne se

(1) Le «transhumanisme» est un mouvement scientifique et philosophique, milite pour l'amélioration illimitée des facultés physiques et intellectuelles des humains par tous les moyens, génétiques, chimiques, mécaniques, informatiques ; (cf Luc FERRY La révolution transhumaniste 2016 éditions PLON)
Par ailleurs, des économistes étudient l'impact «disruptif» de l'Internet sur l'organisation sociale et la répartition des richesses qualifiée tantôt d'ubérisation de la société dans son versant négatif, en référence à la société implantée originairement aux Etats Unis qui a bouleversé l'organisation des transports individuels, ou « d'économie participative » pour mettre en exergue ses aspects positifs et valorisants pour l'homme. Un procès du transhumanisme a d'ailleurs eu lieu à la Cour d'appel de PARIS le 27 juin 2017, organisé par le parquet général, l'université de Paris 1et des avocats du barreau de Paris ainsi que l'Ecole nationale de la magistrature.

(2) ANSSI : Agence nationale pour la sécurité des systèmes d'information, créée en juillet 2009.

passe pas un jour sans que des attaques cyber soient mises à jour à l'encontre des acteurs économiques ou des administrations, voire de l'État. Or, la réponse doit, pour être efficace cibler précisément l'objectif poursuivi : à l'État d'assumer la cyberdéfense, aux entreprises de renforcer les dispositifs de cybersécurité avec l'aide de l'ANSSI[2] pour les plus sensibles d'entre elles, et enfin à la Justice d'assurer la répression des faits qualifiés délits ou crimes.

Le procureur général Marc Robert, dans son rapport sur la lutte contre la cybercriminalité « Protéger les internautes », page 12, de février 2014, a définit la cybercriminalité comme regroupant « *toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication principalement Internet* » .

(3)Rapport INHESJ « enjeux et difficultés de la lutte contre la cybercriminalité » - 26 e session nationale, page 20.

Ce constat souligne la difficulté de mettre à jour[3] et de poursuivre des atteintes cyber transnationales, anonymes et dont la preuve numérique est particulièrement difficile à rapporter puisque volatile.

C'est dire si la répression de la cybercriminalité par la justice ne constitue qu'un des aspects du problème ; toutefois, les moyens mis à la disposition de la justice doivent lui permettre d'accroître l'efficacité de la répression, en permettant d'identifier les auteurs et de les appréhender en vue de leur comparution devant les juridictions pénales.

Trois axes seront analysés :

La mobilisation des acteurs de la lutte (ministère de la justice, magistrature et services enquêteurs),

Le renforcement des incriminations et de la répression

Les spécificités procédurales

La mobilisation des acteurs de la lutte

L'administration centrale du ministère de la justice

La mission de prévention et de lutte contre les atteintes à la probité et contre la cybercriminalité au sein de la direction des affaires criminelles et des grâces, coordonne

les actions, au plan national, de lutte contre la cyber criminalité tout en assurant le suivi de l'action publique dans ces domaines et en apportant un soutien documentaire pédagogique et méthodologique.

Les juridictions parisiennes

La section F1 du parquet de Paris a priorisé la lutte contre la cybercriminalité, notamment en matière d'atteintes aux systèmes de traitement automatisé de données, et comporte en son sein, outre des magistrats, un assistant spécialisé capitaine de la police nationale afin de renforcer la coordination avec les services enquêteurs.

Ayant une grande expérience dans l'exercice des poursuites en la matière, il a élaboré un cyber-lexique afin d'expliciter le langage cyber plus que complexe.

Le parquet général de la Cour d'appel de Paris a confié le pilotage de ces affaires à l'un des six services centraux et comporte un référent cybercriminalité qui coordonne l'action.

Les parquets du ressort de la Cour, tout comme ceux de la Cour de VERSAILLES limitrophes, dont Nanterre, ont de même priorisé cet objectif de politique pénale au même titre que la lutte contre le terrorisme dont la cybercriminalité est souvent l'un des leviers.

La formation des magistrats spécialisés « référents cyber » a été assurée en 2017 notamment par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) à Nanterre, permettant le renforcement des liens avec les enquêteurs spécialisés ainsi qu'avec les juges d'instruction sensibilisés à cette matière.

Les services de police spécialisés

L'Office central anime et coordonne au niveau national la lutte contre la cybercriminalité. Il est de plus chargé de fournir une assistance technique aux services de police et de gendarmerie pour les dossiers complexes.

Depuis janvier 2009, il assure la gestion de deux plateformes sur lesquelles le public peut effectuer des signalements : PHAROS et INFO ESCROQUERIE ;

Un projet de plateforme de recueil et traitement des plaintes en ligne en matière de cyber escroqueries est à l'étude afin de procéder à des recoupements pour pouvoir identifier et localiser les auteurs, y compris à l'international.

Enfin, l 'office assure le lien avec les services internationaux de police (Interpol et Europol) et dans les instances stratégiques internationales.

La direction de la police judiciaire de Paris comporte en son sein une Brigade d'enquête sur les fraudes aux technologies

de l'information (BEFTI) avec un groupe d'enquête et d'initiative et un groupe d'assistance, compétents sur Paris et la petite couronne.

Les services de gendarmerie spécialisés

Outre les brigades territoriales, le pôle judiciaire de la gendarmerie nationale dispose d'un plateau d'investigation cybercriminalité et analyses numériques qui intervient dans les investigations et au plan transversal en faisant l'interface entre les opérateurs et les enquêteurs et en assurant la formation l'équipement et l'information des unités territoriales de gendarmerie. (PICyAN) .

Le renforcement des infractions et de la répression

Le droit pénal commun permet d'appréhender certains comportements délictueux : usurpation d'identité (en ligne), contrefaçon de bases de données, escroquerie et faux et usage de faux (faux ordres de virement), (escroquerie au Président), fraude aux cartes bancaires, ou encore blanchiment, mais le droit pénal s'est enrichi, par la loi GODFRAIN du 5 janvier 1988, d'infractions spécifiques visant précisément les accès et maintiens frauduleux dans un système de traitement de données informatisées (STAD), l'entrave au fonctionnement du système, l'introduction de données frauduleuses ou la falsification ou la suppression frauduleuse de données.

Le droit pénal d'exception, en matière terroriste, appréhende les comportements via Internet notamment :

– par le délit d'apologie de l'article 421-2-5 inséré dans le code pénal pour renforcer la répression, les peines étant portées à 7ans d'emprisonnement lorsque les faits ont été commis en utilisant un service de communication au public en ligne.

– pour sanctionner la consultation habituelle d'un service de communication au public mettant à disposition des messages images ou représentations provoquant à des actes de terrorisme sauf consultation résultant de l'exercice normal d'une profession destinée à informer le public (article 421-2-5-2 du code pénal (deux ans d'emprisonnement et 30 000 euros d'amende).

Les spécificités procédurales

Dans le même temps, la procédure pénale met en œuvre des techniques d'enquête et de preuve diversifiées :

- par le recours aux procédures classiques, aux expertises perfectionnées par les nouvelles évolutions technologiques, comme le bornage des téléphones portables et smartphones, la géolocalisation - juridiquement réglementée en avril 2014 -, l'interception de fichiers et de données numériques apparentes ou cryptées.

- par la mise en œuvre de procédures dérogatoires au droit commun, comme la

procédure d'infiltration qui doit tendre à la constatation d'infractions préexistantes et non à la provocation à la commission des dites infractions, introduite en procédure pénale dans les enquêtes de pédopornographie, les enquêtes sous pseudonyme sur les réseaux numériques, la captation et l'enregistrement de données informatiques en temps réel (loi du 3 juin 2016/ imsi catchers) et les intrusions informatiques sans consentement.

Les perquisitions informatiques permettent quant à elles d'accéder à des données conservées dans un équipement informatique tels les smartphones, tablettes, imprimantes ou dans un réseau de stockage (nuage).

Toutes ces modalités probatoires sont soumises au principe de loyauté qui fait obstacle aux données ou éléments obtenus par provocation des services de police ou de gendarmerie visant la commission de l'infraction.

Les juridictions françaises sont compétentes lorsque la victime des infractions réside en France. C'est le parquet ou le juge d'instruction du tribunal de grande instance du domicile de la victime, ou encore celui du siège social de la personne morale qui assurera la conduite de l'enquête.

Article 113-2-1 du code pénal :
« *Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République* ».

À l'heure de la révolution numérique et de la mondialisation, il devient urgent de placer la réponse pénale à la cybercriminalité comme une priorité de politique pénale interne aux Etats mais aussi de coopération internationale et européenne. Le parquet européen, en lien avec les parquets des Etats membres et Europol, pourrait apporter une réponse de poids aux défis de la cybercriminalité sans frontières.

AUTEUR

Après avoir exercé des fonctions de substitut au Havre puis au sein de plusieurs sections spécialisées du parquet de PARIS, dont la section financière, Sylvie Sclanger a exercé au sein de la direction des services judiciaires en administration centrale, puis en cabinet ministériel dans le domaine des affaires sociales, à l'inspection générale des services judiciaires, en qualité de secrétaire générale du conseil national pour l'accès aux origines personnelles -(CNAOP)- au Parquet général de Versailles puis de Paris. Elle est auditrice de la 26e session de IIN-HESJ et à ce titre elle a présidé un groupe de diagnostic sur les moyens de lutte contre la cybercriminalité en juin 2015.

Fotolia - Ruslan Grumble

UNE RÉORGANISATION DE L'APPAREIL JUDICIAIRE POUR FAIRE FACE AUX NOUVELLE FORMES DE CYBERCRIMINALITÉ

Le développement de la cybercriminalité concerne globalement les atteintes aux traitements automatisés, à la personnalité et une transposition d'une criminalité traditionnelle qui profite des atouts de la toile en matière d'opacité. La riposte judiciaire s'organise par la création d'un arsenal juridique et l'appui de services européens. Le ministère de l'Intérieur a engagé le renforcement et une coordination de ses moyens d'action. En conséquence, les forces de sécurité ont constitué un corps d'experts et d'enquêteurs spécialisés. Au sein du pôle judiciaire de la gendarmerie nationale, le Centre de lutte contre les criminalités numériques (C3N) dispose de compétences uniques utiles aux unités de terrain. La magistrature a suivi la même tendance. Le parquet de Paris dispose d'une section dédiée à la cybercriminalité et au-delà de cette spécialisation, la juridiction parisienne dispose depuis la loi du 3 juin 2016 d'une compétence nationale en matière d'attaques des systèmes de traitement automatisé des données (STAD). Par contre, la création d'un Big Data judiciaire mérite réflexion car une algorithmie appliquée sur les décisions de justice pourrait rendre instable l'acte de juger.

Du cybercrime
au cyberjuge

Par XAVIER LEONETTI

A chaque instant, particuliers, entreprises, institutions sollicitent cet assistant multifonctions qu'est Internet. Sans outil numérique, toute activité est devenue impossible. Si les intrusions dans les systèmes constituent le plus souvent une forme évoluée de la délinquance astucieuse, elles sont désormais aussi le chemin occulte pour influer sur les décisions du chef d'entreprise ou des institutions. Dans ce contexte, jamais sans doute, le prédateur n'a été aussi près de sa victime puisqu'au moyen de l'ordinateur, des smartphones et des objets connectés il est partout, constamment avec elle et peut-être demain en elle avec le recours à des organes ou prothèses connectés. Jamais aussi le délinquant n'a été aussi loin de son juge, ne serait-ce qu'en raison des frontières juridiques et de la lenteur de la coopération judiciaire comparée à la vitesse des transactions sur la Toile.

XAVIER LEONETTI

Substitut placé - Parquet général d'Aix-en-Provence - TGI de Marseille

La généralisation de l'usage d'Internet a ouvert un champ nouveau à l'office du juge qui doit intégrer le cyber espace comme la matière de son action et en même temps comme un outil de travail et d'accompagnement dans sa prise de décision.

Cybercrime et « nouvelles » infractions ?

En matière de cybercriminalité, on observe trois grandes catégories d'infractions cybercriminelles :

• La première est relative aux infractions liées aux systèmes d'information et de traitement automatisé des données (STAD). Il s'agit par exemple, d'intrusions sur un serveur informatique, ou de piratage de données.

• La seconde catégorie regroupe les infractions liées aux formes de criminalité « traditionnelles » qui utilisent Internet et les nouvelles technologies de l'information et de la communication (NTIC) comme étant de nouveaux modes opératoires. Ainsi, un véhicule volé qui était précédemment revendu via les annonces gratuites de la presse, est aujourd'hui vendu par l'intermédiaire de sites Internet spécialisés dans la vente de particuliers à particuliers.

• La troisième catégorie présente les infractions commises par Internet relatives à la dignité ou à la personnalité et les atteintes sexuelles commises par ce même biais. Ces infractions traditionnelles connaissent aussi une nouvelle vie sur le web, au moyen notamment de l'anonymat offert par Internet.

En premier lieu, il convient de souligner que l'étude des formes de cybercriminalité se révèle parcellaire, car elle dépend de la performance des outils de comptage utilisés par l'administration. En la matière, les différents services de l'État utilisent chacun des grilles d'analyse et de comptage différentes. Il s'agit d'un véritable château kafkaïen. Par exemple, s'agissant de l'utilisation du logiciel Cassiopée[1], l'application est déjà interconnectée avec celle de la gendarmerie et bientôt avec celle de la police. Cependant, les critères de Cassiopée ne sont pas identiques à ceux utilisés par la police et la gendarmerie. Il n'existe donc pas de continuité statistique entre les ministères de l'Intérieur et de la Justice. C'est d'ailleurs ce que relevait le Premier ministre, en octobre 2014, à l'occasion du séminaire de rentrée des auditeurs de l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et de l'Institut des hautes études de la défense nationale (IHEDN) : « *Les systèmes d'information des forces de sécurité d'une part, et de la justice d'autre part, sont structurellement incapables de communiquer* ».

(1) CASSIOPEE (Chaine Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants) est un fichier français qui contient des informations relatives aux plaintes enregistrées par les magistrats dans le cadre de procédures judiciaires. Le traitement CASSIOPEE, mis en œuvre dans les tribunaux de grande instance, a pour objectif d'améliorer le délai de traitement des procédures et d'assurer l'information des victimes.

De surcroît, il convient de ne pas oublier qu'une partie des faits statistiques est traitée en dehors du système pénal. Par exemple, le GIE (Groupement d'Intérêt Économique) des cartes bancaires peut être amené à traiter de phénomènes cybercriminels dans le cadre de solutions de conflits à l'amiable. Enfin, le « chiffre noir » de la cybercriminalité est l'un des plus élevés, souvent parce que les personnes physiques ou morales visées ignorent les faits. En effet, une entreprise met en moyenne 229 jours pour découvrir la menace dont elle fait l'objet. Ensuite, l'étude statistique permet de relever que plus de 90 % des 70 000 cyberinfractions recensées en 2015 par l'Observatoire national de la délinquance et des réponses

pénales (ONDRP) sont des escroqueries et des attaques financières. C'est à dire qu'à l'image de l'économie réelle qui repose sur la confiance, l'économie souterraine se nourrit de la confiance que l'escroc crée au préjudice de sa victime. La particularité de l'espace cyber est que les internautes font preuve d'une crédulité excessive. En effet, il apparaît que dans l'espace virtuel les individus font preuve d'une négligence plus importante que dans le monde réel. Ainsi, imagine-t-on des personnes distribuer sur la voie publique des prospectus décrivant leurs habitudes illustrées par des photos de leur vie intime ? Non, pourtant, des millions d'internautes le font chaque jour sur Facebook. De même, si une personne vêtue d'un uniforme « Orange » ou « SFR » abordait les passants en leur demandant leur numéro de carte bleue, obtiendrait-elle satisfaction ? Sans doute pas. Malheureusement, sur Internet, cette pratique (dite de *phishing*) fait plusieurs milliers de victimes tous les mois. En fait, ces cyberinfractions ne constituent que la mutation numérique d'infractions traditionnelles d'escroqueries ou d'abus de confiance.

De même, l'ère du numérique accentue les menaces qui pèsent sur l'Etat et sur son fonctionnement démocratique, au travers notamment des possibilités de piratages ou d'intrusions. Par exemple, ces derniers mois les Etats-Unis ont été confrontés à des suspicions de piratages informatiques à l'occasion de la campagne électorale présidentielle. Cette situation, unique dans l'histoire politique américaine, nous enseigne que les acteurs de la vie publique et politique doivent très tôt acquérir des réflexes d'hygiène et de sécurité numérique. A défaut, les informations qu'ils détiennent se trouvent susceptibles d'être interceptées ou modifiées par des tiers ou des puissances étrangères.

On peut ainsi imaginer en France un piratage des listes électorales détenues sur les serveurs informatiques des mairies. Il s'agirait alors moins de compromettre que de désorganiser un scrutin en permettant de créer un doute sur la sincérité des élections. Dans un contexte de défiance vis à vis des autorités publiques et politiques, ce risque est réel d'autant que les scrutins sont de plus en plus nombreux (dernièrement sur la création d'un aéroport à Notre-Dame des Landes par exemple). C'est pourquoi une démarche particulière de prévention à destination des partis politiques a été initiée à l'automne 2015 par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

La riposte judiciaire aux cybercrimes

L'arsenal pénal permettant de réprimer les comportements délinquants s'est particulièrement étoffé, notamment depuis l'adoption de la LOPPSI2 du 14 mars 2011.

Aujourd'hui, les atteintes aux systèmes automatisés de données (art 323-1 à 323-7 du CP) permettent de réprimer les

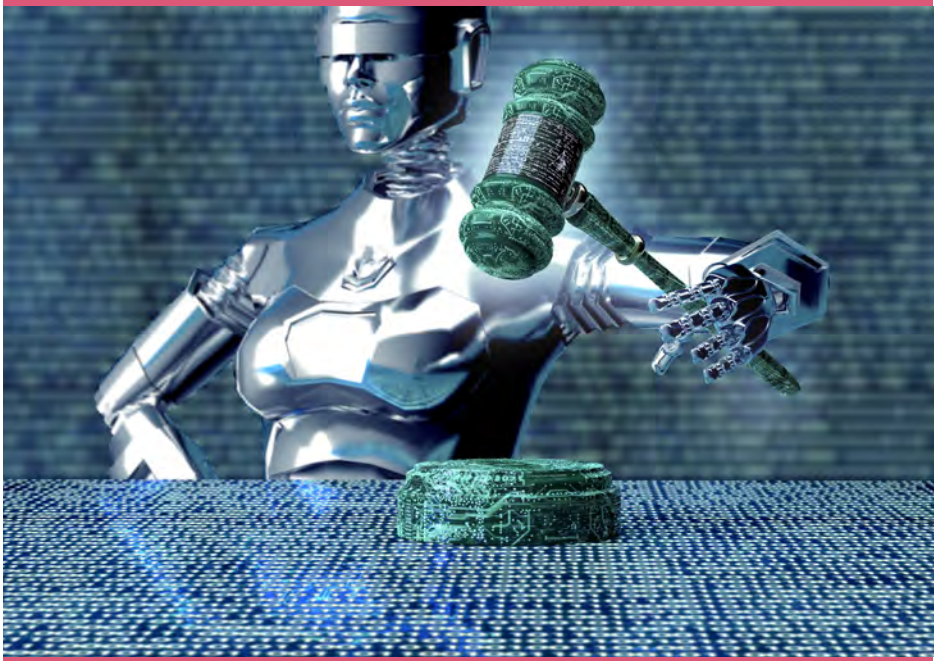
nouveaux types d'infractions. Il en est ainsi de l'accès ou du maintien frauduleux dans un système de traitement automatisé de données (C. pén., art. 323-1, al. 1er) qui permet de réprimer le phishing qui consiste à soutirer des informations personnelles à des internautes en leur envoyant un courriel usurpant l'identité d'une banque ou d'un site marchand. (TGI Paris, 2 sept. 2004). De même, s'agissant de la participation à un groupement de pirates (art. 323-4) : ainsi lorsque des participants n'ignoraient pas que les informations échangées avaient pour finalité de commettre des atteintes au système informatique d'accès à Canal plus, leur participation à l'entente est pénalement répréhensible (T. corr. Carpentras, 25 juin 2004).

En matière de traitement de données à caractère personnel, l'art 226-16 du code pénal permet de sanctionner la mise en ligne du nom d'une personne au sein du contenu rédactionnel d'un site web qui est un traitement automatisé de données nominatives au sens de l'article 5 de la loi de 1978, et qui nécessite la déclaration à la CNIL du site web concerné.

S'agissant de la procédure pénale, le CPP ne fait référence qu'indirectement à la notion de cybercriminalité. S'agissant par exemple du mandat d'arrêt européen, par dérogation, l'article 695-23 du CPP en prévoit l'exécution sans contrôle de la double incrimination des faits reprochés lorsque les agissements considérés entrent notamment dans la catégorie de la « cybercriminalité », de la « contrefaçon » ou de la « falsification des moyens de paiement ».

Depuis 2013 également, des travaux ont été engagés par le ministère de l'Intérieur visant à renforcer et mieux coordonner les moyens d'actions en matière de prévention et de lutte contre la cybercriminalité. Ainsi, il convient de souligner que la gendarmerie et la police nationales disposent de cyberenquêteurs dont la spécialité croît selon le niveau d'infraction. Par exemple, la police nationale s'est récemment dotée d'une sous-direction de lutte contre la cybercriminalité. De même, au sein du Pôle judiciaire de la gendarmerie nationale (PJGN), le centre de lutte contre les criminalités numériques (C3N) dispose de compétences uniques en matière de cybercrime destinées à appuyer les unités locales. Par ailleurs, l'action de la gendarmerie se trouve renforcée par l'apport du réseau de la réserve citoyenne cyberdéfense placée sous l'autorité du ministère des Armées. La direction générale de la sécurité intérieure (DGSI) dispose de compétences spécifiques notamment s'agissant de cyberradicalisation ou de lutte contre le cyberespionnage.

Rappelons d'ailleurs, que les articles 706-102-1 à 706-102-6 du code de procédure pénale créent une nouvelle catégorie de technique d'enquête, relative aux captations des données informatiques. Il s'agit d'un dispositif ayant pour objet, sans le



Adobe Stock

Un *Big data* des décisions judiciaires ouvre la voie d'une justice rendue au gré d'algorithmes reposant sur l'analyse des décisions et la personnalité des juges.

consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre. En outre, s'agissant de la consultation des données personnelles à distance par des enquêteurs, la Cour de cassation, dans un arrêt du 6 novembre 2013, a retenu qu'il s'agit d'une « *simple mesure d'investigation et non d'une perquisition distincte exigeant une nouvelle décision [d'un] magistrat* ». Au sein du ministère des Armées, le Centre d'analyse et de lutte informatique défensive (CALID) opère une veille et une analyse des nouvelles cybermenaces et assure également la cyberprotection des opérations extérieures de la France.

Enfin, du point de vue interministériel, l'Agence nationale de sécurité des systèmes d'information (ANSSI), créée en 2009, édicte les règles de sécurité des

systèmes d'information de l'Etat et joue le rôle de gardien des « *opérateurs d'importance vitale* ».

Au niveau européen, plusieurs organisations ont en charge des missions de cybersécurité. En particulier, le Centre de criminalité en haute technologie d'EUROPOL a pour mission de mener des actions de coordination, de soutien opérationnel, d'analyse stratégique et de formation. De même, le Centre européen de lutte contre la cybercriminalité (EC3) centralise l'expertise et l'information, soutient les enquêtes criminelles et promeut les solutions à l'échelle de l'union européenne en se concentrant sur les activités illicites en ligne menées par des organisations criminelles.

Il est à noter que le 2 avril 2014, une opération, coordonnée par INTERPOL, a permis d'interpeller 58 personnes impliquées dans un réseau criminel responsable d'affaires de « *sextorsion* ». Cette affaire fait suite au suicide de Daniel Perryd, un adolescent écossais victime d'une tentative de chantage sur Internet.

L'office du juge à l'heure du cyberespace

En premier lieu, l'espace cyber opère de perpétuelles mutations des champs infractionnels. Citons l'apparition des monnaies virtuelles qui sont des moyens de transaction permettant d'effectuer des paiements en ligne. Contrairement à une devise officielle, une monnaie virtuelle n'est pas l'incarnation de l'autorité de l'Etat ou d'une banque centrale et échappe à une régulation régalienne. Au cours du mois de juillet 2014, une plate-forme de *bitcoins* a été démantelée en Midi-Pyrénées dans le cadre d'une enquête diligentée par la division économique et financière de la gendarmerie nationale. Plus de 200 000 euros de bitcoins ont été saisis à la suite de mouvements suspects constatés sur les réseaux numériques.

Ensuite, le monde virtuel révolutionne l'office du juge en ce qu'il conduit à revoir la nature même des modes d'enquêtes, de poursuites et de procès. En particulier, les réseaux sociaux sont parfois considérés comme étant de véritables adjoints de sécurité. Plusieurs plateformes de signalement des comportements suspects voire infractionnels se sont développées sur la toile. On se souvient à cet égard de l'affaire de l'adolescent, survenue en 2014, qui s'était filmé en train de lancer un chat contre un mur. Ce dossier a permis d'illustrer la complémentarité possible entre les internautes et les services de police. Pour autant, il convient de rappeler que dans plus de 90 % des cas les traques conduites par des internautes justiciers se soldent par un échec. Le web ne doit pas devenir un *far-west* où chacun règle ses comptes et tente de faire la loi. Par exemple, certains groupes de militants, tels que les *Anonymous* dont n'importe qui peut se prévaloir, se mêlent de nombreuses causes sous prétexte de lutter

contre les injustices. Mais, souvent, ils peuvent se tromper de cible et lyncher la mauvaise personne. Ainsi, dans le Missouri (Etats-Unis) et à la suite de la mort de Michael Brown lors d'une intervention policière, commettant une erreur d'identité, *Anonymous* avait publié sur Twitter l'identité du policier, nullement concerné, que le groupe pensait être à l'origine de l'homicide du jeune homme.

Enfin, une autre question se pose au regard de la mise en ligne et en accès libre et gratuit de toutes les décisions de justice. Bertrand Louvel, premier président de la Cour de cassation indiquait lors de sa rentrée le vendredi 13 janvier : « *la mise en ligne nécessaire, commandée par les progrès de notre temps, de l'ensemble des décisions de l'ordre judiciaire (…) ouvre sur des horizons insoupçonnés* ». Cette réforme issue de la loi Lemaire, du 7 octobre 2016, permettra l'analyse de la jurisprudence par des algorithmes et donc mettra en évidence dans certains cas les écarts entre les décisions rendues par deux chambres d'un même tribunal.

En outre, l'analyse de la jurisprudence constitue un pas de plus vers la création d'une justice prédictive. Comme le souligne Chantal Arens, première présidente de la cour d'appel de Paris, le *Big data* en matière de justice « *peut conduire à une justice prédictive allant de l'identification des références de décisions à des profils de juges ayant rendu tel ou tel type de décision* ». Selon elle, « *l'acte de juger devient instable* ». La prédiction judiciaire fait donc peser un risque sur l'office du juge en ce qu'il pourrait conduire à sa disparition pure et simple ou tout au moins à la raréfaction des affaires qui lui seraient soumises en réduisant celles-ci aux seuls cas non répertoriés dans la jurisprudence numérique. Recueillant, exploitant et analysant l'ensemble des décisions de justice, sachant qu'à elle seule la Cour de cassation dispose d'une base de données de 1,5 millions d'arrêts, une intelligence artificielle pourrait bien rendre des décisions de manière autonome. A l'image du logiciel *Watson* qui propose des diagnostics médicaux sur la base de l'analyse de centaines de critères, l'analyse d'un dossier judiciaire pourrait également s'effectuer par simple consultation d'un algorithme. Aux Etats-Unis, la police utilise déjà ce type de logiciel afin de prédire les infractions en fonction de milliers de paramètres statistiques (géographie, météo, données sociales, consultations google, publications sur les réseaux sociaux…).

Bien évidemment, comme tous les outils numériques d'accès ouvert, ces logiciels et bases de données sont exposés aux intrusions malveillantes dont on imagine les effets dévastateurs. Ainsi, comme le souligne Myriam Quéméner, magistrate et conseiller juridique auprès du délégué ministériel en charge de la lutte contre les cybermenaces : « *lutter efficacement contre la cybercrimnalité est un enjeu*

majeur pour les années à venir. Cette démarche est indissociable de l'amélioration de la connaissance des nouveaux vecteurs d'information tels qu'Internet et les réseaux numériques ».

Déjà, l'organisation judiciaire entend s'adapter à ces nouvelles menaces et les anticiper. Ainsi, en septembre 2014, les services du parquet de Paris ont été réorganisés afin d'être plus efficaces dans le traitement des dossiers financiers, de cybercriminalité et de santé publique. Désormais, le parquet financier de Paris comporte une section dédiée à la cybercriminalité (section F1) au sein de la division économique, financière et commerciale[2]. Le parquet de Paris demeure cependant le seul à disposer d'une section spécialisée dans la lutte contre « *la délinquance astucieuse et la cybercriminalité* ». Elle traite plus particulièrement des dossiers d'atteintes aux systèmes de traitement automatisé de données commises à l'encontre des services de l'Etat et des entreprises situés à Paris.

(2) Au delà d'une spécialisation, la juridiction parisienne dispose depuis la loi du 3 juin 2016 d'une compétence nationale concurrente en matière d'attaques informatiques (atteintes aux STAD).

Les Juridictions interrégionales spécialisées (JIRS) ont à connaître de nombreux cas de cybercriminalité de même que plusieurs cours d'appel qui ont désigné au sein de leurs effectifs des magistrats référents pour les questions de cyberterrorisme.

Enfin, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a reconnu à tout juge d'instruction la possibilité de décider de la captation à distance des données informatiques, dans le cadre des dispositions spécifiques relatives à la criminalité et à la délinquance organisée.

L'enjeu est donc de maintenir le processus de spécialisation judiciaire amorcé avec la création d'un pôle spécialisé au sein du parquet de Paris. Comme nous l'avons vu, les cybermenaces sont multiples, complexes et diffuses et recommandent de ce fait la création de structures adaptées et spécialisées.

De surcroît, nous faisons face à une délinquance de masse, où les infractions sont ventilées façon puzzle sur l'ensemble du territoire. Par conséquent, le regroupement des infractions (au niveau des JIRS par exemple) doit permettre d'étoffer un dossier pour ensuite rendre plus légitime le recours à une coopération internationale.

AUTEUR

Xavier Leonetti intègre l'école des officiers de la gendarmerie nationale en 2002. Après un commandement opérationnel à la compagnie de gendarmerie départementale de Castellane, il revient à l'école des officiers de la gendarmerie nationale comme officier professeur en 2008. Il rejoint en 2010 la direction générale en tant que responsable du service national « sécurité et intelligence économiques ». Il intègre les rangs de la magistrature en 2016 en tant que substitut du procureur au parquet général d'Aix-en-Provence
Docteur en droit, il enseigne au sein du Master 2 « Management de l'information » auprès de l'Université Paul-Cézanne – Aix-Marseille III. Il a publié des ouvrages : « Guide de cybersécurité », Paris, l'Harmattan, octobre 2015. – « La France est-elle armée pour la guerre économique ? », Paris, Armand Colin, avril 2011. – « Les outils de l'intelligence économique », Presses de Science-Po Aix, novembre 2000.

Fotolia

L'ÉDICTION DE DONNÉES ILLICITES SUR UNE AUTOROUTE DE L'INFORMATION DOIT ETRE REGULÉE

La couche sémantique du net implique un contrôle des contenus sensibles. S'il est vrai que l'intelligence artificielle aidera à détecter les signaux illégaux, la capacité de cerner juridiquement l'émetteur de l'information reste délicate notamment en matière de nébuleuse terroriste. La répression des contenus illicites comporte une adaptation aux infractions existantes et touche également les atteintes à l'image et à la dignité des personnes. S'il subsiste un questionnement sur l'autorité qui peut demander le déréférencement de sites, on notera que les dispositions légales rendent responsable l'éditeur des données qui a une obligation d'agir. En tout état de cause, l'accord trouvé entre les majors de l'Internet et le G7 sur la suppression de contenus à caractère terroriste dans les deux heures après leur mise en ligne est une solution pragmatique.

La couche sémantique
de l'espace numérique : espace de liberté ou d'asservissement ?

Par MARC WATIN-AUGOUARD

Depuis la loi Godfrain (1988), les cyberattaques sont le principal sujet de préoccupations, parce qu'elles visent la « couche logique » en atteignant les systèmes de traitement automatisés de données avec un impact de plus en plus redoutable. Il suffit pour s'en convaincre de constater les conséquences du botnet Mirai ou des rançongiciels Wanacry ou NotPetya. Les enjeux relèvent d'une stratégie de cyberdéfense qui doit être soutenue par des moyens dont la croissance est encore nécessaire. Mais, aujourd'hui, la « *couche sémantique* » révèle aussi sa sensibilité et sa dangerosité.

MARC WATIN-AUGOUARD

Général d'armée (2S) de gendarmerie - directeur du centre de recherche de l'école des officiers de la gendarmerie nationale.

La donnée est au cœur de la transformation numérique. L'hyperconnexion la multiplie. C'est elle qui, collectée, traitée, échangée, est porteuse de contenus et donc de sens. Déjà, l'explosion sur la toile du nombre de sites pédopornographiques a justifié l'intervention du législateur et la nécessité d'un contrôle des contenus. Mais, avec l'irruption de la propagande terroriste de Daech (19 000 sites « *défacés* » en janvier 2015) et, plus récemment, avec le cyber-harcèlement ou la manipulation des esprits *via* de fausses nouvelles (*fake news*) à l'occasion d'élections, les regards se portent de plus en plus sur les contenus illicites véhiculés au travers de l'espace numérique. Au risque de pécher par optimisme, on pourrait prédire que la cybersécurité des systèmes sera de mieux en mieux assurée, notamment en amont, à l'aide de l'intelligence artificielle, par la détection des menaces (threat intelligence, analyse des signaux faibles grâce au *Big data*, cyberdéfense, cybersécurité cognitive, *etc.*) et le recours à des mesures de

prévention (sécurité dès la conception, certification, etc.). En revanche, il y a fort à parier que le maillon faible sera l'individu. Sans prise de conscience, l'humain pourrait devenir esclave ou zombie d'un internet pourtant conçu pour être un espace de liberté. Les contenus illicites ont fait l'objet de l'attention du législateur qui les a incriminés au fur et à mesure de leur apparition. Leur consultation habituelle est dans certains cas poursuivie, non sans faire parfois débat. Il est aussi nécessaire d'agir à la source, en entravant les possibilités d'accès aux contenus litigieux. Dans toutes ces hypothèses, l'action des services de l'Etat est nécessaire. Mais elle ne peut être suffisante sans une meilleure concertation avec les « *majors* » d'internet qui doivent être davantage associés à la régulation des contenus illicites.

L'incrimination des contenus illicites et de leur consultation

La répression des contenus illicites et de leur diffusion résulte généralement de l'adaptation à l'espace numérique d'infractions déjà existantes ou de leur aggravation par usage d'un moyen de communication en ligne. Il en est ainsi de la pédopornographie, de l'apologie du terrorisme, des infractions à la loi du 29 juillet 1881 (diffamation, injure publique, incitation à la haine, *etc.*). Le code pénal témoigne aussi de la nécessaire adaptation du droit à des comportements facilités par l'évolution des technologies et donc aux nouveaux mésusages que celles-ci permettent.

Le « *vidéo-lynchage* », la « *vengeance pornographique* », le harcèlement moral ou sexuel en ligne sont la conséquence de la démocratisation des terminaux mobiles et de l'essor des réseaux sociaux. Ces infractions, on le voit bien, atteignent la victime dans son image, sa représentation, son intimité, sa dignité. Elles peuvent exprimer une forme de violence psychique ou morale qui rejoint ou suscite la violence physique dans le monde réel.

Au-delà de l'illégalité des contenus, s'est posée la question de celle de leur accès. La consultation habituelle de sites pédopornographiques a été incriminée par la LOPPSI (mars 2011), sans que le principe ne suscite de controverse. Plus discutée, en revanche, est l'infraction de consultation habituelle de sites provoquant au terrorisme ou en en faisant l'apologie. Issue de la loi du 3 juin 2016, elle a été censurée par le Conseil constitutionnel puis réécrite par la loi du 27 février 2017 avant de faire récemment l'objet d'une QPC transmise par la Cour de cassation. Si les sites pédopornographiques ne soulèvent pas d'ambiguïté, les sites à caractère terroriste sont plus subjectifs et exigent une loi dont la clarté respecte le principe de légalité.

Quel juge pour la police des contenus ?

Pour éviter la consultation des sites illicites, une autre voie est possible : celle du retrait, du blocage ou du déréférencement par l'autorité judiciaire ou au titre de la police

administrative. Ces mesures s'adressent à des opérateurs de plateformes qui ont été définis par la loi pour la confiance dans l'économie numérique et par la loi pour la République numérique : les fournisseurs d'accès, les hébergeurs, les éditeurs, les moteurs de recherches. L'éditeur est pénalement responsable des contenus figurant sur son site, car c'est lui qui les crée, les choisit, les organise, les assemble et les hiérarchise. Les autres acteurs n'ont qu'une obligation d'agir dès qu'ils ont connaissance de l'illégalité des contenus auxquels ils permettent l'accès.

L'autorité judiciaire peut prescrire, en référé ou sur requête, aux hébergeurs ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne. Ainsi l'arrêt d'un service de communication au public en ligne peut être prononcé par le juge des référés, à la demande du ministère public et de toute personne physique ou morale ayant intérêt à agir, pour les faits d'apologie ou de provocation au terrorisme, lorsqu'ils constituent un trouble manifestement illicite.

Considérant que le juge judiciaire est le gardien de la liberté individuelle, certains parlementaires et la plupart des acteurs d'internet (le Conseil national du numérique en particulier) voudraient lui donner le monopole de toute intervention relative aux contenus, eu égard à l'atteinte portée à la liberté d'expression par une mesure de retrait ou de blocage.

Sur le recours à une procédure de police administrative, le rapporteur de la loi à l'Assemblée nationale, Sébastien Pietrasanta, a considéré que « *ce que l'autorité administrative peut faire dans la sphère réelle pour protéger l'ordre public, elle doit également pouvoir le faire dans la sphère numérique*[1] ». Bernard Cazeneuve a renchéri en ces termes : « *Si des appels se produisaient sur un autre espace public, un autre espace de liberté, et non sur la Toile, l'espace numérique, je suis convaincu que tous ceux qui siègent dans l'hémicycle me demanderaient les raisons pour lesquelles je ne fais pas cesser le trouble à l'ordre public, et ils auraient toute légitimité à la faire. Mais dès lors qu'il s'agirait d'internet, il ne serait plus possible de procéder ainsi parce que la prévention du risque et la mesure de police en vue de rétablir ou d'assurer l'ordre public serait liberticides !*[2] ».

(1) Débats à l'Assemblée nationale, séance du 15 septembre 2014.

(2) Sénat, séance du 15 octobre 2014.

Quant à l'intervention du juge judiciaire, par préférence au juge administratif, Jean Jacques Hyest, rapporteur de la loi au Sénat, a déclaré : « Certains voudraient que la justice judiciaire s'occupe de tout. Mais le rôle de la justice judiciaire, c'est de réprimer ! Et si l'on commence à tout

mélanger, à faire intervenir le juge judiciaire dans les affaires de police administrative, on détruira en partie un édifice auquel beaucoup d'entre nous sont attachés[3] ». Les opposants à la police administrative spéciale, précisée par les décrets du 5 février 2015[4] et du 4 mars 20155 n'ont finalement pas eu gain de cause devant le Conseil d'État[6] .

La procédure est désormais rodée : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) applique un principe de subsidiarité : il s'adresse d'abord aux éditeurs et hébergeurs afin qu'ils retirent les contenus dans un délai de 24 heures. En cas d'échec, ou directement si l'éditeur ou l'hébergeur ne peuvent être identifiés[7] (dans la pratique, ils le sont très rarement, car résidant à l'étranger), les fournisseurs d'accès sont invités à bloquer l'accès au (x) site(s) incriminé (s). L'office a également le pouvoir de s'adresser directement aux moteurs de recherche ou aux annuaires pour qu'ils cessent de référencer les sites illicites. Toutes ces opérations sont placées sous le contrôle d'une autorité qualifiée désignée en son sein par la CNIL. Dans son dernier rapport (2017), Alexandre Linden, conseiller honoraire près la Cour de cassation, indique que 5512 demandes ont été adressées par l'OCLCTIC sur une période de douze mois : 874 demandes de blocage de sites, 2 561 demandes de retrait de contenus, 2 077 demandes de déréférencement d'adresses électroniques provoquant à des actes de terrorisme ou en faisant l'apologie, ou à caractère pédopornographique. Les contenus à caractère terroriste représentent 60 % des contrôles opérés. Comme en 2016, Alexandre Linden n'a constaté aucun cas de surblocage, risque mis en avant par les opposants à la loi lors de son l'élaboration. Si le bilan est globalement rassurant, il met en évidence les faibles moyens de l'autorité qualifiée au regard d'une mission dont l'étendue est croissante.

(3) Jean-Jacques Hyest, Sénat, séance du 15 octobre 2014.

(4) Décret n°2105-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

(5) Décret n°2105-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

(6) CE. 2e et 7e SSR Association French Data Network et autres du 15 février 2016.

(7) Par exemple, si l'éditeur ne fournit pas les informations prévues par l'article 6-III de la LCEN (identité, domicile, raison sociale).

L'indispensable coopération avec les « *majors* » d'internet

Les chiffres présentés, quelle que soit leur progression, restent très faibles au regard de l'ampleur des phénomènes incriminés. En près deux années (2015-2017), Twitter annonce avoir supprimé sur l'ensemble de la planète 900 000 comptes faisant l'apologie du terrorisme, dont 300 000 pendant les six premiers mois de l'année 2017. Facebook emploie plus de 150 personnes pour lutter contre les contenus illicites. Ces statistiques expliquent sans doute pourquoi Daech a menacé Mark Zuckerberg et Jack Dorsey, respectivement patrons de Facebook et de Twitter, pourtant souvent accusés de ne pas assez lutter contre le

Sdecoret - Adobe Stock

Les autoroutes de la désinformation ouvertes par l'hyperconnexion rendent impératives des mesures de régulation associant une intelligence artificielle et une intervention humaine.

cyberterrorisme. Lors de leur rencontre, le 13 juin 2017, Theresa May et Emmanuel Macron ont annoncé la mise au point d'un plan d'action contre la propagande djihadiste sur internet. Le lendemain, Facebook a présenté des mesures.

Plus répressive, l'Allemagne veut montrer sa détermination en promulguant une loi[8] obligeant les réseaux sociaux à supprimer les messages haineux dans les 24 heures et de ne pas republier un contenu déjà supprimé, sous peine d'amende pouvant atteindre 50 millions d'euros.

Les réseaux sociaux ne sont pas insensibles aux contenus dont ils favorisent la diffusion, pour le meilleur comme pour le pire, mais ils sont souvent accusés de laxisme. Peu après les attentats de janvier 2015, le ministre de l'Intérieur a décidé d'approfondir le dialogue avec les réseaux sociaux, mission aujourd'hui dévolue à la Délégation interministérielle aux industries de sécurité et à la lutte contre les cybermenaces. Faisant suite au conseil Justice Affaires Intérieures (JAI) extraordinaire du 24 mars 2016, après les attentats de

(8) (NetzDG) approuvée en Conseil des ministres fédéraux le 5 avril 2017 et entrée en vigueur le 1er octobre 2017. Le texte suscite de nombreuses critiques venant notamment de ceux qui craignent un excès de zèle au regard des sanctions encourues.

Bruxelles, la Commission européenne a établi, en mai 2016, un Code de bonne conduite avec Facebook, Twitter, Youtube et Microsoft pour empêcher la propagation de discours haineux illégaux en ligne.

Comprenant sans doute que la pression internationale augmentait, ces mêmes acteurs se sont unis au sein du *Global Internet Forum to Counter Terrorism* (GIFCT) pour détecter les contenus terroristes. Une base de données partagées permet d'identifier les contenus déjà supprimés, tandis que l'intelligence artificielle identifie les nouveaux avec l'aide de personnes qualifiées, car l'apport de l'humain est ici indispensable pour faire la distinction entre la propagande et la liberté d'expression ou d'information.

Le G7 et les majors d'internet (Google, Facebook, Twitter) se sont réunis en octobre 2017, sur l'île italienne d'Ischia pour sceller un accord ayant pour objectif de supprimer les contenus à caractère terroriste dans les deux heures suivant leur mise en ligne. Cet accord supposait que les Etats-Unis fassent preuve de plus de discernement dans l'application du Premier amendement de la Constitution qui privilégie la liberté d'expression. Les européens ont obtenu gain de cause.

La redoutable matérialité du discours sur le web

Avec quatre milliards d'internautes en 2020, un développement fulgurant de la mobilité et des systèmes connectés, avec des services de communication en ligne et des réseaux sociaux qui se développent et permettent une transmission d'informations d'une viralité redoutable, nous voyons émerger la dimension cognitive de l'espace numérique. Avec elle se démultiplie la puissance du verbe, du discours. En 1970, Michel Foucault disait dans sa leçon introductive au Collège de France : « *Je suppose que dans toute société la production du discours est à la fois contrôlée, sélectionnée, organisée et redistribuée par un certain nombre de procédures qui ont pour rôle d'en conjurer les pouvoirs et les dangers, d'en maîtriser l'événement aléatoire, d'en esquiver la lourde, la redoutable matérialité* ».

Depuis, le web, les réseaux sociaux ont profondément modifié nos modes d'expression. La pensée foucaldienne peut-elle encore expliquer le discours, tant la production, la sélection, la redistribution du discours échappent aujourd'hui aux procédures traditionnelles ? Dans une interview au Guardian[9], le 12 mars 2017, Sir Tim Berners Lee s'inquiétait de l'évolution du web qu'il faut, selon lui, sauver, notamment parce qu'il est utilisé pour des actions de désinformation qui peuvent avoir des fins politiques ou financières. Les « *autoroutes de l'information* » peuvent se transformer en « *autoroutes de la désinformation* ». Selon lui, les moteurs de recherche et les réseaux sociaux font de la surenchère avec des nouvelles choquantes, surprenantes, complaisantes qui peuvent être des fausses nouvelles (*fake news*). Si les contenus illicites sont, depuis plusieurs années, au cœur des

(9) Tim Berners-Lee, "I invented the web. Here are trhree things we need to change to save it", The Guardian, 12 mars 2017.

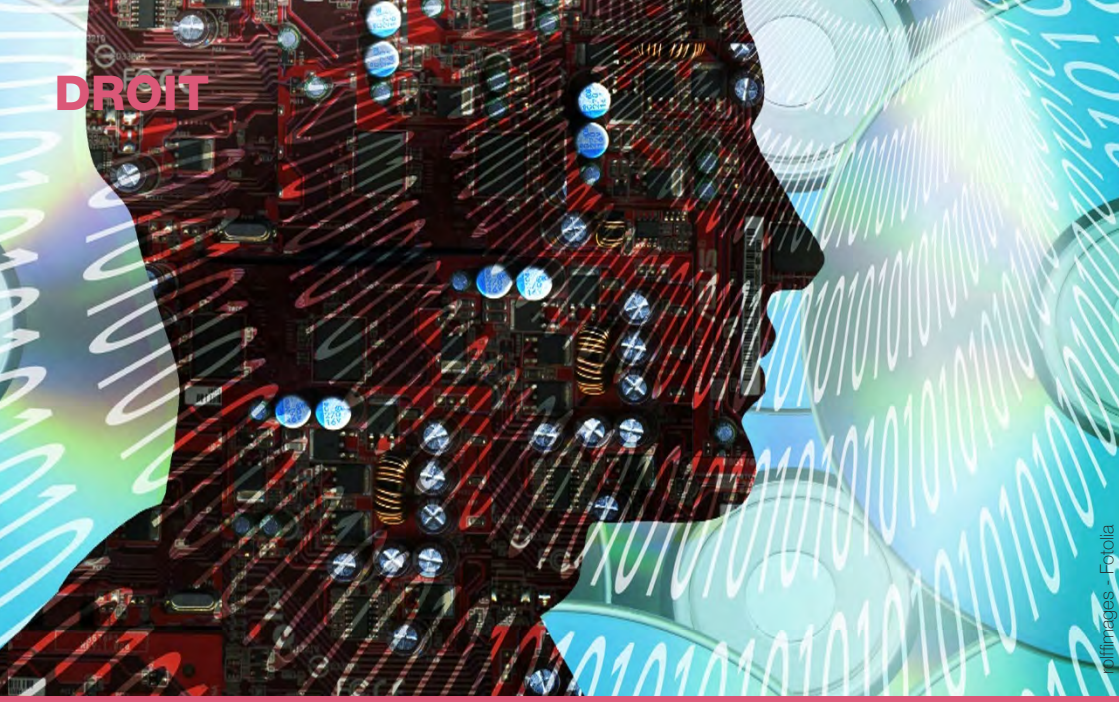
préoccupations, l'utilisation des réseaux sociaux à des fins d'influence et, pire, en vue d'intimider ou de manipuler, est mise en exergue, notamment depuis les élections américaines de 2016.

(10) Facebook est également mis en cause pour le rôle joué lors du referendum du Brexit.

Le Congrès américain a ouvert une enquête sur les ingérences lors de la campagne, par le biais notamment de publicités ciblées émanant des Russes. Google, Twitter, mais surtout Facebook[10] ont été convoqués le 1er novembre 2017 pour se faire reprocher leur inefficacité. Richard Burr, président de la Commission d'enquête leur a demandé davantage de coopération : « *Ne laissez pas d'autres nations perturber notre avenir. Vous êtes notre première ligne de défense. Faites remonter le message à vos entreprises* ». La sénatrice démocrate de Californie, Diane Feinstein, s'est montrée plus directe : « *J'ai longtemps été très fière de représenter cette communauté de la Silicon Valley. Mais franchement, je pense que vous n'avez pas compris. Ce dont on parle ici est un changement cataclysmique. On parle de cyberguerre* ».

Devant la Commission, a été montrée du doigt l'Internet *Research Agency*, société de Saint-Pétersbourg liée aux services de renseignement russe. Cette entreprise a créé, dès 2015, des milliers de faux comptes (trolls) se faisant passer pour des Américains et créant des faux pour susciter des incidents. Selon les chiffres avancés devant les parlementaires, 80000 messages de propagande politique, qui auraient été vus par 126 millions d'Américains, auraient été publiés entre juin 2015 et août 2017. En septembre 2017, lors d'une perquisition dans les locaux de Facebook, le FBI a mis en évidence le versement de 100000 dollars par des organismes proches du gouvernement russe pour insérer plus de 3000 publicités ciblées, nombre d'entre elles étant des fausses nouvelles.

La fragilité de la couche cognitive est sans doute la tendance lourde des prochaines années. Dans cette perspective, il y a fort à parier que le « maillon faible » sera demain, plus qu'aujourd'hui encore, celui des contenus qui viseront des individus abandonnés dans un désert surpeuplé de solitaires. Sans recul, sans esprit critique, sans discernement, les proies fragiles tombent et tomberont plus encore dans le piège d'un mécanisme d'endoctrinement qui emprunte la dangereuse efficacité des dérives sectaires. Du contresens vers le non-sens, le parcours offert aux esprits les plus réceptifs leur offre une lecture déformée par le prisme de la haine. Cela nous invite à replacer d'urgence l'humain au cœur de cyberespace et pose sans doute en des termes inédits la question de l'équilibre entre sécurité et liberté. Comment concilier la lutte contre les contenus illicites sans multiplier les mesures intrusives ? La réponse est sans doute davantage dans la « *soft law* », dans les comportements que dans la loi.



pfinnages_Fotolia

L'ANONYMISATION, UNE TECHNOLOGIE IMPÉRATIVE QUI DOIT ÊTRE ENCADRÉE

Toute accumulation de données dans une base prête à des traitements qui peuvent déroger à la protection de la vie privée des personnes. L'intérêt majeur de la méthode de l'anonymisation est d'empêcher l'isolement d'un individu, de corréler ses informations avec d'autres données et d'en déduire des informations (avis du G 29 d'avril 2014). Cela est d'autant plus important que des dispositions nouvelles visent à mettre en ligne des données publiques et que les pratiques de marketing deviennent sophistiquées et agressives sur des profils ciblés.

Toutefois, une escalade technologique rend plus efficientes les disciplines de réidentification au travers du codage et de recherches croisées. La CNIL dans une posture de contrôle de validité des processus d'anonymisation, le G 29 par son affinement de ses critères et le RGPD, qui par son article 35 préconise une analyse d'impact de ce processus, une prise en compte en amont lors de la conception des applications et l'émission d'une norme, entrent dans un système de régulation de techniques qui peuvent porter atteinte aux droits fondamentaux de la personne.

Le paradoxe juridique
de l'anonymisation des données

Par SABINE MARCELLIN

Dans un contexte de diffusion exponentielle de données, l'anonymisation est l'une des méthodes permettant de les sécuriser. De grands volumes de données peuvent faire l'objet de traitements à des fins de statistiques ou de marketing, à condition de répondre aux exigences légales. L'anonymisation peut contribuer naturellement à la protection de la vie privée des personnes, voire permettre de limiter l'application de la réglementation relative aux données anonymisées. Mais sachant qu'aucune technique n'est totalement infaillible, comment le droit français ou européen appréhende-t-il cette procédure ?

SABINE MARCELLIN

Avocate of counsel Staub et associés

Définition de l'anonymisation

L'anonymisation des données ne fait pas l'objet de définition légale. Seules des définitions techniques sont proposées dans les normes volontaires[1], parmi lesquelles on peut relever celle-ci : « *Procédé selon lequel une donnée à caractère personnel est modifiée irrévocablement d'une manière telle que la personne concernée ne puisse plus être identifiée directement ni indirectement, ni par le responsable de fichier ni par un tiers*[2] ». L'anonymisation doit être clairement différenciée de la pseudonymisation. La peudonymisation consiste à remplacer un attribut par

(1) Une norme volontaire est un cahier des charges élaboré par les acteurs concernés réunis de manière représentative par l'AFNOR. Ce n'est pas une loi et elle n'a pas de caractère impératif. Elle traduit la volonté des acteurs et notamment des entreprises de respecter une référence de qualité du produit ou du service. C'est un cadre révisable cycliquement.

(2) Traduction libre issue de la norme ISO 29100. Version anglaise : *Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party.*

Collection Marcellin

L'anonymisation pose les problématiques des techniques de réidentification et de sa reconnaissance dans les systèmes juridiques français et européens.

un autre, mais l'identification indirecte de la personne reste possible par celui qui a connaissance des attributs modifiés. Prenons l'exemple du nom d'une personne qui serait remplacé par un chiffre. Si ce chiffre, obtenu de manière simple ou complexe (clef de chiffrement) peut être associé au nom, en raison de l'existence de la table de correspondance, il reste possible de retrouver le patronyme. Avec la pseudonymisation, nous restons en présence de données personnelles. En revanche, l'anonymisation est une modification d'attribut irrévocable qui ne permet donc plus, en théorie, d'identifier une personne.

Pourquoi anonymiser ?

Les motivations de l'anonymisation sont multiples et reposent sur la volonté de traiter des informations sans porter atteinte aux droits des personnes. Les applications sont vastes, pour permettre notamment des pratiques innovantes de marketing, de poursuivre le développement de l'open data, c'est-à-dire l'ouverture des données publiques, ou de favoriser les progrès de la recherche médicale.

Techniques d'anonymisation

Les techniques d'anonymisation reposent sur des outils de codage : algorithme, chiffrement, table de correspondance, etc. Les mécanismes majeurs sont la randomisation

et la généralisation. La randomisation est une altération de la véracité des données afin d'affaiblir le lien entre ces données et l'individu. Plusieurs méthodologies permettent cette altération, notamment l'ajout de bruit, la permutation et la confidentialité différenciée. Par exemple, l'ajout de bruit consiste à ajouter aux variables exactes des variables modifiées tout en conservant certaines propriétés statistiques.

La généralisation, quant à elle, dilue les attributs des personnes concernées en modifiant leur échelle ou leur ordre de grandeur respectif. Par exemple : généralisation par regroupement d'enfants de 2 à 5 ans dans un groupe intitulé jeunes enfants.

Pour cela, il existe différentes méthodologies dont le K-anonymat, le L-diversité et le T-proximité[3].

(3) Techniques d'anonymisation, Benjamin Nguyen, Statistique et société, décembre 2014.

(4) La protection des données personnelles dans l'open data : une exigence et une opportunité, Sénat, Rapport d'information n° 469, de MM. Gaëtan Gorce et François Pillet, déposé le 16 avril 2014.

Quelles sont les limites de l'anonymisation ?

Etape utile vers la protection de la vie privée, le recours à l'anonymisation ne semble pas toujours un moyen facile d'accès, car il nécessite des connaissances techniques et l'usage de logiciels appropriés.

De plus, les données anonymisées peuvent toujours comporter des risques pour la vie privée. Les technologies évoluent, tant celles de l'anonymisation que celles de la réidentification. Aucune technique d'anonymisation n'est en théorie infaillible[4]. Ainsi, la sécurité offerte par les procédés d'anonymisation dépend de la confidentialité et de la solidité des outils de codage utilisés mais aussi des données auxquelles ils sont appliqués. Les liens établis entre les données sont parfois aussi identifiants que chacune de ces données prises isolément.

Des illustrations concrètes nous démontrent cette problématique de ré-identification. L'entreprise américaine AOL, fournisseur d'accès Internet, a publié en ligne, en 2006, une base de données qui rassemblait 20 millions de recherches effectuées sur son site par 650 000 utilisateurs. L'objectif de l'opérateur était d'illustrer l'étendue des services qu'il proposait. La base avait été anonymisée en remplaçant chaque identifiant (nom d'utilisateur, adresse IP, *etc.*) par un nombre choisi aléatoirement. L'opérateur avait cependant négligé que l'historique de recherche d'un individu est identifiant ainsi que les recherches sur des services de proximité. Le résultat de cette opération fut que certains internautes furent réellement identifiés.

Un autre exemple de réidentification porte sur l'offre de service de location en ligne de films par l'entreprise américaine Netflix. La notation des films permet à l'entreprise de proposer aux utilisateurs des films susceptibles de leur plaire. Souhaitant affiner ses programmes d'analyse des préférences

des utilisateurs, l'entreprise a publié en ligne, en 2008, les recommandations de 500 000 d'entre eux, afin que des programmeurs indépendants développent des applications plus performantes que le logiciel utilisé par l'entreprise. L'entreprise avait pris le soin d'anonymiser les données directement identifiantes et de modifier légèrement les autres.

Un prix d'un million de dollars était en jeu. Deux informaticiens, Arvind Narayanan et Vitaly Shmatikov, sont parvenus à percer cette anonymisation et à réidentifier plusieurs profils d'utilisateurs. Ils se sont aperçus que la seule information donnée par le croisement entre l'appréciation portée sur trois films et la date à laquelle ils ont été loués, était suffisante pour retrouver l'auteur de ces appréciations, s'il avait fait état d'appréciations identiques aux mêmes dates sur un autre site dans lequel il apparaissait sous sa véritable identité.

Les exemples de réidentification ne sont pas seulement américains. Comme cité dans le rapport du Sénat sur les données personnelles et l'*open data* : « *L'INSEE, dont le travail est pourtant souvent exemplaire du point de vue de la protection des données personnelles, a été, au début de l'année 2013, à l'origine d'une fuite sur l'imposition de certains contribuables. En effet, recourant à la technique du carroyage, l'institut a divisé la France en carrés de 200 mètres de côté, en associant à ces carreaux l'imposition moyenne des habitants concernés. Ces données furent publiées sur internet, dans le cadre d'une démarche d'*open data*. Il s'est cependant avéré que certains carrés, situés dans des territoires peu peuplés, ne comptaient qu'un seul foyer fiscal, dont il était aisé, ensuite, de retrouver l'adresse et donc l'identité. L'institut a depuis revu sa méthodologie* ».

Si les risques de réidentification sont considérés comme limités, les conséquences de publication de données personnelles sont susceptibles d'être graves pour les personnes concernées comme pour les responsables de traitement.

La gravité de l'atteinte portée aux intéressés dépend de la nature des informations en cause et de la portée de la diffusion accidentelle. Dans un tel cas, la responsabilité de l'entreprise ou l'administration responsable pourrait être engagée du fait de négligences commises.

Comment la réglementation appréhende l'anonymisation ?

La loi Informatique et Libertés[5] fait référence à l'anonymisation, comme moyen permettant le traitement des données sensibles (art.8) et comme raison de limiter l'obligation d'informer les personnes pour le responsable de traitement (art. 32.IV).

(5) Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés.

Cependant, le principe essentiel qui permet d'analyser la valeur légale de l'anonymisation repose sur l'une des clefs de la loi à savoir l'identification de la personne (art.2) : « *Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.* »

(6) Guide CNIL, La sécurité des données personnelles - Fiche n° 16, 2010.

(7) Délibération n° 2015-255 du 16 juillet 2015, société JCDecaux.

Quelle est l'approche de la CNIL en matière d'anonymisation[6] ? La Commission a indiqué, dans une délibération de juillet 2016[7] que « *pour qu'une solution d'anonymisation soit efficace, elle doit empêcher toutes les parties d'isoler un individu dans un ensemble de données, de relier entre eux deux enregistrements dans un ensemble de données (…) et de déduire des informations de cet ensemble de données* ». Dans le cas d'analyse des parcours piétons à partir de la captation des adresses MAC de leurs terminaux mobiles, la CNIL a considéré que l'anonymisation par chiffrement irréversible des adresses ne permettait pas de respecter le droit des personnes. La CNIL a refusé d'autoriser ce dispositif de mesure d'audience.

En octobre 2016, la loi pour une République numérique a introduit une nouvelle référence à l'anonymisation dans la loi Informatique et Libertés (art 11.3) : « *A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements (la CNIL) donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis (…)* ». Cette mission de la CNIL permettra aux acteurs de disposer d'un avis du régulateur sur leurs systèmes d'anonymisation.

(8) Conseil d'Etat 12 mars 2014, n° 354629.

(9) Conseil d'Etat 23 mars 2015 n° 353717

(10) Conseil d'Etat 19 juin 2017, n° 396050.

Plus généralement, la jurisprudence française a considéré que les décisions de justice ne peuvent être rendues anonymes que lorsqu'elles portent atteinte à l'intimité des personnes[8]. Un autre arrêt indique que les décisions de justice doivent être anonymisées sur les sites juridiques[9]. Par ailleurs, le Conseil d'État[10] a considéré, en juin 2017, que la CNIL doit anonymiser le nom des sociétés qu'elle sanctionne, deux ans après la publication de ses décisions, afin que cette sanction ne soit pas abusive.

Quel est le cadre européen ? Le G29 (groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales) a publié un avis sur les techniques d'anonymisation en avril 2014. Ce texte présente une analyse de l'efficacité et des limites des techniques d'anonymisation existantes dans le contexte juridique de la protection des données. Pour aider à évaluer une solution d'anonymisation, le G29 propose trois critères :

– L'individualisation : est-il toujours possible d'isoler un individu ?
– La corrélation : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?
– L'inférence : peut-on déduire de l'information sur un individu ?

Le Règlement européen de protection des données[11] ou RGPD du 27 avril 2016, indique dans son considérant 26 que : « *Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche* ».

(11) Règlement 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.

Ce choix y est explicité par l'application des principes essentiels de protection des données de personnes identifiées ou identifiables : « (…) *Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par tout autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable* ».

Cette position d'exclusion des données anonymisées repose sur l'analyse du considérant 26 qui fait référence à l'identification des personnes. Pour déterminer si une personne est identifiable, il faut prendre en compte l'ensemble des moyens raisonnablement susceptibles d'être utilisés. Pour comprendre ce que sont des moyens « *raisonnablement susceptibles* » d'être utilisés pour identifier la personne, doivent être pris en compte l'ensemble des critères objectifs :

– le coût de l'identification,
– le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.
– le coût et le temps sont bien des facteurs objectifs mais nous ne disposons pas ici d'indication permettant de les évaluer.

Beaucoup d'interrogations subsistent à la lecture de ce considérant. Un responsable de traitement pourrait-il se voir reprocher que des données anonymisées soient réidentifiées, si les moyens utilisés reposent sur une technologie adéquate au moment de la mise en œuvre du traitement ? Comment sera assurée la protection des données qui deviendraient personnelles indépendamment de la volonté du responsable ? Comment sa responsabilité peut-elle être mesurée ?

La réglementation française et européenne relative aux données personnelles appréhende l'anonymisation comme un moyen parmi d'autres de sécuriser les données. Le RGPD exclut les données anonymisées du champ de son application. L'avis du G29 souligne le fait qu'aucun procédé n'est infaillible et formule des recommandations sans donner de directives pour limiter ces risques. Les textes restent théoriques et ne donnent que peu d'indications sur les exigences du processus lui-même.

Sur le plan juridique, les acteurs des données personnelles (responsable de traitement, sous-traitant, éditeur de solutions d'anonymisation, conseil en sécurité du numérique, *etc.*) restent dans une situation paradoxale. L'anonymisation fiable peut permettre d'échapper aux exigences de la protection des données personnelles. Mais en cas de faille, les acteurs sont susceptibles de se trouver dans une situation difficile. Leur traitement de données risque de ne plus être en conformité par rapport au RGPD et leur responsabilité pourrait être engagée face aux personnes victimes de divulgation des données.

Quelles solutions d'accompagnement de l'anonymisation ?

Le cadre législatif de l'anonymisation est évolutif et peu rassurant pour les acteurs. Placés face à ce choix d'anonymat des données, ils doivent préalablement procéder à une analyse de risques adaptée aux finalités. Afin de minimiser les risques de désanonymisation, quelles seraient les solutions d'accompagnement envisageables selon les spécialistes[12] ?

• Réaliser une analyse d'impact (art. 35 du RGPD) pour tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes[13] ;

• Faire intervenir l'anonymisation en amont du traitement, afin de manipuler dès que

(12) De-identification of personal Information, Simson L. Garfinkel, National Institute of Standards and Technology, October 2015.

(13) Article 29 Working Party (WP29) Guidelines on Data Protection Impact Assessments, April 2017.National Institute of Standards and Technology, October 2015.

possible des données transformées et non brutes ;

• Recourir à l'anonymisation comme mode de sécurisation des informations personnelles au sein d'une palette d'autres mesures sécuritaires : solutions organisationnelles, techniques et logiques, accompagnées de mesures de contrôle et de sensibilisation des intervenants ;

• Créer des normes pour éprouver l'efficacité des méthodes, sachant qu'une norme ISO traitant des techniques d'anonymisation des données personnelles est en cours d'élaboration[14] ;

•Renforcer la protection des données par une construction contractuelle pour clarifier les rôles et responsabilités des acteurs.

La situation paradoxale de l'anonymisation est peu satisfaisante sur le plan juridique[15]. Les incertitudes juridiques sur ses effets pour la protection des données affectent certainement l'usage de ces mesures[16] et nuisent à l'analyse du risque tant pour les responsables que les personnes concernées.

(14) ISO 20889 Privacy enhancing data deidentification techniques.

(15) Anonymisation et pseudonymisation – « Unique dans la foule » : l'impossible anonymisation de l'analyse des flux piétons, Nathalie Metallinos, Communication Commerce électronique, juin 2016.

(16) Samson Y. Esayas, The role of anonymisation and pseudonymisation Under the EU data privacy rules, European Journal of law and technology, vol.6, October 2015.

NOTES

NOTES

DIRECTEUR DE LA PUBLICATION

Général de division **Philippe Guimbert**

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

Major **Carl GILLOT**

COMITÉ DE RÉDACTION

• Général de corps d'armée **Christian Rodriguez,**
major général de la Gendarmerie nationale
• Général de corps d'armée **Thilbaut MORTEROL,**
Commandant des écoles de la Gendarmerie nationale
• Général de division **Philippe GUIMBERT,**
Conseiller communication du directeur général
de la Gendarmerie nationale - chef du Sirpa-gendarmerie
• Colonel **Stéphane DESCORSIERS,**
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 **Thilbaut MORTEROL,**
Commandant des écoles de la Gendarmerie nationale
• Général de corps d'armée **François GIERÉ,**
Directeur des opérations et de l'emploi
• Général de division **Philippe GUIMBERT,**
Conseiller communication du directeur général
de la Gendarmerie nationale - chef du Sirpa-gendarmerie
• Lieutenant-colonel **Édouard EBEL,**
département gendarmerie au sein
du service historique de la Défense
• Colonel **Laurent VIDAL,**
délégué au patrimoine

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
Avril 2017
ISSN 1243-5619

Le CECyF

Le Centre expert contre la cybercriminalité français est une association permettant aux services chargés de l'application de la loi, aux chercheurs de toutes origines (académiques, industriels, indépendants) et aux établissements d'enseignement de se rencontrer et d'échanger pour créer des projets qui contribuent à la formation, à l'éducation, à la prévention (site CECyF Prévention) et à la recherche & développement contre la cybercriminalité. Le CECyF compte 34 membres dont les douze premiers étaient issus du projet européen 2CENTRE et de leurs 15 partenaires.
Il rassemble des services de l'État, des établissements d'enseignement supérieur et de recherche, des entreprises et des associations. La gendarmerie en assure la présidence et le secrétariat général.
Le CECyF est partenaire du Festival du film de sécurité d'Enghien. Partenaire de Cyberlex, association qui regroupe des spécialistes du droit du cyberespace et des technologies numériques, il organise avec elle une masterclass sur la procédure pénale à l'épreuve du numérique à l'occasion du FIC 2018. En synergie avec cet événement, il co-organise la 4e Conférence sur la réponse aux incidents et l'investigation numérique, CoRI&IN.