REGARDS STRATÉGIQUES > L'État en ordre de bataille

DROIT > Panorama juridique de la confidentialité

TECHNIQUE > La réalité virtuelle

REVUE de la gendarmerie nationale

REVUE TRIMESTRIELLE / DÉCEMBRE 2015 / N° 254 / PRIX 6 EUROS

PROTECTION DES DONNÉES ET VIE PRIVÉE

DATA SECURITY AND PRIVACY

AVEC LA COLLABORATION DU CENTRE DE RECHERCHE DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

retour sur images NUMÉRO 253

© Philippona

L'hybridation des théâtres d'opération, mêlant des postures militaires, civiles et humanitaires, a rapidement accrédité la mobilisation des compétences de forces de police à statut militaire pouvant accompagner les forces armées et soutenir des structures étatiques déficientes.
Ce modèle, capable de travailler au profit d'autorités diverses, dispose d'une grande cohérence doctrinale et d'une indéniable aptitude à planifier ses opérations dans un contexte multipartenarial.

RETROUVEZ UN APERÇU DES POTENTIALITÉS DE LA RÉALITÉ AUGMENTÉE APPLIQUÉE AUX PROCESSUS INDUSTRIELS ET À LA FORMATION EN>
PAGE 142 DE CE NUMÉRO

© middleVR

Les données forment un écosystème numérique global. L'Internet des objets et le Big data, qui les véhiculent, portent des inquiétudes sur la protection des données sensibles des particuliers et des opérateurs principaux tant industriels que commerciaux.

L'agence nationale de la sécurité des systèmes d'information (ANSII) dans une optique « Agir ensemble », les PME regroupées sous Hexatrust, la direction générale de l'armement convergent tous pour reconnaître la part industrielle de la stratégie nationale de sécurité. Elle embrasse les domaines militaires, commerciaux, manufacturiers et la recherche avec une forte connotation juridique. Elle requiert une nouvelle bataille de la formation, de l'acquisition du renseignement utile et l'avènement d'un corps d'analystes capable de structurer la valeur des données disponibles.

La France, dans un cadre européen, se dote des moyens d'une action volontariste et coordonnée tant en mode défensif qu'offensif. À ce titre, le Préfet, chargé de la lutte contre les cybermenaces, bénéficie d'un renforcement significatif du potentiel d'analyse et d'investigation des forces de sécurité qui concourt à la protection des libertés individuelles et des valeurs constituées par le savoir de nos entreprises.

SOMMAIRE

NUMÉRO 254

REGARDS STRATÉGIQUES

DOSSIER

TECHNIQUE

DROIT

DOSSIER

Protection des données et vie privée

fotolia.com

UN NOUVEAU CADRE STRATEGIQUE

En ordre de bataille, l'Etat accompagne la transition numérique et organise la sécurisation de nos intérêts majeurs. Cette stratégie globale s'applique sur le plan diplomatique mais également en mobilisant tous les acteurs publics, privés et les opérateurs de l'industrie du Net.

La donnée, valeur ajoutée et moteur de la croissance de l'industrie numérique, est la cible des cybercriminels. Les systèmes d'informations qui la portent doivent être protégés d'attaques transfrontières et anonymes. Inhérente à un régime inaliénable de libertés individuelles, la protection des données privées est un facteur confiance dans l'économie numérique. Elle conditionne une vision de notre société et une approche européenne spécifique.

L'adaptation des outils juridiques, une coopération internationale entre les services d'investigation, et l'éducation de la communauté des usagers du Net sont au cœur de la stratégie nationale pour la cybersécurité numérique.

L'État
en ordre de bataille

par **JEAN-YVES LATOURNERIE**

« La France est pleinement engagée dans la transition numérique. Forte d'une population très largement connectée et portée par une économie numérique en croissance soutenue, la France dispose de talents et d'atouts à la pointe de l'innovation européenne et mondiale. Le numérique est également un espace de compétition et de confrontation. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme et criminalité, trouvent dans le cyberespace un nouveau champ d'expression ».

C'est par ces mots que le Premier ministre introduit la Stratégie nationale pour la sécurité du numérique présentée le 16 octobre 2015, et en pose les enjeux, en termes de croissance et de compétitivité, mais aussi de défense et de sécurité, et donc de souveraineté.

JEAN-YVES LATOURNERIE

Préfet, conseiller du Gouvernement, Chargé de la lutte contre les cybermenaces

Un nouveau cadre stratégique

Muni de ce cadre stratégique récemment actualisé sous la coordination du Secrétaire général de la défense et de la sécurité nationale (ANSSI), l'État est en ordre de bataille. D'une part il se mobilise activement pour favoriser et accompagner la transition numérique. Le ministère de l'économie et le secrétariat d'État au numérique jouent un rôle moteur à cet égard. Dans le champ de la sécurité, leur action est déterminante pour soutenir le développement d'une filière française de cybersécurité, auquel participe la délégation ministérielle aux industries de sécurité du ministère de l'Intérieur.

L'État organise d'autre part la défense et la sécurité de nos institutions, des acteurs économiques et de nos concitoyens dans le cyberespace. Le ministère de l'Intérieur est pleinement engagé dans cet objectif, qui revêt, pour ce qui le concerne, trois dimensions : la cyberdéfense dans le cadre défini par le livre blanc de la défense et de la sécurité nationale, notamment la lutte contre

le terrorisme ; la sécurité des systèmes d'information, de l'État bien sûr, mais aussi des particuliers, entreprises et collectivités publiques, sur l'ensemble du territoire ; et la lutte contre la cybercriminalité, qui mobilise au côté des magistrats plusieurs centaines de policiers et de gendarmes spécialisés.

Naturellement, le ministère de l'Intérieur n'agit pas seul. Nommé Préfet chargé de la lutte contre les cybermenaces il y a un an, je suis depuis en contact régulier avec mes homologues : le directeur général de l'Agence nationale de la sécurité des systèmes d'information, mais aussi l'officier général de cyberdéfense à l'état-major des armées et l'ambassadeur chargé de la cyberdiplomatie au ministère des affaires étrangères et du développement international. La sécurité dans le cyberespace donne lieu, en effet, à une intense activité diplomatique ; et sur le plan policier et judiciaire, le succès, quand il advient, doit beaucoup à la qualité de la coopération internationale, développée et entretenue depuis très longtemps, bien avant l'apparition du mot cyber.

Enfin, il faut le souligner, la sécurité dans le cyberespace ne peut s'envisager sans la participation active du secteur privé, singulièrement de l'industrie du Net. À l'initiative du ministre de l'Intérieur, la France a pu mettre en place avec les principaux acteurs américains et français, une plate-forme de coopération, dont les premiers résultats sont probants, pour faciliter le travail des enquêteurs dans les affaires les plus graves, et obtenir le retrait rapide de contenus illicites en matière de propagande et d'apologie du terrorisme notamment.

Les données, cible principale des attaquants

C'est dans ce contexte que les organisateurs de ce 8e Forum international de la cybersécurité ont choisi à juste titre de mettre l'accent sur les données. Celles-ci constituent en effet l'essentiel de la valeur et le moteur de la croissance de l'industrie numérique. L'exploitation vertueuse de ce gisement en très fort développement, est en effet porteuse de progrès dans de nombreux domaines, y compris pour assurer la protection des personnes et des biens, voire celle des systèmes d'information eux-mêmes.

Cependant la valeur des données en fait aussi dès aujourd'hui la cible principale des attaquants. Ainsi, le rapport IOCTA 2015 récemment publié par Europol[1] fait état d'une augmentation significative des détournements de données, lors de cyberattaques de plus en plus agressives venant du crime organisé. On sait par ailleurs que le préjudice mondial annuel de la cybercriminalité est estimé à 500 milliards de dollars en 2015, et qu'il atteindrait en 2020 un montant cinq à sept fois supérieur.

(1) Internet Organized Crime Threat Assessment

Un combat inégal

Or en la matière, le combat est inégal. En effet, si les services opérationnels parviennent à mener à terme leurs enquêtes lorsque les cyberattaques visent des individus (pornographie enfantine, cyber-harcèlements, diffamations, injures, délits relevant de la loi de 1881 sur la liberté de la presse,…) ou lorsqu'elles se limitent au territoire français, les obstacles s'accumulent et sont la plupart du temps dirimants lorsqu'il s'agit d'attaques transfrontières et anonymes contre les systèmes de traitement automatisé de données.

L'existence notoire de « cyberparadis », l'inadaptation des outils juridiques classiques - les demandes d'entraide pénale internationale - trop longs à mettre en œuvre alors que la preuve numérique est éphémère, la dépendance des enquêteurs aux acteurs de l'Internet étrangers qui détiennent les données nécessaires à la poursuite des investigations, telles sont les difficultés que les services de police et de gendarmerie et l'institution judiciaire doivent généralement affronter.

Pour y faire face, il faut au besoin adapter le cadre législatif, comme la France a su le faire pour lutter contre le terrorisme et en combattre l'apologie sur Internet et les réseaux sociaux. Mais, comme on le sait, face à une délinquance de masse, il convient aussi de prévenir et d'éduquer, de trouver les parades techniques, culturelles et comportementales à ces agressions d'un nouveau genre. C'est pourquoi la communauté scientifique est invitée à amplifier ses efforts de recherche pour intégrer la sécurité dès la conception des outils numériques. La sensibilisation à la sécurité du numérique et aux comportements responsables dans le cyberespace, dès l'école et dans les formations initiales supérieures et continues, est aussi un objectif inscrit dans la stratégie nationale pour la sécurité du numérique.

Le FIC, un acronyme parfaitement adapté

Pour terminer, je suis tenté de rendre hommage aux concepteurs du FIC en leur empruntant cet acronyme parfaitement adapté à l'enjeu de la lutte contre les cybermenaces, pour livrer, avec une année de recul, quelques premières conclusions.

Le F de forum tout d'abord : il est essentiel que tous les acteurs, publics et privés, travaillent ensemble à une appréhension concertée de l'évolution de la menace cyber et des réponses à y apporter. La France figure parmi les pays qui ont ouvert la voie. La Commission européenne a elle-même repris le concept et lancé officiellement le 3 décembre 2015 l'EU IT Forum l'associant aux ministres de l'intérieur des 28 pays européens ainsi qu'aux grands acteurs du net.

Le I de international ensuite : les cyberattaquants ne connaissent pas les frontières ; le ministère de l'intérieur en est un témoin privilégié. Pratiquement aucune enquête n'aboutit sans coopération internationale. La plupart des grands acteurs du Net sont situés hors d'Europe. Le droit international du cyberespace, pour une large part, reste à construire. De fait, les conditions générales d'utilisation (*terms of reference*) des services offerts par les majors de l'Internet semblent en tenir lieu.

Le C de cybersécurité enfin ; l'action du ministère de l'intérieur dans la lutte contre les cybermenaces ne se résume pas à combattre la cybercriminalité ; ce n'est qu'une partie – certes importante - de son activité. Face à l'ampleur de la tâche, compte tenu de l'inégalité du combat, c'est bien une culture de la cybersécurité qu'il lui appartient de diffuser, de porter. Le maillage territorial du ministère de l'Intérieur, sa tradition de proximité avec tous les publics en font l'un des principaux acteurs de la cybersécurité.

À l'évidence, la Gendarmerie y tient un rôle éminent.

XtravaganT - fotolia.com

UNE CYBERDEFENSE INTEGRÉE AUX AUTRES FORMES DE COMBAT

Une cyberdéfense efficace est un outil de souveraineté numérique. Le combat numérique mobilise de fortes capacités humaines et techniques. Il nécessite un cadre juridique actualisé au regard de l'évolution des menaces et une analyse fine des données.

Son intégration aux autres formes de combat est primordiale en défendant nos systèmes et nos réseaux, en neutralisant la menace et en exploitant les vulnérabilités des ennemis. Au cœur des opérations militaires, le combat numérique combine ses actions avec celles des autres forces.

Si l'action française s'associe aux bonnes pratiques de nos alliés pour coordonner des ripostes défensives et offensives, elle s'est appuyée sur des réformes de fond. Outre l'apport des moyens confiés par la la Loi de programmation militaire, le plan stratégique « Pacte défense Cyber » assure une gouvernance cohérente des acteurs et des actions.

Cyberdéfense militaire : placer le combat numérique au cœur des opérations

par ARNAUD COUSTILLIÈRE

Les acteurs français et étrangers de la cyberdéfense militaire se sont réunis le 24 septembre à Paris lors du colloque « #cyberdéfense, le combat numérique au cœur des opérations ». Cet événement inédit a réuni près de sept cents personnes, trois ministres, les ministres de la Défense français britannique et belge, et une vingtaine de délégations étrangères. Bien plus qu'un lieu de débats et d'échanges, ce colloque a permis d'initier et de renforcer la coopération entre pays partageant les mêmes enjeux dans le domaine de la cyberdéfense militaire.

ARNAUD COUSTILLIÈRE

Officier général cyberdéfense
Etat-major des armées

Coopérer dans l'espace numérique pour mieux faire face à un ennemi commun

En effet, l'espace numérique, transverse et sans frontières matérielles, ne peut s'appréhender de manière autarcique. La session 2016 sera d'ailleurs organisée à Londres par le ministère de la Défense britannique, qui prend ainsi le relais de l'initiative française.

La coopération entre membres d'une même coalition est essentielle pour partager de l'information, échanger les bonnes pratiques, se coordonner face à des ennemis communs et tendre ensemble vers des relations pacifiées au sein de l'espace numérique. C'est également un outil au service de notre souveraineté numérique. Elle permet notamment d'anticiper la menace, d'améliorer nos capacités en bénéficiant d'échanges fructueux, que ce soit dans le cadre d'exercices conjoints, de formations ou encore d'opérations en

La guerre de l'information vise à fausser la perception de la réalité par l'adversaire ou les populations civiles.

coalition, mais aussi de mesurer nos forces et nos faiblesses.

Grâce à une montée en puissance en termes de moyens financiers, humains et techniques, la cyberdéfense militaire française a acquis des capacités lui permettant de proposer son savoir-faire et son expertise à des pays désireux de développer leurs capacités cyber militaires, notamment au travers du Pôle d'Excellence Cyberdéfense récemment constitué autour de nombreux partenaires de la société civile (industriels et universités par exemple).

Conforté par les moyens confiés par la Loi de programmation militaire et sa réactualisation, le ministère de la Défense a opéré une réelle montée en puissance depuis 2010. En cinq ans, un commandement opérationnel de cyberdéfense s'est mis en place au sein de l'état-major des armées, étoffant progressivement ses missions, ses ressources humaines et ses capacités. Un budget de 350 millions d'euros d'équipements, un budget Recherche et Développement multiplié par trois et un recrutement de plus de mille personnes supplémentaires, sont désormais consacrés à la cyberdéfense, enjeu de souveraineté nationale reconnu par le Livre blanc sur la défense et la sécurité nationale de 2013.

Un plan stratégique baptisé « Pacte défense Cyber » met l'ensemble des actions et leur gouvernance en cohérence, mobilisant ainsi tous les acteurs du Ministère vers un objectif commun. Du développement de capacités de lutte informatique défensive et offensive, en passant par le renseignement d'intérêt de cyberdéfense, le ministère de la Défense entend développer sa compréhension et sa maîtrise de l'espace numérique sur son périmètre de responsabilité c'est-à-dire les opérations militaires. Cette maîtrise de l'espace numérique s'étend de la couche technique à la couche informationnelle.

L'intégration de la dimension cyber aux autres formes de combat est primordiale à travers la prise en compte de la menace, en adaptant notre posture défensive ou en orchestrant des opérations cyber en appui des opérations cinétiques. L'arme informatique est un outil qui doit apporter un appui maîtrisé aux forces conventionnelles. Elle doit être

appréhendée comme une nouvelle forme de frappe dans la profondeur mais aussi une forme d'appui tactique aux forces sur le terrain.

La diversité des menaces dans l'espace numérique : de l'attaque informatique à la désinformation

Les forces armées agissent face à des menaces de plus en plus protéiformes et complexes : attaques ciblées de type advanced persistent threats (APT), attaques de faible ampleur visant à perturber, désinformation… Les acteurs sont tout aussi divers : Etats, mafias agissant seules ou au profit du plus offrant, hacktivistes opérant de façon isolée ou en groupe, groupes armés terroristes…

La menace cyber, pour le ministère de la Défense, ne se résume plus seulement à des attaques informatiques pouvant perturber ou détruire des systèmes d'information ; elle prend également place dans le domaine informationnel. Lorsque nos ennemis, contre lesquels nos forces armées sont engagées sur les théâtres, diffusent de fausses informations sur Internet et les réseaux sociaux, menacent les militaires et leurs familles, revendiquent des manœuvres tactiques sur le terrain, le concept de guerre de l'information prend tout son sens.

Les conflits en cours l'illustrent parfaitement. Les groupes armés terroristes, au Levant mais aussi en Afrique ou au Maghreb, ont investi de manière massive l'espace numérique. Cette barbarie numérique vise des objectifs précis : démoraliser et terroriser son ennemi pour l'empêcher de combattre ; apparaître plus fort qu'on ne l'est en réalité ; recruter à l'aide de campagnes de propagande mensongères mais sophistiquées ; désorganiser en propageant de fausses rumeurs, amplifiées là aussi par les réseaux sociaux, comme dans l'exemple de l'attaque contre la chaîne de télévision TV5 Monde, le 8 avril 2015.

Si ces menaces relevant du champ des perceptions prennent une part grandissante dans les conflits, elles ne les transforment pas pour autant. L'espace numérique est certes un domaine d'action militaire se caractérisant par des attributs spécifiques : les menaces, le tempo opérationnel, les acteurs et les frontières revêtent des caractéristiques qui lui sont propres. Cependant, les acteurs agissant dans cet espace ont adopté des modes d'action conventionnels tels que la maîtrise de leur environnement, les actions de déception, de neutralisation et de ruse, le recours à des mercenaires...

Cet espace s'adosse et se superpose aux autres espaces de confrontation que constituent les espaces terrestre, aérien, maritime et extra-atmosphérique. La construction d'un nouvel espace d'affrontement ne révolutionne pas pour autant « la manière de faire la guerre ». Il la refaçonne pour l'adapter aux réalités de

le théâtre d'opération de la cyber est connexe des autres dimensions terre – air – mer.

notre monde contemporain. C'est un espace pleinement reconnu comme un milieu à part entière au sein duquel les forces armées évoluent, veillent, défendent et neutralisent, encadrées par un cadre juridique clair et protecteur.

Le ministère de la Défense a pris en compte cette nouvelle dimension, en particulier cette dimension cognitive, et ses potentiels impacts dans le cadre des opérations militaires.

La formation comme pilier essentiel d'une cyberdéfense robuste

Il est impératif de disposer d'un personnel compétent et formé pour une confrontation positive à un domaine militaire à la fois unique et transverse, complexe et reprenant les modes d'action cinétique,. Ainsi, l'un des axes particuliers d'effort du ministère de la Défense porte sur le développement d'une filière cyber au sein du ministère et sur l'entraînement permanent des forces à travers des formations et des exercices réguliers.

Les exercices DEFNET organisés chaque année permettent notamment de tester nos capacités de cyberdéfense, nos forces et notre organisation de gestion de crise cyber.

Le combat numérique, à travers ses différentes facettes (capacités humaines et techniques, formation, cadre juridique, renseignement…) constitue un véritable enjeu pour le ministère de la Défense. Comme le rappelait le ministre de la Défense, lors du colloque du 24 septembre dernier, nous devons, en premier lieu, garantir la protection des réseaux et systèmes de notre défense. Cette protection suppose des produits et

des services de confiance, mais aussi une conception rigoureuse des systèmes concernés. Le rôle des programmes et des projets de science et technologie conduits par la DGA avec les industriels est donc crucial.

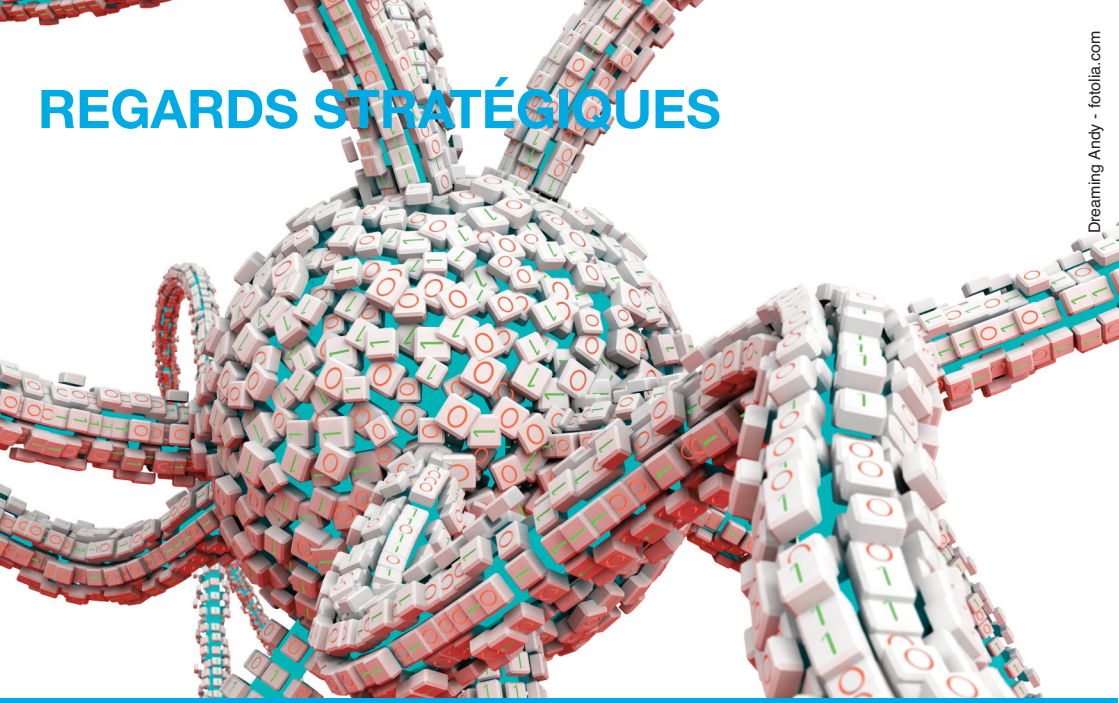
Nous devons ensuite faire monter en puissance notre chaîne opérationnelle de cyberdéfense, qui agit en temps réel pour la sécurité de nos systèmes. Ce volet est aujourd'hui intégré à tout déploiement de forces, par exemple au Levant ou au Sahel. Des dispositifs particuliers sont mis en œuvre au cœur des forces, afin de fabriquer un bouclier protecteur. Une unité a été spécialement créée et équipée dans cet objectif ; elle sera pleinement opérationnelle en 2018, son noyau est déjà en place et nos forces au Levant en bénéficient.

Troisième priorité pour le ministère de la Défense, des efforts restent encore à réaliser dans le renseignement cyber, afin d'anticiper les menaces, de caractériser l'adversaire et d'adapter ainsi nos systèmes de défense. C'est à cette fin que la Direction du renseignement militaire (DRM) est en train de créer un centre de recherche et d'analyse cyber, et que la Direction générale de la sécurité extérieure (DGSE) développe ses propres moyens depuis plusieurs années.

Nous devons, enfin, continuer à nous doter de moyens pour agir. Priver l'adversaire de ses systèmes numériques, en les neutralisant ou en les leurrant, peut conférer un avantage déterminant dans une manœuvre militaire. La guerre de demain doit combiner le cyber dans toutes ses dimensions avec les autres formes de combat. Il s'agira de s'intégrer aux opérations militaires en défendant ses systèmes et ses réseaux, en anticipant et en neutralisant la menace, en exploitant les vulnérabilités des ennemis de façon combinée avec les actions dans les autres milieux. Le combat numérique s'inscrit désormais pleinement au cœur des opérations militaires.

L'AUTEUR

La carrière du vice-amiral Arnaud COUSTILLIERE s'est essentiellement partagée entre des embarquements et commandements opérationnels sur des navires de combat, et des postes de responsabilités en administration centrale, avec une spécialisation plus particulière pour les télécommunications et la cyberdéfense.
Il a été nommé officier général à la cyberdéfense le 1er juillet 2011 à la création du poste. Directement rattaché au sous-chef « opérations » de l'état-major des armées, placé sous la double tutelle du chef d'état-major des armées et du chef de cabinet militaire du ministre, il est responsable de la cyberdéfense du ministère et de sa conduite en situation de crise cybernétique. En février 2011, en cohérence avec l'extension des missions de l'ANSSI1, il avait été nommé chargé de mission « cyberdéfense » auprès du sous-chef « opérations » tout en conservant de façon temporaire ses fonctions précédentes.



Dreaming Andy - fotolia.com

UNE RESPONSABILITE PARTAGEE ET UN INTERET COMMUN

Une division du travail numérique doit permettre, dans une solidarité fonctionnelle sans faille, de sécuriser les produits dès leur conception, d'assoir une hygiène des pratiques - personnelles et professionnelles - et de protéger les données des particuliers et des entreprises.

La nouvelle stratégie nationale de sécurité déclinera par ministère, selon cinq axes stratégiques, la protection des infrastructures critiques et une assistance aux victimes d'actes de malveillance. Elle promouvra des mesures de formation et de sensibilisation des acteurs et favorisera la transformation de standards de sécurité en atouts commerciaux majeurs tout en recherchant une mobilisation des instances européennes compétentes.

Dans ce cadre, le Préfet, chargé de la lutte contre les cybermenaces, continuera à coordonner l'action des forces de sécurité pour renforcer la défense et la sécurité numérique de la Nation.

« Responsable de tous »

par GUILLAUME POUPARD

Le Premier ministre a présenté le 16 octobre dernier la « stratégie nationale pour la sécurité du numérique », en présence notamment de la secrétaire d'État chargée du numérique, du secrétaire général de la défense et de la sécurité nationale, du Président du Conseil national du numérique et des coordonnateurs ministériels des questions liées au cyberespace des ministères des Affaires étrangères et du Développement international, de l'Économie, de l'Industrie et du Numérique, de la Défense et de l'Intérieur.

GUILLAUME POUPARD
Directeur général de l'Agence nationale de sécurité des systèmes d'information

Cette participation des plus hautes instances de l'État montre que, transition numérique aidant, les questions liées à la cybersécurité issues de la seule sphère technique sont devenues de réels enjeux de société dans lesquels le politique s'implique.

Une stratégie déclinée au niveau ministériel

Issue d'un travail interministériel engagé un an plus tôt, la stratégie nationale pour la sécurité du numérique présente cinq objectifs stratégiques et propose des orientations pour chacun d'entre eux. Il appartient aux ministères, soutenus par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de contribuer à l'atteinte de ces objectifs par des actions relevant de leurs champs de compétences.

Le premier axe de la stratégie est dans la continuité des orientations données par les Livres blancs sur la défense et la sécurité nationale de 2008 et 2013. Il vise à renforcer la protection des infrastructures critiques de la France par

Une stratégie nationale pour la sécurité numérique repose sur une responsabilité partagée.

une croissance de la sécurité de leurs systèmes d'information. C'est le sens du travail engagé entre l'ANSSI et les opérateurs d'importance vitale pour la mise en œuvre des dispositions législatives relatives à la sécurité des systèmes d'information, contenues dans la loi de programmation militaire.

Le deuxième axe concerne plus particulièrement la protection de la vie numérique des Français. Complémentaire du premier axe, il s'agit d'une part de promouvoir et défendre dans le cyberespace les valeurs de la République et d'autre part d'apporter une aide aux entreprises et particuliers victimes d'actes de cybermalveillance. Sur ce dernier point, un groupe de travail co-piloté par le préfet chargé de la lutte contre les cybermenaces du ministère de l'Intérieur et l'ANSSI a permis de poser les bases de ce que sera le dispositif d'aide qui sera mis en place courant 2016. La gendarmerie nationale aura un rôle de premier plan dans ce dispositif.

Le troisième axe aborde les enjeux des formations initiales et continues. La stratégie évoque l'opération « Permis internet » initiée par la gendarmerie nationale pour souligner que l'ensemble des Français doit être sensibilisé et que toute formation initiale supérieure doit intégrer un volet sensibilisation ou formation à la cybersécurité adapté à la filière.

Le quatrième axe vise à favoriser le développement d'un écosystème favorable au développement de produits et services de sécurité performants et de

confiance. Il s'agit également de transformer la contrainte budgétaire et humaine, liée à l'intégration de la sécurité informatique dans les produits et services, en avantage concurrentiel pour l'entreprise et en valeur ajoutée pour le client. Le cinquième axe, enfin, vise à mobiliser les États membres de l'Union européenne pour atteindre une véritable souveraineté numérique propice au développement d'acteurs européens de la cybersécurité. L'objectif est également de renforcer l'influence française dans les instances internationales.

Une solidarité impérative pour une sécurité collective

Au-delà des orientations mises en avant, trois idées irriguent la stratégie nationale pour la sécurité du numérique.

La première idée est commune dans son expression mais prend une dimension particulière dans le cyberespace : chacun d'entre nous a une part de responsabilité effective dans la sécurité et la défense nationale. Il ne s'agit pas simplement d'une sorte d'incarnation numérique de « l'esprit de défense » que chacun devrait posséder dans le monde matériel et qu'il faudrait développer dans les réseaux. Comme le montrent les traitements de nombreuses attaques informatiques, les caractéristiques propres au cyberespace font que le comportement d'un seul peut compromettre la sécurité de beaucoup, de tous.

Trois communautés sont identifiables.

On distingue d'abord celle qui regroupe les innovateurs, les créateurs des nouveaux usages, services et produits du numérique, les chercheurs, les opérateurs de réseaux de communications électroniques, les entreprises du domaine de la cybersécurité, les équipementiers et les intégrateurs. Cette communauté a le devoir de proposer des produits et services dont le niveau de sécurité correspond aux besoins exprimés par la nécessaire analyse de risque qui doit accompagner tout projet numérique.

La deuxième communauté est constituée de tous ceux qui prennent les décisions concernant la « *gestion de la cité* » : élus, gouvernement, administrations centrales et territoriales et syndicats. La mission de cette communauté est d'intégrer la sécurité et la défense du numérique dans leur vision politique des entités dont ils ont la charge. Il appartient, par exemple, à l'élu d'une collectivité territoriale de demander à ses services que le site internet de sa collectivité bénéficie du niveau de sécurité nécessaire comme il lui appartient de faire voter les budgets requis.

La troisième communauté, la plus large, est constituée de tous les utilisateurs du numérique, de chefs d'entreprise ou de responsables d'associations, de tous les citoyens. Il leur revient d'utiliser les ressources du numérique avec la

prudence nécessaire afin de ne pas se mettre en danger, mettre en danger leurs proches ou leurs entreprises, leurs clients ou leurs fournisseurs.

Dans les faits, chacun appartient au moins à deux communautés. Dans le cyberespace, comme l'a écrit Antoine de Saint-Exupéry : « *Chacun est responsable de tous. Chacun est seul responsable.* Parce qu'elle appartient elle-même à la première communauté, parce qu'elle est en contact avec des représentants de ces trois communautés — élus, chefs d'entreprises, responsables d'associations, la Gendarmerie nationale a un rôle important de sensibilisation et d'animation au sein de ces communautés.

La deuxième idée contenue dans la stratégie nationale pour la sécurité du numérique est encore naissante même si, intuitivement, chacun peut en comprendre les fondements. Elle a trait à la captation des données personnelles des Français. On peut l'illustrer par deux exemples. D'une part une captation massive de ces données personnelles à des fins d'exploitation économiques par des acteurs étrangers peut entraîner un déséquilibre défavorable susceptible de mettre en danger une part de l'économie nationale voire européenne. D'autre part,et dans certains cas, une captation ciblée de données personnelles — par exemple celle disponibles sur les réseaux sociaux concernant directement ou indirectement tous les personnels du ministère de l'Intérieur — et leur exploitation peut constituer un problème de sécurité nationale.

Si quelques cas d'exploitation de données personnelles obtenues par attaque informatique ont mis en danger les personnes concernées ou les entreprises victimes, il n'y a pas, à ce jour, de démonstration corroborant cette menace même si on en comprend aisément les mécanismes.

La troisième idée est issue d'une anticipation fondée sur l'observation des faits: depuis plusieurs années, les attaques informatiques sont en croissance forte en nombre et en sophistication. Plus la France avance dans sa transition numérique… plus elle augmente sa « *surface d'attaque* » et plus le risque d'être victime d'attaque informatique est important ! Ce raisonnement est applicable dans tous les pays. Pourtant, pour l'entreprise, pour l'administration et pour chacun d'entre nous, la sécurité est présentée et vécue comme une contrainte et un coût.

Des standards de sécurité pour une plus-value concurrentielle

La stratégie nationale pour la sécurité du numérique propose en quelque sorte d'inverser la charge de la preuve. La sécurité informatique doit devenir un avantage concurrentiel pour les produits

et services proposés par les entreprises françaises. Dans un marché mondial concurrentiel et face à des menaces révélées quotidiennement, notamment contre la confidentialité des données ou la résilience de produits connectés, les utilisateurs se tourneront demain vers les produits et services qu'ils estimeront de confiance. Ainsi, pensée et intégrée en amont de la conception, la sécurité numérique des produits et services proposés par les entreprises françaises seront, à performance égale, en position favorable sur les marchés internationaux.

La gendarmerie nationale joue d'ores et déjà un rôle majeur dans la stratégie nationale pour la sécurité du numérique. Outre la mise en place du dispositif d'assistance aux victimes d'actes de cybermalveillance évoqué plus haut, les actions engagées au travers de la sensibilisation des écoliers via le passeport internet, du Forum international sur la cybersécurité, la formation des N'Tech, la sensibilisation des entreprises et des collectivités territoriales comme le développement des compétences nécessaires au déploiement de la mobilité sécurisée procèdent déjà de cette stratégie. Je me réjouis du dynamisme montré par la Gendarmerie nationale et de la bonne coopération qu'elle a su installer avec l'ANSSI.

L'AUTEUR

Guillaume Poupard est ancien élève de l'Ecole Polytechnique, promotion X92. Ingénieur de l'armement en option recherche, il est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques Stern à l'Ecole Normale Supérieure de Paris et soutenue en 2000. Il est également diplômé de l'enseignement supérieur en psychologie.
Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). Cette direction sera transformée en 2009 pour devenir l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).
Il rejoint en 2006 le Ministère de la défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense. En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction Générale de l'Armement (DGA), responsable de l'expertise et de la politique technique dans le domaine de la cybersécurité.
Le 27 mars 2014, il est nommé directeur général de l'Agence nationale de sécurité des systèmes d'information.

Il reste beaucoup à faire. La stratégie nationale pour la sécurité du numérique va être déclinée par ministère. En ce sens, le travail effectué par le préfet Jean-Yves Latournerie, préfet chargé de la lutte contre les cybermenaces, permettra la coordination optimale des parties prenantes du ministère de l'Intérieur dont le rôle est essentiel pour la défense et la sécurité de la vie numérique de la Nation.

rolfimages - fotolia.com

LA CNIL : UNE EXPERTISE ET UN ACCOMPAGNEMENT PRECIEUX

La CNIL, dans un cadre juridique renforcé, veille à la protection des données personnelles considérée comme un droit fondamental par l'article 8 de la charte des droits fondamentaux de l'Union européenne.

Sa forte expertise juridique et technologique l'autorise à participer pleinement à la régulation de l'écosystème de la donnée personnelle qui est un enjeu stratégique. Outre une classique compétence transversale de contrôle, elle met en œuvre un accompagnement des responsables des traitements. Elle dispose d'un pouvoir de coercition et d'une capacité d'émettre des recommandations qui généralement suffisent à remédier aux insuffisances décelées. Ses programmes de formation intéressent le grand public et les professionnels.

La protection des données
personnelles au cœur de la cybersécurité

par **EDOUARD GEFFRAY**

Alors que les données personnelles sont désormais au cœur de l'économie numérique, la CNIL accompagne les entreprises pour assurer une protection optimale de ces données, dès la conception du produit (« privacy by design ») comme ultérieurement. Ses contrôles comportent également celui des systèmes d'information, favorisant ainsi la mise en conformité des acteurs. La cybersécurité est en effet un enjeu majeur de libertés individuelles, de compétitivité, et de confiance.

Le constat de l'accroissement sensible des cybermenaces serait incomplet s'il n'était mentionné le fait qu'elles ciblent également de plus en plus des données personnelles. Certaines d'entre elles sont classiquement visées (par exemple les données bancaires), mais d'autres sont désormais ciblées par les cybercriminels, soit à des fins de nuisance gratuite, soit à des fins de chantage. La multiplication d'affaires médiatisées, comme la divulgation de comptes d'utilisateurs d'un site de rencontre, révèle les failles informatiques des sociétés tout en cristallisant une prise de conscience collective sur le sujet. Dans ce contexte, la Commission nationale de l'informatique et des libertés, en tant que régulateur de la protection des données personnelles, accompagne les acteurs et s'assure, dans le cadre de ses contrôles, de la conformité des traitements aux règles de sécurité applicables.

EDOUARD GEFFRAY
Secrétaire général de la CNIL

La cybersécurité, élément de protection des libertés individuelles

Les données personnelles sont au cœur de l'économie numérique. Alors que la question de leur valeur marchande n'était pas prioritaire jusqu'au début des années 2000, elles constituent

désormais un actif financier pour les entreprises, permettant de mieux cerner les goûts de leurs clients, de leur proposer de la publicité ciblée ou d'imaginer de nouveaux services. Se sont ainsi créés des « *capitaux informationnels* » dont la valeur économique est désormais élevée.

Mais, comme tout trésor, ces « *capitaux* » peuvent susciter les appétits de cybercriminels, à des fins de chantage, ou d'acteurs publics ou privés structurés à des fins d'intelligence économique. Sur le premier point, des recherches récentes ont notamment montré l'importance des attaques contre les données de santé, qui font l'objet d'un marché noir intense (cf. les travaux du *Ponemon Institute think tank on data protection policy*). Quant à l'intelligence économique, la donnée personnelle constitue là aussi son dénominateur.

Les enjeux soulevés sont nombreux. Le premier d'entre eux porte sur la protection des libertés individuelles. La protection des données personnelles constitue un droit fondamental, garanti par l'article 8 de la charte des droits fondamentaux de l'Union européenne comme un droit à la liberté. Elle est, à bien des égards, ce que l'on pourrait appeler un « *droit d'infrastructure* », c'est-à-dire qu'il rend possible l'exercice d'autres droits (par exemple, la liberté d'opinion et d'expression ou le droit de vote, dans le cas du vote électronique). Protéger les données personnelles dans l'univers numérique, c'est donc protéger un droit fondamental et, au-delà, l'exercice des libertés individuelles dans cet univers.

L'atteinte potentielle aux libertés dépasse cependant la dimension individuelle. À travers des atteintes massives aux données personnelles, c'est bien la défense nationale qui, dans certains cas, peut être mise en cause. C'est d'ailleurs le sens de la Stratégie nationale pour la défense numérique proposée par l'ANSSI.

Enfin, toute atteinte massive aux données à caractère personnel constitue un préjudice économique et d'image potentiellement important pour les entreprises. L'impact des révélations d'Edward Snowden sur les entreprises américaines du cloud, parfois évalué à plusieurs dizaines de milliards de dollars, en est un exemple. Plus généralement, la combinaison de la masse, de la précision et de la combinaison des données traitées implique une très grande confiance du citoyen-consommateur dans les acteurs auxquels il confie ses données personnelles. Sans confiance, la numérisation de l'économie sera bridée. La cybersécurité constitue donc aujourd'hui un des éléments de la confiance collective dans l'économie numérisée.

La CNIL, acteur de la cybersécurité

Dans ce contexte, la CNIL est désormais un acteur de la cybersécurité. Elle l'est

d'abord en vertu du droit européen et national. Tant le futur règlement européen sur la protection des données personnelles, qui devrait être adopté en fin d'année, que le droit national, imposent en effet aux « responsables de traitements » de données à caractère personnel d'assurer la confidentialité et l'intégrité des données conservées. La CNIL est compétente pour contrôler le respect de cette obligation, inscrite à l'article 34 de la loi du 6 janvier 1978, et en sanctionner le non-respect.

Ce cadre législatif a été progressivement renforcé. Depuis 2011, les opérateurs de communications électroniques ont l'obligation, sous peine de sanctions, de notifier à la CNIL toute violation de données à caractère personnel, afin notamment de s'assurer que celles-ci étaient conservées dans des conditions de chiffrement suffisantes pour éviter leur compromission ou, à défaut, d'assurer l'information du public. Cette obligation devrait être étendue avec le projet de règlement européen à l'ensemble des traitements de données.

Enfin, depuis mars 2014, la CNIL a également la possibilité de procéder à des contrôles en ligne, ce qui lui permet notamment d'intervenir rapidement et le cas échéant de prononcer des sanctions en cas de failles de sécurité sur internet. Concrètement, lorsqu'elle constate une faille, la CNIL peut, dans des délais brefs, mettre en demeure l'organisme d'y mettre un terme et s'assurer de la nature, de la qualité et du caractère suffisant des mesures techniques mises en œuvre. À défaut, elle peut prononcer une sanction pécuniaire, le cas échéant publique.

Un indicateur de confiance dans des produits ou procédures

La sécurité informatique fait donc partie de l' « ADN normatif » de la CNIL. Elle est également au cœur de son action opérationnelle.

La CNIL s'est tout d'abord dotée d'une expertise informatique et technologique forte, qui permet, pour chaque demande d'autorisation d'un traitement de données, une double instruction juridique et technologique. Les aspects de sécurité des données sont ainsi systématiquement examinés dans les délibérations adoptées par la CNIL et publiées sur Légifrance, conduisant à la diffusion de bonnes pratiques en amont de la création des traitements.

De même, les 450 contrôles menés chaque année par la CNIL comportent cette double dimension. Dans plus de 75 % des cas, les contrôles opérés par la CNIL donnent lieu à des observations sur la sécurité des données, tandis que la plupart des mises en demeure ou

sanctions de la CNIL se fondent également sur des manquements aux dispositions précédemment mentionnées. En pratique, les demandes de la CNIL en matière de sécurité portent sur la sécurité logique et physique des systèmes d'information, le recours à des protocoles sécurisés de type https, la mise en place de mesures de chiffrement, etc. Dans l'immense majorité des cas, les responsables de traitement se mettent en conformité : 89% des contrôles et 91% des mises en demeure aboutissent ainsi à une mise en conformité dans les délais requis ce qui explique que les sanctions soient en nombre plus réduit.

La CNIL, parce qu'elle a une compétence transversale sur l'ensemble des traitements et leurs responsables, est également en mesure d'accompagner ceux-ci, en amont, selon une logique dite de « *privacy by design* », c'est-à-dire de la protection de la vie privée dès la conception du produit. La protection des données personnelles constitue, à l'ère numérique, un enjeu majeur de compétitivité ; Dans un marché fortement concurrentiel, la protection des données personnelles devient un élément de différenciation des entreprises. La CNIL a ainsi, en vertu de l'article 11 de la loi « informatique et libertés », un pouvoir de labellisation des produits et des procédures. Elle a, à titre d'exemple, créé un label en matière de coffre-fort électronique. De même, la CNIL a diffusé des guides en matière de sécurité, promouvant à la fois une méthode (issue de la méthode EBIOS) et des mesures techniques que tout responsable de traitement peut suivre et mettre en place pour assurer une protection optimale de ses données.

Enfin, la cybersécurité est, fondamentalement, une question non seulement technique, mais aussi de responsabilité et d'éducation collective. La CNIL mène donc, en la matière, une action dans trois directions. D'une part, elle mène une action de mise à niveau à destination des professionnels sur l'ensemble de la loi « *informatique et libertés* », y compris dans son volet « *sécurité des données* ». Tout organisme public ou privé peut en effet se doter d'un « *correspondant informatique et libertés* » (CIL), qui assure, en interne, la conformité de son organisme à la loi. Ce CIL est un correspondant privilégié pour la CNIL, auprès de laquelle il bénéficie d'une permanence juridique téléphonique, à laquelle il peut adresser des demandes de conseils, et qui organise des ateliers permettant de partager les bonnes pratiques au sein de cette communauté. En trois ans, le nombre d'organismes dotés d'un CIL a doublé, pour atteindre plus de 16000 organismes fin 2016.

D'autre part, la CNIL est chargée par le législateur d'une mission d'information du grand public sur la protection des données personnelles. Elle a, à ce titre,

lancé un collectif pour l'éducation au numérique, qui regroupe une trentaine d'organismes et permet ainsi un passage à l'échelle en la matière. Les actions du collectif ont été démultipliées par des conventions avec, notamment, les ministères de l'éducation nationale et de la jeunesse et des sports (diffusion dans la plupart des collèges et lycées de l'affiche de la CNIL : « *10 conseils pour rester nets sur le web* »). De la même façon, la CNIL a lancé un outil de questions/réponses en ligne en juillet 2015, qui fait l'objet de près de 1000 interrogations par jour en moyenne.

Enfin, parce qu'elle est un enjeu stratégique et collectif majeur, la cybersécurité doit impliquer l'ensemble des acteurs concernés. C'est dans cette perspective de partage de pratiques et d'expertises que la CNIL et l'ANSSI développent des coopérations techniques croissantes.

Protection des données personnelles et cybersécurité sont donc, à l'ère numérique, indissociables. La CNIL, en tant qu'autorité chargée de cette protection et de la régulation de cet écosystème de la donnée personnelle, constitue un acteur clé de la cybersécurité. Compte tenu du champ de la loi informatique et libertés, applicable, dans ses obligations, à toute entité qui traite des données personnelles, comme en termes de droits, à toute personne physique, la CNIL est en mesure d'assurer le « passage à l'échelle » de la diffusion des bonnes pratiques. Elle constitue, en complémentarité avec l'action d'autres acteurs comme l'ANSSI, un puissant levier pour le déploiement de l'hygiène informatique de base et la mise à niveau collective en matière de cybersécurité. Dans un univers où la sécurité des données est un enjeu stratégique, une culture numérique partagée aussi bien par les entreprises que par les particuliers constitue un actif stratégique pour notre pays.

L'AUTEUR

Secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL), Edouard Geffray, maître des requêtes au Conseil d'Etat, était auparavant directeur des Affaires juridiques, internationales et de l'expertise de la CNIL. Précédemment, il a été successivement, rapporteur à la 10e sous-section du Contentieux du Conseil d'Etat de 2005 à 2008, responsable du centre de documentation et de recherches juridiques – service chargé d'effectuer les recherches juridiques pour les membres du Conseil d'État – en 2008 et rapporteur public à la 3e sous-section de 2008 à 2012. Ancien élève de l'ENA, Edouard Geffray est diplômé de l'Institut d'études politiques de Paris et titulaire d'une maîtrise d'histoire.

ANTEROVIUM - fotolia.com

LA CYBERSECURITE : UN ENJEU DE COOPERATION INTERNATIONALE

La collecte massive des données et sa valorisation par les Etats, des acteurs privés ou sociaux d'envergure mondiale sont un objet de gouvernance.

Sur la scène internationale, la préservation des intérêts de la France repose sur un tryptique fondamental. Outre un attachement atavique au respect des libertés individuelles soutenu par une législation européenne, la France milite pour une transparence des états garante d'une information accessible et une stratégie globale de cybersécurité embrassant les domaines militaires, économiques et sociaux. Face à des acteurs de dimension mondiale, porteurs de vulnérabilités pour nos sociétés, l'émergence d'un pôle européen autonome au sein d'un cyberespace mieux régulé est impératif.

Cyberdiplomatie : les données au cœur des négociations internationales

par DAVID MARTINON

Les enjeux diplomatiques de la « *mise en données du monde* » ont conduit le ministère des Affaires étrangères et du Développement international à adapter ses structures pour répondre à ce défi majeur du XXIe siècle. Dans le cadre de cette « cyberdiplomatie », la France cherche à promouvoir un équilibre entre liberté, sécurité et compétitivité, tout en plaidant pour l'autonomisation d'un pôle numérique européen.

Le traitement, souvent croisé, des données que les citoyens, les entreprises et les États produisent au quotidien répond à des exigences en matière de liberté, de compétitivité et de sécurité. « *Or noir* » du XXIe siècle, les données sont en effet désormais pleinement constitutives de notre identité, de notre richesse et de notre sécurité. Ces enjeux renvoient aux grands thèmes qui structurent traditionnellement notre diplomatie, dont le rôle est d'assurer à l'international la préservation des intérêts politiques, sécuritaires et économiques de notre pays, tout en faisant rayonner ses valeurs, et notamment notre attachement aux droits de l'Homme. À l'ère du numérique, la diplomatie doit aujourd'hui adapter ses outils pour être en mesure d'assumer ce rôle au XXIe siècle. C'est pourquoi le ministère des Affaires étrangères et du développement international a récemment décidé de créer le poste d'Ambassadeur en charge de la cyberdiplomatie et de l'économie numérique, fonction que j'ai l'honneur d'assumer depuis octobre 2015.

DAVID MARTINON

Ministère des affaires étrangères
Ambassadeur en charge de la cyberdiplomatie et de l'économie numérique

Liberté, compétitivité, sécurité. Dans le cyberespace, il serait illusoire de penser séparément ces trois concepts. Ma mission est justement de faire en sorte

Une gouvernance internationale d'internet repose sur un délicat équilibre entre la souveraineté numérique, la transparence, les libertés individuelles et les flux économiques.

que ce triangle ne soit pas un « *triangle d'incompatibilité* » à la manière de celui de R. Mundell, célèbre casse-tête de la théorie économique des années 1960[1]. Dans les négociations internationales sur les données, dont cet article entend présenter les grands enjeux (protection des données personnelles, libre circulation des données, ouverture des données, cybersécurité), plus que dans toute autre négociation, ces concepts sont inextricablement liés, ce qui rend la tâche de notre diplomatie d'autant plus complexe et passionnante.

(1) Le triangle montrait l'impossibilité pour un Etat de satisfaire simultanément les trois objectifs de fixité des taux de change, de mobilité parfaite des capitaux et de souveraineté monétaire.

Les données personnelles : la défense d'une vision européenne

La France compte parmi les pionniers en matière de protection des données personnelles, avec la création de la CNIL (Commission nationale informatique et libertés) dès 1978. À l'ère du tout numérique, elle continue aujourd'hui de porter sa conception de la vie privée à l'échelle internationale et européenne. Notre objectif est de réguler le développement de collectes toujours plus massives de données, qui assemblées, exploitées ou revendues à des tiers, peuvent nourrir des processus particulièrement intrusifs.

En 2013, les révélations d'Edward Snowden sur les activités de surveillance de la NSA ont initié une séquence diplomatique visant à faire reconnaître le droit à la vie privée à l'ère numérique comme un droit fondamental pour les citoyens du monde entier. À l'Assemblée générale des Nations Unies, des travaux soutenus par la France ont conduit à

l'adoption d'une résolution sur la vie privée à l'ère numérique, érigeant le droit à la vie privée au rang de droit fondamental et rappelant aux États leurs devoirs en la matière. La France a pris en compte les orientations de l'ONU dans la nouvelle loi sur le renseignement du 24 juillet 2015, qui renforce les garanties en matière de respect des libertés fondamentales pour les citoyens.

Au niveau européen, un travail de refonte des textes de 1995 sur la protection des données personnelles touche aujourd'hui à sa fin. La France et l'Europe promeuvent une conception exigeante du respect de la vie privée, en comparaison d'une vision plus ouverte au marché développée par certains de nos partenaires commerciaux. Les récentes décisions de la Cour de justice de l'UE (Google vs. Spain en 2014, Schrems en 2015) dessinent les contours de cette conception. La protection des données ne doit pas pour autant constituer un frein à l'économie, mais bien constituer un argument de compétitivité et d'attractivité pour l'Europe. Un juste équilibre entre protection et laissez-faire doit être défini. C'est le sens de l'engagement de la France en faveur d'un principe de « loyauté » des grandes plateformes numériques (ex : Facebook, Google) vis-à-vis de leurs utilisateurs, qui doivent notamment être informés de l'usage qui est fait de leurs données personnelles.

Enfin, la sécurité doit également être prise en compte dans ces travaux. À ce titre, il est crucial que les Européens s'entendent sur une législation relative à la conservation des données de connexion par les opérateurs de télécommunication, enjeu clé de la lutte contre la cybercriminalité, ainsi que sur le projet de registre des noms de passagers aériens (Passenger Name Record) européen, dont les tragiques événements de Paris viennent rappeler l'urgente nécessité.

La libre circulation des données contre la « balkanisation de l'Internet »

La France agit pour la préservation d'un Internet libre et ouvert à l'échelle globale, tant du fait de notre attachement à la liberté d'expression et d'information que des opportunités économiques que procure cette interconnexion planétaire.

Dans les enceintes de négociations relatives à la gouvernance de l'Internet, comme les réunions de l'ICANN (Internet Corporation for Assigned Names and Numbers, organisme en charge des noms de domaines sur Internet) ou de l'UIT (Union internationale des télécommunications), la France plaide pour le maintien d'une approche « multi-acteurs » de cette gouvernance, où non seulement les États, mais également le secteur privé et la société civile, parties prenantes fondamentales de l'Internet, doivent être entendus. Pour autant, le système ne fonctionne pas aujourd'hui de manière optimale et doit être rénové pour plus de démocratie, d'inclusivité et de transparence. Les États, seuls dépositaires de la légitimité représentative, ont un rôle central à jouer

dans cette gouvernance dès lors qu'elle emporte des conséquences sur nos politiques publiques (sécurité, fiscalité, protection de la jeunesse, indications géographiques…).

La volonté de préserver l'interconnexion globale et le refus d'une fracturation de l'Internet selon des lignes nationales (« balkanisation »), ne doivent cependant pas nous aveugler sur les limites d'une application indifférenciée et systématique du « *free flow of data* » (libre circulation des données) à l'échelle globale. Alors que le cloud computing permet aujourd'hui un stockage des données à tout endroit de la planète, un maintien de certaines données sur un territoire géographique donné doit rester envisageable, tant pour des raisons de souveraineté que de préservation des libertés.

L'ouverture des données publiques : un gisement de libertés et de croissance

L'ouverture des données publiques, aussi appelée « open data », n'est pas un phénomène nouveau en France, où dès 1978 est créée, au même moment que la CNIL, la Commission d'accès aux documents administratifs, la CADA. A l'heure d'Internet, les possibilités de cette ouverture sont démultipliées, permettant de renforcer encore l'information du citoyen et d'ouvrir de nouveaux gisements de croissance pour les entreprises souhaitant valoriser ces données, par le biais du big data (traitement massif des données) notamment.

Très impliqué dans ce processus d'ouverture, le ministère des Affaires étrangères et du Développement international a rendu publiques de nombreuses informations relatives à ses activités (ex : données sur l'expatriation ou le travail à l'étranger). Au niveau diplomatique, la France a rejoint en 2014 le Partenariat pour le gouvernement ouvert (PGO), une initiative internationale créée en 2011 visant à promouvoir la transparence et l'intégrité des gouvernements à l'ère d'Internet. La France prendra la présidence du PGO en 2016 pour un an.

La cybersécurité : un enjeu de coopération internationale

Un grand nombre de données circulant sur nos réseaux aujourd'hui sont constitutives de notre sécurité économique et de notre sécurité nationale. Le citoyen doit lui aussi être préservé des attaques sur les réseaux où transitent ses données. Il est donc impératif de garantir l'existence de systèmes d'information et de communication sûrs. Dans un environnement toujours plus interconnecté, la coopération internationale sur les enjeux de cybersécurité est incontournable.

Dans les organisations régionales dont elle est membre, comme l'UE ou l'OTAN, la France agit pour que les données sensibles manipulées par ces organisations, qui touchent aux domaines politique, commercial, militaire et qui constituent autant d'actifs partagés entre la France et ses partenaires, soient protégées par une cybersécurité exigeante. Ces enceintes doivent également accompagner, dans la

mesure de leurs moyens et de leurs compétences, la montée en puissance de leurs États membres, qui demeurent responsables de leur propre cybersécurité. À l'échelle de l'UE, la France plaide par ailleurs depuis plusieurs années pour l'émergence d'une filière industrielle européenne de la cybersécurité et du numérique de confiance. Le rapprochement effectué avec l'Allemagne en la matière, comme le montre l'exemple du cryptage des mails, doit constituer un socle pour nos travaux futurs.

À l'échelle des Nations Unies, les discussions portent sur la sécurité internationale du cyberespace. Un groupe d'experts gouvernementaux, au sein duquel a siégé la France, a remis en juillet 2015 au Secrétaire général un rapport comportant des recommandations pour un comportement responsable des États dans le cyberespace. Dans cette enceinte, la France plaide notamment pour que la cybersécurité ne soit pas utilisée comme un prétexte par certains États pour exercer un contrôle liberticide de leur Internet national. Enfin, sur le plan économique, lors du G20 d'Antalya en novembre 2015, la France a admis avec ses partenaires que les États ne devaient pas soutenir le vol, par des moyens cyber, de données compétitives d'une entreprise, visant à en faire bénéficier leurs propres entreprises ou secteurs commerciaux.

En conclusion, l'émergence d'un pôle européen autonome et dynamique au sein d'un cyberespace global mieux régulé s'avère aujourd'hui nécessaire. L'Europe développe une conception propre en matière de protection et de sécurité des données, pour lesquelles elle constitue une véritable terre d'accueil. Elle dispose par ailleurs d'un énorme potentiel technologique et industriel, lui permettant de prendre toute sa place dans la révolution technologique à l'œuvre. Elle doit désormais se doter des outils réglementaires, financiers et politiques pour être en mesure de s'autonomiser. C'est dans cet esprit que la France a proposé dans sa nouvelle stratégie de sécurité du numérique en octobre 2016, l'élaboration d'une feuille de route vers l'autonomie stratégique de l'UE en matière de numérique. C'est de cette autonomie que l'UE tirera la force de faire respecter son système de valeurs et de s'intégrer pleinement à la nouvelle économie de la donnée, tout en assurant la sécurité de ses citoyens.

L'AUTEUR

David Martinon est un haut fonctionnaire du ministère des Affaires étrangères et du Développement international, où il occupe actuellement le poste d'Ambassadeur pour la cyberdiplomatie et l'économie numérique au. Auparavant, il a notamment occupé le poste de conseiller diplomatique du ministre de l'Intérieur, puis de porte-parole de la présidence de la République française, avant d'être nommé Consul général de France à Los Angeles.

DOSSIER

PROTECTION DES DONNÉES ET VIE PRIVÉE

La donnée,
cible privilégiée des prédateurs

par MARC WATIN-AUGOUARD

Jamais sans doute l'humanité n'a connu, sous l'effet de la transformation numérique, un bouleversement aussi universel dans son application, aussi intense dans ses manifestations, aussi profond dans ses conséquences.

Un monde modelé par une vaste palette technologique

Les données sont les ressorts de la puissance et de la dynamique d'une métamorphose qui combine les applications de nombreuses innovations technologiques : – l'informatique en nuage ou le *cloud computing* offre des capacités de stockage et de traitement jusqu'à aujourd'hui inégalées, mais soulèvent des questions de sécurité et de souveraineté ;

MARC WATIN-AUGOUARD

Général d'armée (2S)
Directeur du centre de recherche de l'école des officiers de la gendarmerie nationale.

– le big data ou mégadonnées, associé aux algorithmes, permet de mieux comprendre la réalité du monde et de favoriser l'analyse prédictive par la mise en perspective de milliards de données captées et analysées en temps réel ;

– la réalité augmentée va notamment superposer l'image virtuelle à la vision du monde réel et accroître les capacités intellectuelles et physiques de l'homme;

– la robotique pose, dès à présent, la délicate question de la relation entre l'homme et le robot doté d'intelligence artificielle, capable de s'adapter par l'auto-apprentissage ;

– l'internet des objets va tout mesurer, décrire, organiser nos vies et peut-être décider à notre place ;

A tout cela s'ajoute la convergence des nanotechnologies, des biotechnologies, de l'informatique et des sciences cognitives.

Bref, les nouvelles technologies de l'information et de la communication vont remodeler notre monde, en se conjuguant, en

stimulant mutuellement leurs effets, en entrant en « résonnance ». Le secteur quaternaire, ou secteur numérique, celui qui émerge avec l'interconnexion mondiale des systèmes ayant recours au tout numérique, offre une extraordinaire opportunité pour la criminalité et la délinquance.

La donnée est un instrument de la puissance numérique

La cybercriminalité frappe notamment la couche cognitive, celle des contenus, qui constitue le patrimoine informationnel porteur de valeur, de sens, source du savoir et donc du pouvoir. La cible principale des prédateurs est bien la donnée sous toutes ses formes. Elle permet de s'en prendre directement ou indirectement aux personnes, aux biens, aux services, aux systèmes de traitement automatisé de données. Cette donnée, thème central du prochain Forum international de la Cybersécurité, est visée pour ce qu'elle représente, parce qu'elle est une parcelle de la souveraineté, de l'influence, de la compétitivité économique ou parce qu'elle est une monnaie d'échange, un moyen de chantage ou, pire, un moyen de dominer les esprits. Aujourd'hui, la donnée n'est plus annexe, ni connexe : elle est désormais au cœur de l'écosystème du cyberespace. Elle est intimement liée à l'individu, auquel elle confère une identité numérique, à l'entreprise, dont elle constitue le patrimoine immatériel, à l'Etat qui accroît avec elle sa liberté d'action. Personnalité, compétitivité, souveraineté, telle pourrait être la trilogie servant de « devise » pour la donnée.

L'algorithme, un instrument de pouvoir en voie d'autonomie

Hier fruit de l'action humaine, la donnée s'autonomise désormais sous l'influence des machines connectées, plus nombreuses, depuis 2008, que la population de la planète. Les objets "intelligents", sans échapper au dialogue avec les individus, deviennent des objets bavards qui communiquent entre eux, de machine à machine malgré l'homme, créant ainsi des données et métadonnées, structurées ou non, qui ne se perdent pas, se transforment et, même, se reproduisent. Les algorithmes, la vitesse de calcul, la capacité de stockage sont les moteurs de leur fertilité.

Lorsqu'elle rencontre le *big data*, la donnée s'inscrit dans le temps de son créateur tout en le devançant par son pouvoir prédictif. La donnée est vivante, survivante, sauf si le droit à l'oubli la rend mortelle.

Donnée kidnappée, donnée usurpée, donnée dénaturée, mais donnée libérée au profit de la transformation numérique ! Trop ouverte, la donnée peut conduire l'homme à l'état de zombie, d'esclave des colonisateurs du numérique. Trop fermée, elle peut être un frein au progrès. La juste voie est celle de l'équilibre qui garantit une divulgation maîtrisée. Cela passe assurément par une nouvelle conception du secret : secret de l'intimité de chaque être humain à l'heure de « l'exposition de soi », secret des affaires qui préserve la compétitivité, voire la survie des entreprises, secret de l'Etat, sans lequel il ne peut affirmer sa souveraineté et donc son indépendance. Le mot « secret » n'est guère à la mode, tant il est décrié par les partisans d'un nouveau totalitarisme : celui de la transparence. Choisissons alors pour le remplacer le « mystère » en ce qu'il a d'inaccessible, tout en révélant ce qui est juste nécessaire.

Données en cyberdéfense,
le Big Data par excellence ?

par AXEL LE POUPON

À l'instar des autres disciplines issues de l'essor numérique, la cyberdéfense n'échappe pas au défi de l'accroissement exponentiel des données. Tous les acteurs du domaine, étatiques ou privés, y sont désormais confrontés. Avoir la maîtrise des données liées aux opérations numériques, c'est s'assurer la compréhension, donc le contrôle, d'un champ hautement conflictuel et stratégique.

Sources ouvertes, données forensiques et fichiers de log sont autant d'informations qui viennent alimenter des bases dont la forme et les fonctions se démultiplient. Ainsi, la maturité d'une organisation œuvrant en cyberdéfense dépendra grandement de sa capacité à construire et manipuler un large corpus de données cohérent, consolidé, fiable et exploitable. Pour en mesurer les forts enjeux sous-jacents, nous allons détailler les raisons justifiant d'une telle importance, balayant tous les aspects relatifs à ces données.

AXEL LE POUPON
Normalien, docteur de Telecom ParisTech, stagiaire Mastère Spécialisé en cyberdéfense

De vastes besoins

En premier lieu, il convient de recenser les nombreux usages des données au profit de la cyberdéfense. En effet, leur gestion dans ce domaine est primordiale car elle conditionne ou participe à de nombreuses activités.

On pourra notamment citer le rôle essentiel des données techniques dans la détection des traces d'un acte malveillant, que ce soit par le biais de sondes passives ou au gré d'une campagne de recherche de compromission précise. Autre exemple, l'étude approfondie d'une attaque informatique est largement conditionnée par une connaissance *a priori* des données et mécanismes pouvant

fotolia.com

Des fonctions d'analyse, de détection et d'attribution pour gérer des données hypertrophiées.

intervenir dans celle-ci. En permettant l'analyse d'un incident ou le recoupement de plusieurs événements suspects, les données déjà connues ou alors identifiées consolident la compréhension du mode opératoire d'un attaquant. Enfin, graal inaccessible pour certains, véritable leitmotiv pour d'autres, l'attribution d'un acte malveillant n'est envisageable que par la conjonction de nombreuses données périphériques. En effet, seules des informations accumulées dans le temps et agrégées sur plusieurs campagnes garantissent la pertinence d'une telle analyse.

On pourrait aussi citer les perspectives de neutralisation des effets[1], voire de riposte, contre une attaque ciblant des réseaux critiques. Officiellement portée par l'État français[2], la politique visant à dissuader des acteurs malveillants ne pourra s'appuyer uniquement sur le développement d'une capacité offensive, aussi tangible soit-elle. En effet, la faculté à appréhender une attaque (de sa détection à son attribution) par des données concrètes est une condition *sine qua non* à une dissuasion crédible puis à la mise en œuvre efficace d'une réaction le moment venu. On comprend dès lors que la constitution d'un « *Big Data*

(1) Telles que stipulées dans l'article 21 de la LPM 2014-2019

(2) Comme l'a rappelé le ministre de la Défense lors de la conférence #Cyberdéfense2015 du 24 septembre 2015

cyberdéfense » en France n'est pas uniquement un problème à la portée strictement technique mais un enjeu majeur assurant un des piliers de la stratégie nationale.

On notera par ailleurs que les fonctions de détection, d'analyse et d'attribution constituent un cercle vertueux. Chaque activité s'appuie sur de nombreuses données issues des autres et en produisent de nouvelles au profit de celles-ci. Les proportions engendrées par une pratique régulière de ce cycle peuvent alors être rapidement qualifiées de massives. Cette accumulation progressive de données nous amène donc à nous interroger sur la question de leur structuration et leur nature.

Hétérogénéité et pertinence

Quand on parle de données d'intérêt en cyberdéfense, on fait non seulement référence à des données techniques (marqueurs de compromission, signatures…) mais aussi à des données plus contextuelles (comme le nom d'une opération numérique, l'identité de victimes identifiées…) voire à des informations de type comportemental (heure de travail des hackers, langue de programmation d'un code malveillant, heuristique *ad hoc*…). Bien entendu, toutes ces données se doivent d'être aussi horodatées (date de création, de première découverte, de dernière détection…), tracées (trouvées en propre, présentes dans un rapport tiers, issues d'une conclusion d'expert…), adjointes d'un niveau de classification (notamment dans le cas d'éléments trouvés sur des réseaux sécurisés ou obtenus par le biais de rapports confidentiels) et d'un niveau de fiabilité approprié (qui permettra par exemple de mesurer le risque de faux positif[3] correspondant ou de donner une cotation sur une hypothèse).

(3) Un faux positif ou fausse alarme peut survenir selon la nature du test, d'un algorithme de classification ou d'un choix fonctionnel.

Si l'on poursuit la réflexion, on retrouve alors toutes les problématiques et les travaux inhérents à la structuration de données complexes. La multitude d'informations disponibles correspond aussi bien à des objets qu'à des relations entre ces objets. À titre d'illustration, on devra pouvoir intégrer dans le modèle des notions telles que « *une signature A ayant permis de détecter un logiciel malveillant B présent sur un ordinateur C appartenant à la société D* ». Or, à l'heure actuelle, il n'existe pas de format qui s'impose. De nombreux modèles ont été proposés, avec des structures plus ou moins évoluées, sans qu'aucun ne devienne incontournable. On pourrait évoquer, entre autres, STIX[4], MISP[5] ou OpenIOC[6]. Leurs vocations respectives visent à traiter de manière plus ou moins exhaustive, avec des considérations plus

(4) Structured Threat Information eXpression

(5) Malware Information Sharing Platfor

(6) IOC pour Indicator Of Compromise

ou moins pratiques, les problématiques évoquées ci-dessus.

Reste que, si le problème de la structuration d'une base de données propre aux besoins en cyberdéfense est déjà bien adressé, il subsiste des marges de progression significatives dans la mise en œuvre de celle-ci.

Des fonctionnalités encore peu développées

Se doter d'une base de données adaptée aux besoins en cyberdéfense est essentiel, mais sa taille et sa structure, à l'instar d'un Big Data, impose de penser de nombreuses fonctionnalités sous une forme adaptée. Devant l'ampleur d'une telle base, il faut être à même d'en appréhender l'alimentation (par des données ou des processus externes), la visualisation (par des utilisateurs aux objectifs et aux droits variés), l'extraction (de données pour un partage vers un tiers) et le traitement (pour le croisement et l'analyse).

Concernant l'alimentation d'une telle base, il paraîtrait préjudiciable de ne prévoir que des possibilités de saisie manuelle. Cependant, l'alimentation automatique se confronte à de multiples difficultés : *parsing* intelligent de fichiers, données très lacunaires, redondances *a posteriori* de données, … Les solutions semi-automatiques offrent plus de souplesse, mais réclament un réel investissement, ainsi qu'une certaine capacité à normaliser les entrées dans la base, indépendamment de l'opérateur les saisissant. Devant ces obstacles, et ce malgré sa pertinence et son degré de raffinement, il existe un risque non négligeable qu'une telle base ne soit jamais alimentée correctement si ces exigences ne sont pas prises en compte en amont.

La visualisation est quant à elle un champ d'exploration à part entière, d'autant qu'elle dépend grandement de la finalité attendue. Avec un tel corpus structuré de données, on peut envisager des usages très différents : un décideur cherchant à obtenir une vue d'ensemble sur une campagne d'espionnage numérique donnée, un expert voulant recenser l'intégralité des marqueurs techniques sur la phase d'exfiltration d'une attaque, un responsable SSI souhaitant s'assurer qu'une victime s'est bien vue communiquer les données relatives à un incident… Les problématiques respectives d'affichage de données pertinentes et intelligibles sont, certes différentes, mais tout aussi complexes : il n'existe pas de manière unique d'aborder une telle base. Il faudra faire appel à tous les ressorts d'ergonomie et de dataviz actuellement développés, en lien étroit avec les utilisateurs concernés. Nous ne traiterons toutefois pas ici plus avant ce long sujet qui mériterait une littérature complète.

L'extraction est une problématique plus abordable, quoiqu'elle nécessite une maîtrise très fine des niveaux de classification des données et d'habilitation des utilisateurs. Or, les modèles de données évoqués précédemment développent tous cette notion de partage et d'échanges d'informations, confirmant le fort besoin des intervenants dans ce domaine. Toutefois, la multitude d'acteurs en cyberdéfense, en France et au niveau international, constitue un écosystème complexe, aux normes de confidentialité parfois disparates, sans équivalence simple : classifications *Secret* anglo-saxonnes, Confidentiel français ou codage TLP[7] entre autres. Des problématiques réelles en résultent, telles que la mise à disposition et la recherche de marqueurs classifiés sur des réseaux non classifiés. De plus, le niveau d'habilitation adéquat ne garantit pas toujours à lui seul l'accès à l'information : la notion de confiance joue un rôle important dans les échanges en cyberdéfense, la non-dissémination des informations étant souvent une contrainte forte. Enfin, on peut ajouter la notion de propriété d'une donnée qui, bien qu'elle semble parfois inappropriée (à qui appartient le *hash* MD5 d'un *malware* ?), peut se justifier dès qu'elle découle d'un niveau d'expertise rare. Il conviendrait alors de s'interroger sur le risque de voir apparaître un marché de la donnée en cyberdéfense, au même titre qu'il existe un marché (plus ou moins officiel) des vulnérabilités.

(7) *Traffic Light Protocol*

En dernier lieu, le sujet du traitement des données représente un challenge élevé sur un *Big Data*, auquel on se réfère alors sous le terme de *Data Mining*. L'hétérogénéité des données, la nature des mécanismes en jeu et les caractéristiques du cyberespace (ubiquité, intangibilité, transnational, …), couplées à une culture de la SSI parfois faiblement développée (cf. la récente stratégie française[8], dont l'un des axes d'effort est le renforcement de la sensibilisation) offrent de nombreuses perspectives pour un attaquant d'évoluer sans être inquiété. Il en résulte que les recherches et recoupements doivent être menés tous azimuts, chaque pièce à conviction conservée et chaque détail archivé. Pour le traitement de cette myriade d'indices, formidable puzzle, l'utilisateur devra faire preuve d'une capacité d'analyse dédiée à un nombre restreint d'experts. Encore faudrait-il qu'ils aient accès aux outils et méthodes adaptés…

(8) Conférence du Premier Ministre sur la sécurité du numérique du 16 octobre 2015

Ces fonctionnalités, bien connues sur des bases de données plus communes, restent aujourd'hui d'épineux problèmes, peu étudiés dans le cadre de la cyberdéfense. Leur résolution passe par une vraie capacité d'innovation qui fait

défaut jusqu'ici. La communauté française (notamment les organismes spécialisés de la Défense, l'ANSSI et des acteurs privés) pourrait avantageusement bénéficier de tels travaux : si les notions de partage doivent être traitées avec prudence, la constitution d'un socle commun de travail, serait une première étape très profitable, offrant une interopérabilité future.

Une excellence française à construire

L'exacerbation croissante des conflits géostratégiques qu'engendre le cyberespace appelle à s'intéresser très sérieusement au sujet de la capitalisation coordonnée des connaissances en cyberdéfense. Or, au titre des projets de souveraineté numérique nationale, il existe un véritable enjeu à construire une appréciation critique et cohérente des cybermenaces au sein d'une communauté française. Cette solution de « *Big Data* cyberdéfense », fondée sur des moyens pérennes prenant en compte l'ensemble des facteurs évoqués précédemment, pourrait représenter un atout majeur dans la stratégie engagée par la France.

La donnée : source
d'information ou vecteur de confusion

par PATRICK PERROT

Le monde qui se construit aujourd'hui connaît une métamorphose structurelle en mutant de l'information vers la donnée. Alors que notre actualité est inondée d'informations, s'ajoute un déluge de données qui se déverse chaque jour autour de nous. C'est l'annonce d'une révolution annoncée comme informatique mais qui s'oriente bien plus vers un changement sociétal. Celui-ci porte un nom : le Big Data.

Le changement en cours a des conséquences sur notre appréhension de la donnée comme, d'une façon plus globale, sur celle des concepts découlant de la donnée. Les répercussions sont perçues dans le monde de l'information bien entendu mais aussi dans l'univers médical, financier, dans la sécurité ou l'économie. En effet, comme le précise Manuel Castells dans l'Ère de l'information : « *une révolution technique centrée sur des processus informationnels remodèle à un rythme accéléré les fondements matériels de la société* ». Face à ces bouleversements, il nous faut d'urgence comprendre le sens de la donnée afin que celle-ci soit source de valorisation et non porteuse de confusion.

PATRICK PERROT
Lieutenant-colonel de gendarmerie affecté au Service Central du Renseignement Criminel

Un déluge annoncé

Le terme de Big Data avait déjà fait son apparition dans différentes publications dès 1997 au sein de la bibliothèque numérique de l'ACM (Association For Computing Machinery). Pourtant, à cette époque, les GAFA (Google, Apple, FaceBook, Amazon) n'ont pas encore révélé tout le potentiel des bases relationnelles, du calcul parallèle et de l'accroissement des capacités matérielles et logicielles. Cela ne saura tarder. Dès 2004, au sein de Google Labs, émerge un

algorithme reposant sur des opérations analytiques à grande échelle; c'est la naissance de Map Reduce. Cet outil permet d'effectuer des calculs parallèles et distribués à partir d'un nombre particulièrement conséquent de données. Dès lors, Doug Cutting, travaillant chez Apache optimise ses développements en cours et crée Hadoop, une plate-forme distribuée pour le stockage et le calcul. Le concept du Big Data existait, il peut désormais se déployer à partir des outils proposés par Map Reduce et Hadoop.

Il est alors possible de faire face à un volume gigantesque de données, de nature hétérogène, non structurée et à la temporalité éphémère. La vitesse d'exécution des algorithmes de traitement de l'information permet en outre d'envisager une réactivité en temps réel. La règle des 3V (volume, variété,vélocité) émis par Gartner en 2012 a d'abord défini le Big Data: « *Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization.*(1) ». Rapidement ont fleuri de nouveaux V : la visibilité, la véracité et la valeur. Parce que Big Data comprend sept lettres, nous pourrions conclure cette liste par un 7e V, la volatilité. En effet, le déluge de données se signifie pas, bien au contraire, une donnée robuste, stable et fiable. Face à cette croissance des données qui défie la loi de Moore(2), la question est de savoir si nous sommes aujourd'hui en capacité de l'analyser de façon objective, d'éviter des erreurs d'appréciation et d'appréhension de la continuité de la donnée génératrices de risques sur le théâtre opérationnel. En d'autres termes, le challenge est d'assurer la transition entre la maîtrise de l'information et celle de la donnée.

De l'information à la donnée

Les cinquante dernières années sont souvent définies comme le règne de l'information et de la communication, né de l'extension exponentielle de technologies numériques et informatiques. Il en ressort une transformation de nos relations et de notre appréhension du réel. Nous sommes passés d'un monde fondé sur des rapports matériels à un espace plus élargi reposant sur des rapports immatériels. Des précurseurs comme Henri Laborit avait, dès les années soixante-dix, compris le rapport entre l'homme et l'information : « *Il faut propager au plus vite cette notion que l'homme n'est pas une force de travail, mais une structure qui traite l'information.* » Pourtant, ce règne en est déjà à son crépuscule, cédant progressivement sa place à celui de la donnée. La différence entre ces deux notions n'est pas anodine. La donnée se définit comme un élément brut et fondamental. Elle ne possède pas de sens à proprement parlé, elle n'apporte pas de valeur, elle n'en enlève pas non plus. L'information quant à elle, peut se définir comme une donnée placée dans un contexte et est, dès lors, sujette à interprétation. Elle est porteuse de sens et influe sur le contexte.

Alors que le réel est un concept continu, l'information se caractérise de manière discontinue en apportant des éclairages ponctuels et précis pouvant expliquer le réel. L'avènement de la donnée diminue le pas d'échantillonnage au sens de la théorie de l'information. Ce dernier se restreint et tend vers une appréhension continue du réel. Claude Shannon, théoricien des mathématiques, avait parfaitement défini la nécessité de l'échantillonnage (à l'origine notamment de la numérisation des signaux) eu égard à notre incapacité à intégrer l'ensemble des informations de manière continue. Par l'émergence de la donnée, nous pouvons désormais tendre vers la fin de l'échantillonnage à la condition de disposer de données exhaustives. La donnée constitue l'outil permettant de faire le grand écart entre la globalisation et l'individualisation. Il est à la fois possible de suivre et d'anticiper les grandes épidémies à l'échelle mondiale tout en analysant le comportement individuel de monsieur X par rapport à ses déplacements ou ses achats.

La donnée génératrice de confusion

Aujourd'hui dans un monde de la donnée, il nous faut développer des méthodes en mesure d'appréhender ce nouvel espace, ce qui n'est pas sans difficulté. Richard Belmann a évoqué la malédiction mathématique de la dimensionnalité [1] [4] qui rend difficile la discrimination, la détection ainsi que la classification au sein d'un ensemble de données. En effet, analyser des données dans des espaces de grande dimension génère divers phénomènes qui n'apparaissent pas dans des espaces de dimension moindre.

Face à cette question, les méthodes de réduction ont permis de simplifier le problème en construisant des invariants si possibles robustes aux conditions externes. Malheureusement, la construction de règles générales comme la mise en évidence d'invariants tend à lisser l'influence de paramètres ne disposant, certes pas, de la plus grande variance mais dont la nature hors norme est à prendre en compte. C'est l'ambition de méthodes comme les réseaux neuronaux ou l'inférence bayesienne qui cherchent à améliorer la stabilité des décisions et à ajouter de l'*a priori* pour contredire l'adage « *plus d'information tue l'information* ». Le Big Data, par sa capacité à engendrer une multitude d'informations diverses et à l'analyser, doit répondre à ce challenge. La donnée pourra sortir d'une malédiction de la dimensionnalité à la condition d'être appréhendée par des spécialistes du traitement de l'information.

Compliquant la situation d'exploitation objective des données, la vulgarisation des algorithmes mais surtout la disponibilité des outils par l'intermédiaire d'Internet notamment, accroissent le risque d'une mauvaise utilisation. Exploiter la donnée est en apparence aujourd'hui accessible à tout un chacun, alors que les concepts mathématiques sous-jacents sont bien souvent complexes. Que ce soit les “vaches de Gamow”[3] ou l'affaire Alan Sokal[9] qui témoigne de l'appropriation par une

fotolia.com

La donnée informationnelle, fiable et valorisée, doit résulter d'une application de méthodes mathématiques maîtrisées avant d'être mise à la disposition des opérateurs.

communauté non scientifique de théories erronées, le raccourci dans l'analyse comme dans l'interprétation des données est un risque bien réel. Alors que la vulgarisation [2] assure en général d'une manière plutôt positive une transition simplifiée entre un sachant et un public profane, l'accessibilité, sans intermédiaire, des méthodes scientifiques offre des possibilités analytiques sans contrôle. Dans une perspective d'élargissement culturel, la vulgarisation comme l'accessibilité aux méthodes revêtent un caractère très positif. Pour autant, nous ne pouvons ignorer les conséquences de la mise en œuvre d'applications par des non-initiés. Outre le risque appréciatif, c'est aussi un changement de paradigme qui fait émerger l'outil en lieu et place de la méthode. Avec Internet apparaît l'illusion d'un espace ouvert à tous, abolissant la nécessité de la maîtrise théorique au profit d'un raccourci guidé par l'empirisme. Internet, en donnant accès à une masse quasi infinie d'informations et d'outils, peut à la fois donner l'illusion d'un savoir et contribuer à une conception qui instrumentalise la connaissance. Celle-ci ne se perçoit alors qu'à travers son utilité pour une utilisation pré établie.

L'explosion de la donnée nous renvoie bien évidemment à la fiabilité offerte par le web. Depuis déjà de nombreuses années, l'espace virtuel constitue un lieu à la potentialité criminelle avérée [7], mais plus qu'hier, la notion de fiabilité de la donnée accessible demeure, aujourd'hui, essentielle. Qui n'a pas consulté l'encyclopédie en ligne Wikipedia pour s'informer sur une thématique particulière ? Pour autant qui s'est assuré de la véracité des propos tenus ? Nous pouvons légitimement considérer que la fiabilité des informations délivrées n'engendre que peu de conséquences dans le cadre d'un usage personnel. Néanmoins, lorsque les consultations ont trait à des investigations d'intérêt criminel via des blogs et des réseaux sociaux, la fiabilité de l'information doit être une indispensable préoccupation notamment à l'heure du web invisible. Il est admis aujourd'hui qu'une grande majorité des flux d'information transite au sein de cet espace. La question est alors de savoir si le web visible ne peut pas constituer un vecteur de désinformation utilisé par les groupes criminels (comme par le délinquant isolé) alors que l'information d'intérêt circulerait *via* la face cachée du web. Pourquoi ne pas émettre sur sa page Facebook des photographies de fausses

destinations, de faux amis, de fausses relations, voire tout simplement un faux compte Facebook ?

De même, nous pouvons nous interroger sur l'exhaustivité des informations présentes sur le web visible. Une utilisation croissante par tout un chacun du web invisible, non plus pour masquer une activité illégale mais dans le cadre de la protection des libertés individuelles et éviter ainsi d'être tracé par les grands acteurs du web est parfaitement envisageable. La donnée disponible sur ce que nous qualifions de sources ouvertes doit, en dépit de l'attrait immédiat, faire l'objet d'une attention particulière. N'oublions pas non plus qu'une donnée en sources ouvertes est déposée par un individu qui fait un choix partial et est indexée par un unique moteur de recherche qui en 2015 est utilisé à près de 94 % en Europe. Qui utilise Qwant, le moteur européen, Bing, Yandex RU, WolframAlpha, ou encore Base pour consulter d'autres sources, prendre en compte des données non apparentes sous Google, voire confronter les données indexées par ce dernier? Comprendre les raisons de la présence d'une donnée en source ouverte peut s'avérer particulièrement pertinent.

Ainsi à travers le problème de la dimensionnalité, de l'accessibilité et de la fiabilité se dessine une malédiction de la donnée capable d'apporter des résultats erronés ou mal interprétés et générer des confusions aux conséquences néfastes dans les champs applicatifs. Pourtant, et à partir de précautions d'utilisation établies, la donnée ouvre des perspectives extrêmement intéressantes en terme d'optimisation du renseignement notamment dans le domaine de la sécurité.

La valorisation de la donnée au service de la sécurité

Le challenge ouvert aujourd'hui aux forces de l'ordre est sans précédent dans la capacité à appréhender un monde criminel confus et en évolution permanente. La donnée constitue une pièce essentielle à l'élaboration d'un renseignement ciblé et précis. Le succès et la pertinence de l'exploitation de la donnée reposent néanmoins sur la maîtrise et le développement de méthodes mathématiques novatrices capables d'exploiter et de sécuriser des données massives, hétérogènes et éphémères.

Au sein du service central de renseignement criminel de la gendarmerie nationale, la donnée de masse a aujourd'hui été prise en compte avec la volonté de comprendre la criminalité et, dans la mesure du possible, de l'anticiper. Structurante dans le cadre du renseignement criminel, qui a vocation à exploiter dans un cadre légal tout type de données utile à la baisse de la criminalité en vue d'apporter des éléments proactifs d'aide à la décision, l'analyse de données est le fait de scientifiques, de criminologues et d'enquêteurs judiciaires [5][6]. En effet, la compétence « métier » associée à la compétence scientifique permet de prévenir les risques mentionnés préalablement. La création de valeur peut objectivement se concevoir à partir de la réunion de savoir-faire englobant la mobilisation de données de sources plus ou moins hétérogènes, en construisant des modèles mathématiques adaptés et adaptatifs et en réévaluant les

résultats obtenus au plus près du besoin opérationnel. La disponibilité des données notamment sur Internet ne doit pas faire oublier la donnée d'intérêt qui est bien souvent interne et qui doit constituer le socle de l'analyse. Bien entendu les informations obtenus *via* l'open data peuvent s'avérer pertinentes mais elles doivent d'abord enrichir une base bâtie sur des sources internes. Cela permet de se garantir de différents écueils tels que le manque de fiabilité, le manque d'exhaustivité ou encore la partialité. Les sources internes qui revêtent un caractère confidentiel en raison de leur nature peuvent concerner des données propres aux services de sécurité, aux entreprises, voire aux individus, notamment par l'essor des objets connectés. La confidentialité attachée à cette forme de donnée, ne signifie pas qu'elle ne doivent pas être exploitées mais plutôt que leur exploitation doit répondre à des règles objectives de protection des libertés individuelles. L'intérêt principal de la donnée issue de sources internes est sa maîtrise, sa précision, sa fiabilité voire son exhaustivité, c'est-à-dire des caractéristiques qui bien souvent manquent aux données disponibles en sources ouvertes. Dès lors, la valorisation de la donnée ne peut s'affranchir d'une méthodologie qui consiste à appliquer de manière raisonnée des méthodes mathématiques maîtrisées, à établir un socle à partir d'un patrimoine interne, à l'enrichir à partir de données externes pour enfin aboutir à une interprétation exploitable et pertinente. Ce cheminement rigoureux conditionne la valorisation de la donnée en minimisant le risque de confusion.

Ainsi, la donnée, richesse disponible à chacun, nécessite un examen, une structuration, une analyse comme une interprétation alliant diverses compétences que l'illusion de la disponibilité ne doit pas altérer. A cette condition, le Big Data répondra aux espoirs suscités dans notre approche comme notre appréhension du réel et nous garantira de la confusion pour nous guider vers la valorisation.

Bibliographie

[1] Bellman, R. E. Dynamic programming, Princeton University Press, 1957
[2] Cartellier D., La vulgarisation scientifique à l'heure de libre accessibilité des savoirs. Quelle place pour les médiateurs? Mémoires du livre - Studies in Book Culture, Volume 1, numéro 2, 2010
[3] Gamow G., Le Nouveau monde de M. Tompkins, Russell Stannard Editions le Pommier, 2007
[4] Giraud C., Introduction to High-Dimensional Statistics, Chapman and Hall/CRC, 2014[] Raichwarg D. et J. J., Savants et ignorants. Une histoire de la vulgarisation des sciences, Paris, Le Seuil, 1991, 296 p.
[5] Perrot P. L'analyse du risque criminel : l'émergence d'une nouvelle approche
[6] Perrot P. , Kader T. A. Forecasting analysis in a criminal intelligence context - Proceedings International Crime and Intelligence Analysis Conference, Grande-Bretagne 2015
[7] P. Perrot Mondes virtuels : un nouvel espace ouvert à la criminalité - Proceedings Workshop Interdisciplinaire sur la sécurité globale, France 2009
[8] Rapport final du groupe d'experts de haut niveau, Commission européenne, Construire la société européenne de l'information pour tous, Office des publications officielles des Communautés européennes, 1997, p. 17.
[9] Sokal A., Transgressing the Boundaries: Towards a Transformative Hermeneutics of Quantum Gravity, Social Text 46/47, printemps/été 1996, p. 217-252.

L'AUTEUR

Officier de gendarmerie au sein du service central de renseignement criminel, le lieutenant-colonel Patrick Perrot a combiné des commandements opérationnels et des fonctions de nature scientifique. Auteur de nombreuses publications dans le domaine des sciences forensiques et du renseignement, il est ingénieur et titulaire d'un doctorat de Télécoms Paris Tech.

Gendarmerie nationale : une nécessaire adaptation aux nouveaux défis cyber

par NICOLAS DUVINAGE

Vénérable institution pluriséculaire, la gendarmerie nationale a néanmoins toujours su innover en matière de cybercriminalité: création d'un laboratoire de criminalistique numérique (1992)[1], ouverture d'une "cellule de veille Internet" (1998), organisation de stages d'enquêteurs spécialisés (dès 1999), *etc.* En 2014-2015, elle s'est engagée dans une vaste modernisation de son dispositif, intégrant l'ensemble des dimensions de la problématique cyber, bien au-delà de la seule cybercriminalité.

(1) M.Jean-Yves LATOURNERIE, préfet chargé de la lutte contre les cyber-menaces.

NICOLAS DUVINAGE

Colonel de Gendarmerie
Chef du Centre de lutte Contre les Criminalités Numériques (C3N)
Service Central du Renseignement Criminel
Pôle Judiciaire de la Gendarmerie Nationale

Le livre blanc sur la défense et la sécurité nationale de 2008, la création puis la montée en puissance de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en 2009, la nomination en 2012 d'un officier général - conseiller cyber du chef d'état-major des armées - puis la mise en place en 2015 d'un commandement cyber au sein du Centre de planification et de conduite des opérations (CPCO) des armées, l'institution d'un "cyber-préfet"[2] et d'un "cyber-ambassadeur"[3] en 2014, le rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité dit rapport Robert la même année, *etc.* : l'Etat s'est profondément réformé et adapté, se plaçant véritablement en ordre de bataille.

(2) M.Jean-Yves LATOURNERIE, préfet chargé de la lutte contre les cyber-menaces.

(3) M.David MARTINON, ambassadeur pour la cyber-diplomatie et l'économie numérique

Outre la définition d'un plan ministériel cyber et la création de la Délégation de lutte contre les cybermenaces dirigée par le "cyber-préfet", le ministère de

l'Intérieur a fait évoluer la Direction générale de la police nationale (DGPN) (création de la sous-direction de la lutte contre la cybercriminalité) et a renforcé les moyens de la Direction générale de la sécurité intérieure (DGSI). Il a également mobilisé la Direction de la coopération internationale (DCI) (stimulation du réseau des services de sécurité intérieure dans les ambassades, désignation d'un coordinateur cyber) et institué un point de contact privilégié avec les entreprises fournissant des solutions innovantes (Délégation ministérielle aux industries de sécurité – DMIS). Outre son autorité sur les brigades spécialisées[4], le préfet de police de Paris dispose désormais d'un conseiller cyber au sein de son cabinet.

(4) En particulier: Brigade d'enquête aux fraudes aux technologies de l'information (BEFTI), Brigade des fraudes aux moyens de paiement (BFMP), Brigade de protection des mineurs (BPM), Brigade de répression de la délinquance astucieuse (BRDA).

La gendarmerie a su, elle aussi, moderniser sa stratégie et son organisation. Un poste de coordinateur pour la lutte contre les cybermenaces a été créé au sein du cabinet du directeur général de la gendarmerie nationale (DGGN), pour sensibiliser le plus haut niveau décisionnel aux enjeux, assurer de façon optimale le positionnement de l'Arme aux côtés des autres administrations, des entreprises et à l'international, et veiller au développement des capacités cyber de la gendarmerie.

Anticipation opérationnelle: des troubles "dans la vie réelle" annoncés sur Internet

Longtemps cantonnée à la recherche traditionnelle du renseignement territorial par des contacts locaux avec des sources humaines, l'anticipation opérationnelle est désormais solidement ancrée dans le XXIe siècle. Sans renier de vieilles méthodes qui ont fait leurs preuves, les gendarmes scrutent aujourd'hui l'émergence de troubles à l'ordre et à la sécurité publics également sur Internet: appels à la mobilisation en faveur de manifestations violentes d'opposition aux grands projets d'aménagement du territoire, individus en voie de radicalisation, routes clandestines des passeurs de migrants, annonces de rave-parties non autorisées, "d'apéros géants Facebook" ou de "cannonball" (courses automobiles sauvages sur routes ouvertes), menaces proférées en ligne par des hooligans, *etc.* Grâce à un stage dédié au Centre national de formation au renseignement opérationnel (CNFRO), et sous la coordination de la section de veille numérique de la nouvelle sous-direction de l'anticipation opérationnelle (SDAO) de la DGGN, (presque) plus rien ne surprend les gendarmes!

Enfants et entreprises: des cibles de choix à protéger

En matière de prévention, à l'attention de nos plus jeunes concitoyens, la gendarmerie s'est inspirée du dispositif "Permis piéton" en milieu scolaire pour créer, aux côtés d'un partenaire privé (AXA Prévention), le dispositif "Permis

(5) http://www.permisinternet.fr

Internet"[5]. Mis en oeuvre dans les classes de CM2, ce programme national vise à responsabiliser les enfants et leurs parents, pour un usage vigilant, sûr et responsable d'Internet. « *On apprend à un enfant à utiliser Internet comme on lui apprend à traverser la route* », telle pourrait être la devise du "Permis piéton".

Les entreprises, et en particulier les PME qui sont les garantes de la vitalité économique de notre pays, sont une autre cible fragile, tant pour des cyberdélinquants que pour des concurrents prêts à tout. En parfaite coordination avec la Direction générale de la sécurité intérieure (DGSI) et la Direction générale de la police nationale (DGPN), la DGGN a récemment intégré la dimension cyber dans la formation délivrée aux référents sûreté et aux référents intelligence économique. Ces correspondants territoriaux des entreprises jouent un rôle crucial de sensiblisation aux risques. Sans jamais prétendre être des spécialistes de l'audit en sécurité informatique, et sans jamais se départir de leur neutralité à l'égard de produits, services ou solutions commerciales, ces référents peuvent également donner des conseils pratiques, élémentaires mais trop souvent ignorés ou méconnus, pour rendre plus robuste la protection des entreprises en matière cyber.

Réprimer...sans se priver des armes des cybercriminels

Le dispositif de lutte contre la cybercriminalité de la gendarmerie a, lui aussi, été profondément rénové.

S'appuyant sur une structure déjà existante (ex-division de lutte contre la cybercriminalité de Rosny-sous-Bois), le Centre de lutte contre les criminalités numériques (C3N) a été créé au sein du nouveau Pôle judiciaire de la gendarmerie nationale (PJGN) de Pontoise. Il constitue la véritable tête de pont d'un dispositif territorial décentralisé, dénommé réseau Cybergend.

Point d'entrée unique de la gendarmerie dans ce domaine spécifique de la police judiciaire, le C3N est le correspondant naturel de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), de l'ANSSI et de nombreux partenaires institutionnels ou privés. Il participe pleinement aux réunions spécialisées d'Europol et d'Interpol. Membre, sous l'impulsion du cyber-préfet, du groupe de contact permanent avec les opérateurs étrangers (Google, Apple, Facebook, Microsoft, Twitter, *etc.*), le C3N a contribué à l'élaboration de formulaires standard de réquisitions judiciaires pour les enquêteurs. Créé dès 2005, son site intranet Cyber-Aide, mettant en ligne de plus de 7 000 fiches pratiques et recevant plusieurs milliers de visites chaque semaine, apporte des conseils précieux à tous les gendarmes et policiers.

Menant ses propres enquêtes judiciaires avec une compétence nationale, le C3N assure également l'animation et la coordination du réseau Cybergend, fort de 2 000 enquêteurs spécialisés "NTECH" et "C-NTECH" répartis sur tout le territoire. Ces derniers sont désormais concentrés,

soit dans des groupes d'investigations dédiés au sein des sections de recherches (SR) chefs-lieux de juridictions inter-régionales spécialisées (JIRS), soit au sein de plateaux criminalistiques départementaux en cours d'accréditation assurance-qualité.

En complément des structures génériques de la gendarmerie qu'il éclaire de son expertise-métier (direction du personnel, sous-direction de la police judiciaire, services logistiques), le C3N participe à la définition et à la cohérence de la politique de formation cyber, du plan d'équipement spécifique tant matériel que logiciel, de la doctrine d'emploi, et contribue à la veille juridique et aux propositions d'évolutions normatives. En synergie avec le département informatique-électronique de l'IRCGN, il développe des outils et élabore des processus de travail harmonisés[6], tout en ayant une capacité de projection à des fins d'appui opérationnel ponctuel aux unités territoriales. Fer de lance des enquêtes sous pseudonyme sur Internet, il doit aussi savoir identifier, valoriser et propager les bonnes pratiques du réseau Cybergend. Riche de la diversité de ses enquêteurs et enquêtrices et des situations opérationnelles rencontrées localement, ce réseau est ainsi à l'origine de remarquables innovations, tant procédurales que techniques, ayant été parfois déterminantes pour la réussite d'enquêtes sensibles. Toutes les bonnes idées sont à prendre quand il s'agit du Darknet, des bitcoins, de logiciels de messagerie chiffrée, de fichiers hébergés sur le cloud à l'autre bout du monde, des "coups d'achats" anonymisés sur Internet ou de la captation de données informatiques à distance à l'insu d'un suspect!

(6) Un "manuel des opérations NTECH" est en cours de diffusion au sein du réseau Cybergend.

Placé sous l'autorité du nouveau Service central du renseignement criminel (SCRC), le C3N a enfin une mission d'étude et d'analyse de la menace criminelle: mieux identifier – notamment par des outils de big data - des recoupements entre affaires pour proposer aux magistrats et aux unités locales des stratégies d'enquête, détecter précocément les modes opératoires émergents des délinquants, connaître la "signature" de groupes criminels organisés, trouver des "capteurs humains" de renseignement, tels sont les nouveaux défis à relever.

L'AUTEUR

Colonel de gendarmerie, Nicolas Duvinage est le chef du Centre de lutte contre les criminalités numériques (C3N). Polytechnicien (X1995) et titulaire d'un mastère spécialisé de Télécom ParisTech, il a été chef du département informatique-électronique de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN). Il a commandé la compagnie de gendarmerie départementale de Rezé (44) et a été chef en second de l'Office central de lutte contre les atteintes à l'environnement et à la santé publique (OCLAESP).

Le Dark Web, place de marché des données volées

par **ADRIEN PETIT**

« Lieu d'anonymat absolu », « repaire pour pédophile ou encore « eBay de la drogue », le Dark Web fait l'objet de nombreux mythes et fantasmes. Cet espace comprend un ensemble de pages Web intentionnellement cachées via des réseaux anonymes comme Tor, I2P ou Freenet. Le Dark Web peut ainsi être utilisé aussi bien à des fins légitimes (échapper à une répression politique) que pour dissimuler des activités illicites (commerce de produits issus du banditisme classique). Ces réseaux sont également utilisés pour échanger les données qui ont été dérobées au cours d'attaques informatiques : adresses e-mails, mots de passe, coordonnées personnelles ou bancaires ou encore courriels confidentiels.

ADRIEN PETIT

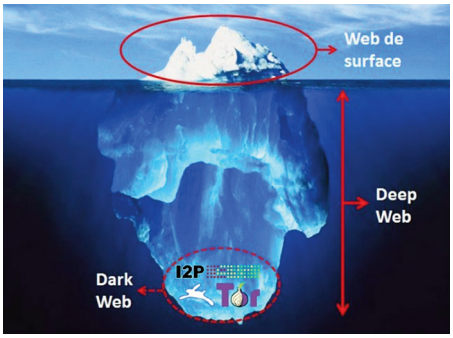
Consultant cybercriminalité Compagnie européenne d'intelligence stratégique (CEIS)

Si certains des mythes qui entourent le Dark Web sont justifiés, il convient dans un premier temps de revenir sur des notions souvent confondues.

Clear Web, Deep Web, Dark Web… ?

Afin de comprendre les différences entre le Clear, le Deep et le Dark Web, l'analogie de l'iceberg permet de délimiter précisément ces concepts ainsi que de schématiser la façon dont ils s'organisent :

Le Clear Web (ou le Web de surface) représente la partie émergée de l'iceberg (environ 5% du Web). Il comprend l'ensemble des contenus indexés par les moteurs de recherche classiques (Google, Yahoo, Bing). Le Clear Web contient notamment les blogs, les réseaux sociaux, les sites de diffusion, *etc.*



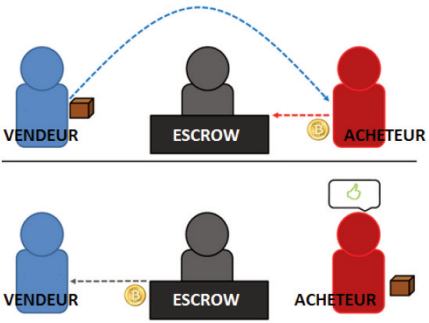
Le Deep Web (ou le Web profond/invisible) est la partie immergée de l'iceberg (environ 95% du Web). Il contient les contenus non-indexés que les moteurs de recherche ne parviennent pas à référencer. Il s'agit par exemple des bases et des banques de données, des bibliothèques en ligne ou encore des adresses IP.

Le Dark Web est quant à lui un sous-ensemble du Deep Web. Il regroupe les contenus non-indexés mais pour lesquels il est nécessaire de posséder des applications dédiées pour y accéder. Cet espace ne possède pas de panneaux d'indication (comme les moteurs de recherche classiques) permettant l'optimisation de la navigation de l'utilisateur. Cette carence est cependant compensée par le recours aux wikis (The Hidden Wiki de Tor étant le plus connu) qui recensent des centaines de liens (et leur descriptif) renvoyant vers des sites .onion.

De par sa facilité d'installation, sa simplicité et sa rapidité d'utilisation, Tor Browser est un des outils les plus utilisés pour accéder au Dark Web. Ce logiciel gratuit permet de naviguer et de communiquer de manière quasi-anonyme sur le réseau Tor. L'objectif initial de ce type d'outils est de protéger la vie privée et la liberté de ses utilisateurs. Il a permis notamment aux militants durant les printemps arabes, tout comme à d'autres dissidents politiques, de communiquer et de publier au sein de régimes répressifs. Tor et les autres réseaux anonymes ont cependant été détournés de leur usage premier au profit d'activités criminelles (plateformes de vente de produits illicites, réseaux pédopornographiques).

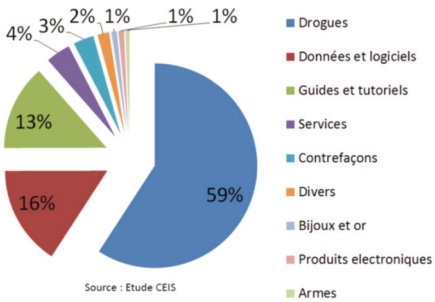
Black markets : nouvel Eldorado des cybercriminels

Un grand nombre d'activités criminelles sur le Dark Web s'organise au sein de black markets. Silk Road a été le pionnier de ce type de plateformes. Créé en 2011 et uniquement accessible via le réseau Tor, il était dédié au commerce des biens illégaux issus du banditisme classique tels que les stupéfiants, les armes ou encore les faux papiers. Sa spécificité était qu'il ne proposait pas directement la vente de ces biens. Le site reposait sur un système, appelé « escrow », de mise en relation entre acheteurs et vendeurs. L'« escrow », également appelé dépôt fiduciaire, est un système de paiement qui fait appel à une tierce personne neutre (dans le cas de Silk Road, le rôle était endossé par les administrateurs) qui se rémunère en prélevant une commission sur les transactions. Les activités du site



ont été plusieurs fois suspendues mais il n'a été définitivement fermé qu'en novembre 2014 suite à l'opération Onymous qui visait à arrêter des activités illicites de 400 sites. Selon le FBI, Silk Road aurait généré en trois ans un trafic équivalent à 1.2 milliards de dollars de vente et 80 millions de dollars de commissions empochés par les administrateurs du site.

Depuis la chute de Silk Road, entre 80 et 90 black markets opèrent sur Tor et fonctionnent sur le même business model, mais seul une vingtaine d'entre eux génère assez de profits pour assurer une activité régulière. Agora, AlphaBay et



Nucleus sont les trois plus grosses plateformes du secteur. Ces sites proposent quotidiennement 65 000 annonces dont la majorité concerne les produits liés au banditisme classique : environ 60 % des annonces publiées sur ces trois plateformes concernent le trafic de drogues. Les échanges effectués sur ces black markets témoignent aussi de la montée rapide en compétences des pirates informatiques : les produits digitaux (logiciels, malwares) et leurs guides d'utilisation associés permettent au premier venu d'acquérir un certain niveau de connaissances et de revendre le fruit de ses activités illégales (données volées) sur ces mêmes black markets. Ce phénomène représente environ 30 % de l'activité des trois principales plateformes.

En parallèle de l'hégémonie des black markets généralistes, une nouvelle tendance émerge au sein du Dark Web : le développement de black markets spécialisés dans le commerce de produits à très haute valeur ajoutée de type 0day ou nouveau malware, comme le témoigne l'apparition en avril 2015 du black market TRD[1]. Ce dernier propose toute une série de produits : exploits 0day[2] (vendu entre 500 et 40 000 USD), exploits FUD (indétectables par les antivirus, environ 500 USD), exploits 1day private (le code source n'a jamais été

(1) https://www.deepdotweb.com/2015/04/08/therealdeal-dark-net-market-for-code-0days-exploits/

(2) Une vulnérabilité jour zéro n'a fait l'objet d'aucune publication ou n'a aucun correctif connu. L'exploit est une technique exploitant cette faille.

partagé, entre 1 300 et 87 000 USD). Ce type de produits s'échange traditionnellement de manière directe et physique entre deux individus pour des raisons de confiance. Dans le cas présent, l'administrateur de TRD assure un rôle d'intermédiaire (système d'escrow) entre le développeur des exploits et un panel d'acheteurs anonymes. Les enchères permettent de faire monter la valeur du produit et ainsi de tirer un bénéfice plus important lors de la vente du produit.

Les forums restrictifs : point névralgique des échanges entre pirates

Les forums restrictifs possèdent la particularité d'imposer des barrières au moment où le visiteur souhaite créer un compte sur la plateforme. L'objectif de ces barrières est de restreindre l'accès au forum à une certaine communauté préalablement sélectionnée. Ces limites se traduisent notamment par la cooptation par un utilisateur déjà membre qui se porte garant de la légitimité du nouvel inscrit, ou encore la mise à l'épreuve du candidat via un acte de piratage sur une cible préalablement identifiée. Certaines plateformes couplent aussi le paiement d'un droit d'entrée élevé et ces barrières sélectives : le but est de décourager le premier venu possédant certaines compétences ou ressources mais qui ne souhaite pas s'investir pleinement dans les activités de la communauté.

Ces forums restrictifs possèdent une double fonction. Il s'agit dans un premier temps de plateformes de communication qui s'articulent autour de grandes catégories : techniques de piratage, retours d'expérience sur des logiciels et annonces de services. Ils remplissent également une fonction commerciale : l'échange entre membres de données volées suite à des actes de piratage ou bien d'outils destinés à perpétrer ces exploits malveillants.

Hell est un forum qui a acquis une grande notoriété auprès de la communauté underground en février 2015 lorsque ROR[RG], un de ses membres, a proposé gratuitement sur la plateforme plusieurs fichiers composés de données personnelles de près de quatre millions de personnes (coordonnées personnelles et bancaires des victimes). Elles ont été obtenues suite au piratage du site de rencontre Adult Friend Finder, qui possède près de 60 millions de membres.

La maîtrise des risques liés aux fuites de données par la Cyber Threat Intelligence

Il existe donc un marché conséquent , au sein du Dark Web, du recel des données volées. Les forums et les black markets sont des places de marchés priviligiées par les cyber-criminels. Certains ont développé des « shops » automatiques afin de vendre les données volées : il n'y a plus d'annonces, à la manière des plateformes classiques d'e-commerce, l'acheteur filtre ses choix en remplissant

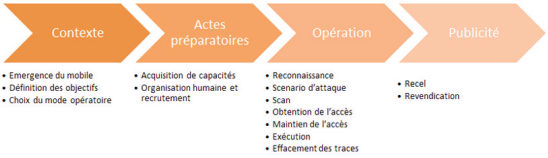
un ensemble de champs permettant d'affiner sa recherche. Les résultats obtenus permettent de finaliser et de livrer automatiquement l'achat dématérialisé. La principale plateforme du Dark Web propose quotidiennement 6 000 données volées uniques (numéros de cartes bleues ou comptes personnels comme eBay, Paypal, Amazon, Netflix, *etc.*).

Il apparaît donc essentiel de surveiller l'ensemble de ces plateformes afin de limiter au maximum les risques (intrusion informatique, spear-phishing[3]) liés au commerce de ce type de produits. Cette surveillance permet également d'identifier les groupes d'attaquants et leurs méthodes, et par conséquent de mettre en place des contre-mesures afin de limiter le vol de données.

(3) Le spear phishing est un message électronique qui semble émaner d'une personne ou d'une entreprise connue mais qui est issu d'un cybercriminel qui tente l'obtention de numéros de carte de crédit et de compte bancaire, de mots de passe et d'informations financières présentes sur un support.

La phase opérationnelle d'une cyber-attaque se découpe en 7 étapes majeures : la reconnaissance, le scénario d'attaque, le scan, l'obtention de l'accès, le maintien de l'accès, l'exécution et enfin l'effacement des traces. Se focaliser uniquement sur cette phase opérationnelle ne permet pas de couvrir l'ensemble de la chaîne opératoire d'un cyber-attaquant. Il est impératif d'observer également les événements situés en amont et en aval de l'opération aussi bien sur le Clear et le Deep web afin d'obtenir une vision globale des cyber-menaces potentielles. Cette approche de type Cyber Threat Intelligence se matérialise par le schéma suivant :

Le choix du lancement d'une attaque se construit tout d'abord autour d'un contexte : ce dernier s'explique par



l'émergence d'un ou plusieurs mobiles ainsi que des objectifs qui déterminent le choix du mode opératoire de l'attaque. Par la suite, il existe la phase de préparation pendant laquelle le cyber-attaquant acquiert des capacités (achats de malwares, exploits, *etc.*), et procède si nécessaire au recrutement de ressources. Ce n'est qu'une fois ces deux phases achevées qu'a lieu l'opération. Enfin, la dernière étape se traduit par la publicité de l'opération au travers de la revendication en cas d'un acte de type « hacktivisme » ou le recel des données volées si l'attaquant recherche le profit.

Au cours de ces trois étapes qui précèdent l'opération et lui succèdent, les cyber-attaquants interagissent par alternance sur le Clear Web et le Deep Web. Il est nécessaire de surveiller ces deux espaces afin d'anticiper une cyber-attaque ou pour limiter les dégâts causés par celle-ci. L'infiltration dans certains forums d'hacktivistes permet d'identifier des sujets de contestation, des motifs ou

des consignes annonçant une attaque. Surveiller les black markets et les forums restrictifs sur le Dark Web permet de dégager les tendances des produits recherchés par les cybercriminels ou encore d'observer l'acquisition de matériels et techniques pour mieux s'en prémunir. La publicité d'une attaque se fait majoritairement sur le Clear Web et en particulier les réseaux sociaux classiques (Twitter, Facebook). Il est essentiel de poursuivre la surveillance du Deep Web après l'attaque. En effet, suite à une intrusion, il est fréquent qu'un cyber-attaquant propose sur les black markets et les forums les données qui ont été dérobées. Il peut s'agir d'adresses mails, de mots de passe, de numéros de cartes bancaires ou encore de courriels confidentiels.

Surveiller le Deep Web reste cependant une activité complexe. S'il est possible de mettre en place une veille automatique sur les différentes plateformes présentes sur le Clear Web comme les réseaux sociaux, cette approche se révèle insuffisante pour le Deep Web et plus particulièrement pour le Dark Web. L'acquisition d'éléments à haute valeur ajoutée (exploit 0day, nouveau malware) requiert impérativement une approche humaine en raison de l'obligation d'interactions avec les différents acteurs présents sur les forums ou les black markets. Dans ce cas de figure, un simple outil d'indexation et de crawling s'avère inefficace.

Ainsi, le Dark Web est un espace largement utilisé à des fins illégales en raison de l'anonymat qu'il offre à ses utilisateurs. Ses différentes plateformes de commerce et de communication – black markets et forums restrictifs – représentent une importante source d'information en termes d'anticipation de cyber-menaces. Une surveillance efficace de cet espace exige une approche humaine à la fois pluridisciplinaire et multilingue. L'automatisation de la collecte d'informations est quant à elle indispensable sur le Clear Web, les outils sur étagère étant optimisés pour ce genre de tâches, notamment sur les réseaux sociaux. Ces processus de surveillance doivent être appliqués en fonction des différentes étapes d'une cyber-attaque qui sont déterminées par une approche de type Cyber Threat Intelligence[4].

(4) La collection, la classification et la valorisation des connaissances relatives à des adversaires.

L'AUTEUR

Adrien PETIT, consultant en cybercriminalité, a rejoint CEIS en janvier 2015 après une expérience de 4 ans au sein du CERT-LEXSI basé à Singapour où il a exercé le métier d'analyste et chef de projet cybercrime auprès de clients internationaux bancaires et industriels

Les nouvelles problématiques de sécurité des données numériques

par JAUFFREY COLEUR

L'explosion de la production de données numériques, les nouvelles façons de stocker et gérer ces données ainsi que la croissance des échanges amènent à repenser les problématiques de sécurité des données numériques.

La production de données numériques au sein des organisations ne cesse de croître. En complément des bases de données traditionnelles, de nouvelles manières de gérer ce flot de données sont apparues ces dernières années comme data warehouse et big data. Parallèlement, les flux d'échanges de données numériques augmentent de manière exponentielle et les acteurs qui manipulent ces données sont de plus en plus nombreux. Nous sommes passés d'une époque où les données étaient stockées dans une pièce de l'organisation et accessibles par la seule équipe informatique à un hébergement en mode « cloud » où il peut être difficile de connaître l'emplacement physique des données. Ces nouveaux enjeux amènent à repenser la façon dont les problèmes de sécurité sont intégrés. Ainsi, nous examinerons dans un premier temps la manière d'accéder aux données. Dans un second temps, nous nous interrogerons sur la sensibilité des données. Enfin nous examinerons la problématique des mutations et des échanges de données.

JAUFFREY COLEUR
Ingénieur en génie informatique
Mastère spécialisé de la conduite des opérations et de la gestion des crises en cyberdéfense

Traiter les données : une technologie en constante évolution

A la fin des années 90, la majorité des logiciels informatiques manipulant des données en entreprise stockaient ces données sur des serveurs de bases de données. Des clients lourds installés sur chaque poste client accédaient à ces données via le client de base de données. Ce client identifiait l'utilisateur et les autorisations d'accès étaient stockées au plus près de la donnée. Un

La confiance repose sur une accessibilité tracée des données et une classification pragmatique selon les niveaux d'utilisateurs.

travail non négligeable de l'administrateur de base de données consistait à gérer ces autorisations avec la possibilité de définir assez finement les autorisations. Par exemple, il était possible d'autoriser un utilisateur à accéder à une série d'enregistrements mais pas à la consolider avec une autre.

Peu à peu, au cours des années 2000, le client lourd est passé de mode au profit du client léger : une application web en accès depuis le poste client par un navigateur facilitant ainsi le déploiement et les mises à jour. Ce n'est alors plus le client qui accède à la base de données mais le serveur web. Les autorisations d'accès ne sont plus gérées au sein de la base de données mais du serveur web. Ce dernier devient le seul client de la base de données. Parallèlement est né le « cloud », soit le fait d'héberger certaines applications chez un prestataire de service.

Une simple problématique de confiance ?

Les autorisations d'accès possèdent deux faces : une visible et une cachée. La première est celle de la logique applicative. Dans notre exemple les autorisations d'accès seront gérées sur le serveur web. Des traces applicatives pourront nous permettre de savoir qui s'est connecté, à quelle heure, pour consulter quoi : le triptyque « *Qui ? Quand ? Quoi ?*». Cela reste valable tant que l'on accède aux données via le site

web, la face visible. Tout ce qui se trouve derrière ce serveur constitue une bulle qui doit être hermétique si l'on veut pouvoir tracer qui accède à nos données, une bulle de confiance en quelque sorte.

Une face cachée ?

En s'abstrayant des problématiques techniques, la confiance dans un système repose sur celle que l'on aura pour les acteurs constituant la bulle de confiance. Si nous reprenons l'exemple du serveur Web, ses administrateurs pourraient avoir accès à toutes les données de l'application. En effet, les logins et mots de passe sont généralement stockés en clair sur le serveur web afin que celui-ci puisse se connecter à la base. Ainsi, un administrateur web pourra outrepasser tous les mécanismes d'authentification et de cloisonnement mis en place dans l'application car il sera impossible de distinguer qui du serveur ou de l'administrateur s'est connecté à la base de données.

Maintenant, focalisons-nous sur la base de données. Les administrateurs de la base possèdent tous les droits d'accès mais ces derniers sont généralement tracés, ou du moins, il existe une possibilité de les tracer. Par contre l'administrateur du serveur qui héberge la base de données possède un accès direct et brut aux données. Il a, en effet, accès aux fichiers représentant la base de données. Ainsi, il peut dupliquer ces fichiers et les installer sur un serveur non tracé, échappant de cette façon, aux mécanismes d'authentification et de traces. La même logique s'applique à l'hébergeur physique des serveurs. Ce dernier a accès aux disques durs contenant les données. Les mécanismes de tolérance de panne supportent généralement l'échange en fonctionnement d'un disque dur. Il est ainsi possible d'échanger un à un l'ensemble des disques durs d'un serveur de base de données sans interruption de service afin de les dupliquer. Cette logique s'applique partout où est stockée la donnée : les bandes de sauvegarde, les baies réseaux de stockage sont d'autres exemples où les problématiques de contrôle d'accès ne sont généralement pas bien prises en compte.

Prenons l'exemple d'une société faisant appel à une société de services informatiques Soc1 pour implémenter sa gestion comptable. Soc1 va le faire via un progiciel de gestion développé par Soc2. Afin de faciliter le déploiement et le maintien en condition du progiciel, Soc1 propose d'utiliser la version cloud du progiciel développé par Soc2. Soc2 pour héberger son cloud fait appel à la société Soc3, spécialisée dans la gestion des applications web. Soc3 se concentre sur son cœur de métier et délègue l'hébergement physique de ses serveurs à la société Soc4. Soc3 possède aussi un contrat de sous-traitance pour gérer ses sauvegardes avec Soc5. Enfin Soc4

possède un contrat de sous-traitance pour recycler ses déchets électroniques (les disques durs en panne) avec Soc6.

Dans ces conditions, comment garantir que seul le bureau comptabilité aura accès aux données financières de l'entreprise ? A l'échelle d'une organisation qui garde la maîtrise d'œuvre informatique en interne, les mêmes questions se posent en remplaçant les différentes sociétés par les différentes équipes d'administration. Quel est le niveau de confiance mis sur le technicien en maintenance manipulant au quotidien les sauvegardes ?

Des données à classer

S'il est important de s'interroger sur la manière dont les acteurs manipulent les données, il faut aussi s'interroger sur la sensibilité des données. Afin de mettre en œuvre des moyens adéquats de protection sur les données, il faut pouvoir discriminer ces données en fonction de leur sensibilité. Il s'agit alors de trouver une méthode de classification ad hoc. Généralement, cette classification reposera sur le risque encouru pour une donnée de sortir du cercle de confiance délimité.

Si nous reprenons le cas de notre société précédente, les données comptables n'auront certainement pas la même sensibilité que l'annuaire téléphonique interne. Dans certains cas, des facteurs extérieurs – normatifs, réglementaires – peuvent venir imposer des classifications particulières. Par exemple, les données médicales devront avoir un traitement particulier ne dépendant pas de la seule volonté de l'organisation. Mettre en place une classification des données est une procédure complexe qui impose des choix structurants pour l'organisation.

Une fois que chaque donnée est rangée dans la bonne case, de nouvelles problématiques émergent.

Des données en mutation

L'agrégation est une problématique complexe à gérer. Un document pris individuellement peut avoir une sensibilité faible. Prenons, par exemple, le service achat d'une entreprise agro-alimentaire qui achète des matières premières auprès de différentes sociétés et interrogeons-nous sur la sensibilité des factures. A priori, une facture sortie de son contexte ne risque pas de mettre en danger l'entreprise (sauf accords commerciaux particuliers), même si généralement, une facture n'aura pas une sensibilité nulle. Si nous considérons l'ensemble des factures de matières premières, il pourrait être possible d'en déduire les quantités consommées pour concevoir certains produits et ainsi révéler un secret industriel (une recette dans notre cas). Dans ce cas, cette donnée mériterait certainement d'être classifiée au plus haut niveau de sensibilité.

A contrario, la sur-classification des

données à un niveau élevé pose des problématiques de liberté de circulation de l'information. Dans un contexte croissant d'échange, il est de plus en plus difficile de cloisonner la donnée à un espace restreint d'utilisateurs, non pas pour des problématiques techniques, mais pour des problématiques d'analyse et de développement de l'organisation. L'ensemble des données est agrégé par différents services, sous différents prismes, afin d'en déduire des axes stratégiques ou d'amélioration pour l'organisation. Si nous reprenons notre exemple de factures pour notre société agro-alimentaire, il est probable que les chiffres des factures sortiront du seul bureau comptable afin d'être analysés. Dans ce cas, il est imaginable de n'utiliser qu'une partie de l'information car la quantité de matière première pourra ne pas intéresser le service d'audit financier par exemple. La problématique sera d'obtenir le bon niveau de granularité de la donnée. A trop grosse maille, le risque est de limiter la circulation de l'information, à trop petite maille, le risque est de complexifier de manière artificielle la gestion de données.

Des données en transit

Les flux d'échanges de données numériques ne cessent de croître. Face à des organisations qui ont chacune leur propre système de classification de la sensibilité de la donnée, il est difficile de connaître les garanties de confidentialité qui seront apportées à une donnée échangée entre deux organisations. Étant donné qu'il n'existe pas de système technique universel de classification de la donnée, les garanties reposeront sur la confiance entre les deux organisations à traiter la donnée confiée avec un système de niveau de sensibilité équivalent. Ce qui nous amène à deux problématiques différentes : l'équivalence des méthodes utilisées pour qualifier la donnée et deux niveaux de classification différents dans deux organisations différentes. Faire confiance au système de classification de l'autre n'est pas une chose aisée car il subsiste une interrogation sur le niveau de maturité technique et organisationnelle de l'autre entité impliquée dans l'échange. Prenons un échange de données classifiées « SECRET INDUSTRIEL » entre une entreprise du CAC 40 et une PME. Les deux sociétés auront certainement des mesures de protection très différentes pour un même niveau de classification.

Quels enjeux pour la Défense ?

L'État s'est doté de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale ainsi que de l'instruction ministérielle n° 920 relative aux systèmes d'information traitant des informations classifiées de défense de niveau confidentiel défense. Ces deux documents posent les problématiques de classification et de protection des données numériques classifiées de défense. Notamment, elles

posent des limites strictes à l'interconnexion des systèmes et l'échange de données en précisant deux cas de figure : l'utilisation d'une passerelle agréée garantissant que seules des informations du bon niveau de classification soient échangées et l'usage d'une passerelle unidirectionnelle du niveau le plus faible vers le niveau le plus élevé de classification.

Or, face à la complexité de la tâche, il n'existe pas encore de passerelle agréée permettant d'échanger des données classifiées de défense. Seul le deuxième cas de figure est utilisable, ce qui limite *de facto* les possibilités d'échange. Dès lors, face au besoin croissant d'échange, les organismes traitant des données classifiées de défense pourront-ils se permettre d'attendre une solution technique permettant d'échanger, ou bien, une révision normative sera-t-elle nécessaire ?

Peer-to-peer dans le monde du pier-to-pier(1) ?

par BARNABÉ WATIN-AUGOUARD

(1) « Pier-to-Pier » : de quai à quai.

Le cyber et la mer… Rien ne semble *a priori* rapprocher ces deux mondes. Certes, on qualifie souvent ces entités *de res communis* ou *res nullius* sur lesquelles on « navigue » en toute liberté en évitant les pirates et le *phishing*… ou le *fishing* ! Le cyberespace et la mer sont cependant désormais étroitement liés. Moteurs de la croissance de demain - il suffit de regarder les efforts consentis par la Chine et les États-Unis dans ces deux domaines pour s'en convaincre. La rencontre de ces deux mondes est en effet le nouveau défi auquel sont confrontés les marins. Si la prise de conscience des menaces cyber liées à la mer est récente, la question de la protection des données en mer a toujours été un enjeu majeur bien que parfois dépassée par la numérisation galopante de l'économie maritime.

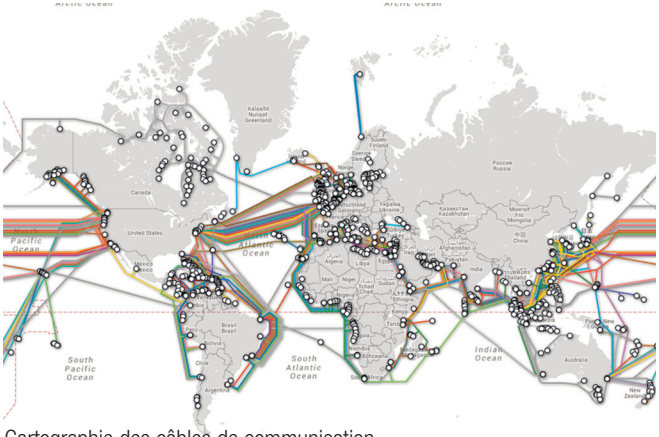
BARNABÉ WATIN-AUGOUARD

Chargé de mission Secrétariat général de la me

20 000 Tbps sous les mers

Le monde maritime n'a pas attendu la révolution numérique pour s'intéresser à la protection physique des données. En effet, avec plus de 260 câbles sous-marins supportant des débits supérieurs à 5 Gbps, 99 % des communications de données et de téléphonie intercontinentales passent désormais par le fond des océans en s'affranchissant du trajet aller-retour vers un satellite, coûteux en temps. L'installation d'un câble reliant New-York à Londres est d'ailleurs en cours avec une bande passante prévue de 52 Tbps !

Dans ce contexte, la protection du contenu passe avant tout par la protection du contenant et revêt un caractère stratégique pour les années à venir. Si des dispositions sont prises



Cartographie des câbles de communication (TeleGeography et www.submarinecablemap.com)

pour éviter toute destruction involontaire à proximité des côtes, en réglementant le chalutage ou le mouillage par exemple, des actes de malveillance ne sont pas à exclure. La redondance, notamment transatlantique, peut pallier cette difficulté, mais certains pays ne sont raccordés que par un unique câble. En haute mer, les câbles reposent par plusieurs centaines de mètres de fond, excluant ainsi toute dégradation, du moins non-intentionnelle.

Port sniffing

Points nodaux multimodaux recevant 90 % du commerce international en volume, les ports constituent par ailleurs le maillon central du transport de marchandises. Une cyberattaque majeure sur un grand port serait par conséquent susceptible de désorganiser massivement toute la chaîne d'approvisionnement et donc l'économie d'un pays. La problématique n'est toutefois pas proprement maritime. En effet, les menaces cyber pesant sur les ports sont les mêmes que celles pouvant atteindre un pôle logistique « terrestre ».

Les systèmes d'information des administrations de l'État bénéficient d'attentions et d'exigences spécifiques. Ceux des acteurs privés, notamment les opérateurs d'importance vitale, peuvent cependant présenter des vulnérabilités qu'il peut être plus difficile de corriger. Si l'interconnexion des systèmes d'information, renforcée par la mise en place d'un guichet unique portuaire[2], apporte une réelle souplesse administrative, une vigilance toute particulière doit être apportée à la sécurisation de ces réseaux déployés sur une grande étendue géographique et mêlant parfois la gestion des droits d'accès… à l'accès internet par Wifi des marins en escale !

(2) Centralisation des déclarations d'escale, de la cargaison, des listes d'équipage et de passagers, du manifeste des matières dangereuses…

La protection des données logistiques ou à caractère économique et commercial est également primordiale. On ne citera, pour mémoire, que l'exemple du port d'Anvers, victime de 2011 à 2013 d'une cyberinfiltration par un cartel de narcotrafiquants leur permettant de récupérer des conteneurs remplis de

(3) http://www.lalibre.be/economie/actualite/comment-anvers-a-ete-pirate-et-s-en-est-sorti-5269e7ea35708def0d93513c

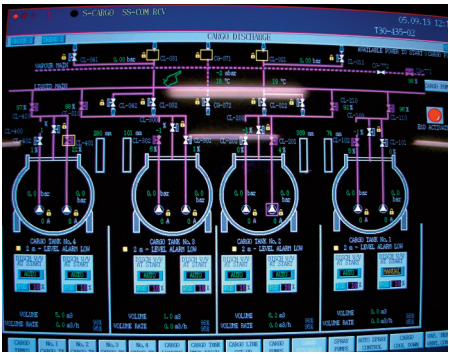
stupéfiants sans éveiller les soupçons des autorités douanières[3].

Piège en haute mer

Les systèmes d'information et les réseaux informatiques ont également progressivement envahi les navires. Les enjeux de cybersécurité n'avaient, jusqu'à présent, que faiblement été pris en compte. L'ENISA[4] a ainsi souligné, en 2011, dans un rapport sur la cybersécurité maritime, que « *la sensibilité à la problématique varie de faible à inexistante* ». Plus récemment, le « *Livre bleu* », publié en 2013 par le « *Cluster marétique*[5] » et traitant de l'apport des nouvelles technologies numériques au secteur, fait totalement l'impasse sur la sécurité des systèmes d'information. La prise de conscience vis-à-vis des cybermenaces est toutefois en train d'émerger.

(4) « European Network and Information Security Agency » - agence européenne chargée de la sécurité des réseaux et de l'information.

(5) Ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations maritimes et fluviales.



SCADA d'un méthanier (marine-marchande.net)

Parmi les éléments les plus sensibles figure l'informatique embarquée, constituée des systèmes industriels et des automates omniprésents sur les navires. Si ces systèmes présentent des vulnérabilités intrinsèques souvent connues[6], le risque s'est cependant fortement accru notamment au travers de la maintenance en mer, réalisée de plus en plus souvent à distance, ou encore de l'utilisation croissante de systèmes informatiques « *sur étagère* » et largement interconnectés pour permettre un échange en temps réel des données. Si, pour l'heure, la prise de contrôle à distance d'un navire peut sembler hypothétique et relever de la filmographie bondesque, un logiciel malveillant implanté à l'occasion d'une opération de maintenance à quai, volontairement ou non, peut avoir des conséquences désastreuses : d'un *ransonware* immobilisant un navire en haute mer jusqu'à une bombe logique neutralisant l'appareil à gouverner lors des phases portuaires critiques.

(6) Certains SCADA utilisent encore Windows 95 tandis que certains navires sont dotés du système WinCC de Siemens, cible du virus Stuxnet.

Du sextant au tout écran

D'autres fonctions essentielles aux navires n'ont pas échappé à la numérisation. En

effet, la modernisation des outils simplifie considérablement la pratique de la navigation pour un équipage de plus en plus réduit… du fait de l'automatisation grandissante ! La navigation et la sécurité nautique reposent désormais sur de multiples dispositifs[7] dont certains semblent particulièrement vulnérables : citons par exemple l'ECDIS[8] qui peut présenter des vulnérabilités ou encore le GPS que des étudiants américains ont réussi à leurrer sur un navire en 2013 sans qu'aucune anomalie ne soit détectée.

(7) Météorologie, informations nautiques, phonie et échanges de données, détresse, alerte de sûreté (SSAS : Ship Security Alert System).

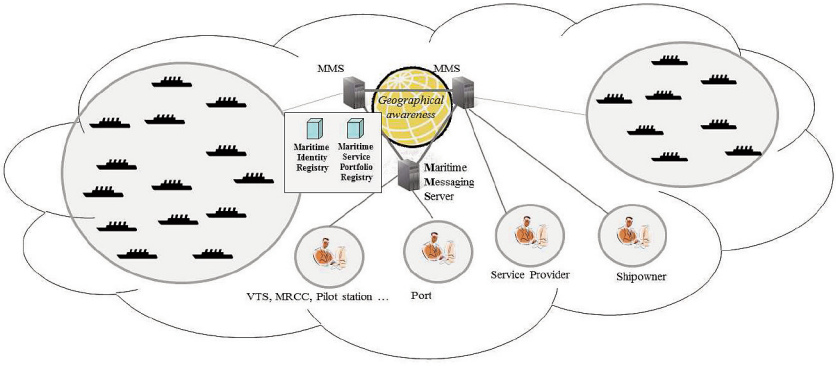
(8) « Electronic Charts Display Information System » (ECDIS) autrement dit de la cartographie électronique.

L'Organisation maritime internationale a adopté, par ailleurs, en 2014 la stratégie de l'e-navigation : « *collecte, intégration, échange, présentation et analyse harmonisés d'informations maritimes à bord et à terre par voie électronique dans le but d'améliorer la navigation quai à quai et les services connexes, la sécurité et la sûreté en mer et la protection du milieu marin* ».

Cette stratégie s'appuie sur la mise en place d'un cloud maritime permettant, de manière « *efficace, sûre, fiable et transparente* », les échanges électroniques d'informations entre tous les acteurs maritimes agréés.

L'âge du capitaine

C'est bien un des rares éléments qui ne soit pas facilement accessible. En effet, beaucoup d'informations, pourtant sensibles, sont disponibles en source ouverte. Si l'exploitation de certains systèmes de transmission d'informations est « réservée » aux administrations comme le *Vessel Monitoring System* (VMS) des pêcheurs ou le *Long-Range Identification and Tracking* (LRIT), d'autres, comme l'*Automatic Identification System* (AIS), sont accessibles au grand public.



À l'origine, l'AIS permet l'échange automatisé de messages[9] entre navires par radio VHF. Il s'agit alors d'un système d'anticollision, équivalent du TCAS des aéronefs. Puis, l'utilisation du système s'est progressivement étendue aux centres de surveillance du trafic maritime puis aux ports et aux armateurs pour, finalement, être consultable par

(9) Identité du navire, route, vitesse, position mais également type de cargaison, destination, heure prévue d'arrivée, nombre de passagers…

(10) Exemple : http://www.marinetraffic.com/fr/

AIS dans le détroit du Pas-de-Calais (marine-traffic.com)

quiconque sur internet - gratuitement pour la plupart des informations[10]. Moyennant un abonnement mensuel, on accède à l'ensemble des services dont l'AIS satellitaire qui élargit considérablement la couverture.

(11) Cf. http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais

La faiblesse des protocoles utilisés[11] rend ce système vulnérable à plusieurs titres. Il est en effet facile de modifier les données émises par un navire - notamment la position en faisant du GPS spoofing – ou de se faire passer pour un autre : en 2013, un pétrolier en provenance du Pakistan modifie son AIS et se fait passer pour un chimiquier pour contourner l'embargo américain envers l'Iran. En outre, les informations transmises facilitent le ciblage ou l'approche discrète comme cela a déjà été fait par certains groupes de pirates.

Abandonner le navire ?

Le tableau dépeint peut sembler catastrophiste tant les failles semblent nombreuses. Toutefois, la prise de conscience des enjeux par les acteurs du monde maritime donne une occasion unique d'anticiper ces menaces. Pour les navires, et les normes associées, le niveau international est le plus pertinent. L'OMI s'est d'ailleurs saisie des questions de cybersécurité, inscrites à l'ordre du jour des sessions du comité de la sécurité maritime en 2016. Pour sa part, l'Union européenne aborde ces menaces dans sa récente stratégie de sûreté maritime. Le niveau européen semble d'ailleurs le plus adapté pour la problématique portuaire.

Au niveau national, la loi de programmation militaire du 18 décembre 2013 constitue une première réponse à ces enjeux même si elle ne concerne qu'une partie des acteurs du secteur maritime. Un arrêté du Premier ministre viendra concrétiser ces dispositions d'ici fin 2015. L'ANSSI et la direction des

affaires maritimes mènent d'ailleurs une étude sur le domaine maritime listant les fonctions impliquées, les rares normes existantes et les vulnérabilités potentielles. Couvrant l'ensemble du spectre, cette étude permettra d'établir une cartographie des risques, de définir des priorités et d'orienter la veille.

Il ne faut évidemment pas exclure les principaux acteurs de la réflexion : les armateurs, les équipages, les industriels, les assureurs… Il s'agit de trouver ensemble un compromis entre sécurité des systèmes, viabilité économique et défense de nos intérêts. À cet égard, lors du comité interministériel de la mer du 22 octobre 2015, le Premier ministre a annoncé la création d'un groupe de travail copiloté par l'ANSSI, le SGDSN et le SG Mer associant l'ensemble des administrations de la fonction garde-côtes, les ministères concernés et les principaux acteurs du secteur maritime afin d'approfondir la réflexion nationale sur le sujet, notamment en termes de résilience.

Si dans le domaine des attaques cyber, tout semble possible, il faut se concentrer dans un premier temps sur le « probable » pour construire progressivement une défense pragmatique et efficace en s'orientant vers le secured by design. N'oublions pas, enfin, que l'humain est souvent au cœur de la problématique cyber. Il convient donc de favoriser la « *cyberhygiène* ». Mais ne soyons toutefois pas complètement négatifs ; c'est souvent l'humain qui permet de détecter les anomalies et d'assurer la résilience en fonctionnant en mode dégradé : suivant la situation, on appellera cela « *le sens marin* » ou « *le flair du gendarme* » !

L'AUTEUR

Chargé de mission auprès du Secrétaire Général de la Mer depuis sa sortie de l'école de guerre en 2012, le lieutenant-colonel Barnabé Watin-Augouard, ancien élève de l'école navale, a rejoint la Gendarmerie en 2004 après huit années passées dans la Marine nationale. Son portefeuille actuel comprend l'ensemble des questions relatives à la sûreté maritime : ordre public, terrorisme, piraterie, prolifération, sûreté maritime et portuaire, planification de sécurité nationale, immigration… Il est notamment chargé, au sein du Secrétariat Général de la Mer, des travaux d'élaboration de la stratégie nationale de sûreté des espaces maritimes.

Le cyberespace, un espace stratégique qui doit être régulé

par HENRI D'AGRAIN

Le cyberespace a une histoire. Elle permet d'expliquer la polysémie du terme et de mettre en exergue des approches, parfois contradictoires, souvent antagonistes, entre les différents acteurs qui participent à sa construction. C'est cette histoire que nous tentons de présenter dans cet article.

Tarte à la crème de la « littérature » consacrée au numérique, celui-ci est partout et submerge tous les secteurs d'activité. Le monde d'avant l'informatique disparaît progressivement. Ma génération – celle des cinquantenaires – est la dernière à avoir connu un monde, et à en conserver la mémoire, où le seul écran était celui de la télévision, et le seul clavier celui de la machine à écrire. Quant à la souris, elle n'était que ce petit personnage sympathique de dessin animé. Il y a à peine trente ans, l'hypothèse même de l'atmosphère numérique, dans laquelle baignent désormais toutes nos activités, était impensable, sauf dans la littérature d'anticipation et les films de science-fiction. C'était il y a trente ans que paraissait Neuromancien, premier roman de science-fiction de William Gibson. C'est dans ce roman qu'apparaît pour la première fois le terme de cyberespace. Neuromancien est généralement considéré comme le roman fondateur du mouvement cyberpunk, l'ouvrage canonique de ce genre, premier d'une longue série d'œuvres telles que Matrix au cinéma.

HENRI D'AGRAIN
Directeur général du Centre des Hautes Etudes du Cyberespace (CHECy)

À l'origine du cyberespace

Dans ce roman, Gibson décrit un monde sordide, où la drogue est omniprésente, et qui est dominé par le capitalisme le

plus sauvage que gouvernent des multinationales sans pitié. Des pirates du cyberespace se connectent au réseau informatique, la matrice, *via* une prise neuronale pour disposer d'une perception sensorielle des données numériques qu'ils manipulent. William Gibson a le génial pressentiment de ce qui va devenir le fait marquant, dans le domaine des technologies, de la décennie suivante : Internet. Dans ce roman, il fait véritablement œuvre d'anticipation, en imaginant un futur où la technologie, au développement hypertrophique, finit par envahir l'environnement humain, et par le remplacer. Il décrit un univers froid où l'informatique révèle son pouvoir de contrôle en renforçant celui des autorités, où les technologies numériques s'installent au cœur des organismes humains, au moyen de tout un arsenal de dispositifs électroniques. On retrouve dans cette description onirique et déprimante, du cyberespace les prémisses d'une certaine forme de la pensée transhumaniste sur l'homme augmenté.

Le rêve libertaire du cyberespace

Pourtant, et malgré la noirceur de la vision de Gibson, le terme « cyberespace » fait l'objet d'une rapide récupération pour faire référence, d'abord, à une vision très libertaire de l'espace numérique. Dans cette acception, celui-ci est d'abord compris comme un lieu d'échange et de partage qui doit demeurer vierge des velléités régulatrices des États. C'est ici que la figure de John Perry Barlow apparaît. Ce militant libertaire né aux Etats-Unis en 1947 crée l'Electronic Frontier Fondation en 1990. C'est une organisation non gouvernementale internationale à but non lucratif, dont l'objectif essentiel est de défendre la liberté d'expression sur Internet. Le 8 février 1996 à Davos en Suisse, Barlow rédige la Déclaration d'indépendance du cyberespace. Ce document est un vrai morceau de bravoure, un condensé de la pensée la plus cyberlibertaire. Il énonce le refus de l'appropriation d'Internet par un gouvernement extérieur, en particulier celui des États-Unis. Il affirme que les États n'ont pas eu le "consentement des gouvernés" pour appliquer leurs lois sur Internet, et que l'Internet est à l'extérieur des frontières de n'importe quel pays. Il précise qu'Internet se régule lui-même, avec ses propres codes et langages sociaux, basé sur l'éthique de réciprocité. L'introduction de ce texte illustre de manière très évocatrice la tonalité générale : « *Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur, je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté où nous nous rassemblons* ».

C'est grandiloquent, c'est assez comique comme ton, mais ça dit vraiment quelque chose de cette vision libertaire de l'Internet qui a prévalu dans les temps héroïques de la « *conquête du réseau* ». Cette acception libertaire du cyberespace existe toujours, mais ce sont aujourd'hui les grands opérateurs américains du numérique, notamment les GAFA, et jusqu'à l'administration américaine, qui se sont approprié cette vision en la détournant, de manière assez habile, à leur profit. En effet, ils revendiquent conjointement une gouvernance de l'Internet dans une logique dite multistakeholders ou « *multipartieprenantes* », indépendante des États, afin de s'affranchir d'une approche intergouvernementale ou, pire à leurs yeux, onusienne de cette gouvernance.

L'approche militaro-sécuritaire du cyberespace

C'est en réaction à cette vision libertaire du cyberespace que s'est construite, au cours des années 2000, une doctrine sécuritaire de ce qui est apparue comme un nouvel espace de confrontation et de conflictualité qu'il convenait donc, à l'inverse, de contrôler. Le cyberespace a été dès lors considéré comme un cinquième espace de bataille, après la terre, la mer, l'air et la stratosphère popularisée par la guerre des étoiles, où peuvent se déployer une force et une pensée stratégique. Le cyberespace,

CHECy
Centre des Hautes Etudes du
Cyberespace

Le Centre des Hautes Etudes du Cyberespace (CHECy) propose à des cadres et des dirigeants des secteurs publics et privés une formation innovante sur les enjeux de transformation numérique, la culture digitale et les méthodes de raisonnement de cyber-intelligence. Elle leur fournit les clés de compréhension de la révolution numérique, dans une approche pluridisciplinaire, afin de leur permettre de décider et d'agir dans leurs différents champs de responsabilité. Formation d'excellence unique en France, elle est adaptée à l'emploi du temps professionnel de cadres de haut niveau. Son programme de formation est conçu pour offrir aux auditeurs une vision à 360 degrés du cyberespace, hybridant les connaissances des différents champs disciplinaires ayant développé un discours sur le numérique. Le CHECy propose un parcours pédagogique et relationnel exceptionnel, qui se caractérise par la qualité des contenus et des intervenants, la diversité des points de vue et des profils, et l'originalité des méthodes pédagogiques mises en œuvre, au service du développement professionnel de chaque auditeur. Le CHECy offre également aux auditeurs les moyens de développer un réseau professionnel de qualité et d'intégrer la nouvelle communauté du CHECy organisée autour de ses activités de formation et de réflexion.

malgré les apparences, est perçu à ce titre comme un espace opaque où il est très difficile de dresser le lien entre une action malveillante et son auteur. Cette acception militaro-sécuritaire du cyberespace est très en vogue et a la faveur d'une foule nombreuse de dirigeants et décideurs, qu'ils soient occidentaux ou non. C'est sur la base de cette acception, qui correspond à une réalité concrète et qui se mesure de manière significative, que s'est développé en France, par exemple, un ensemble d'initiatives dont les plus emblématiques sont l'élaboration d'un corpus doctrinal national de cybersécurité, le renforcement de l'Agence nationale de la sécurité des systèmes d'information, l'ANSSI, la création du commandement de la cyberdéfense auprès du Chef d'état-major des armées, ou encore la création d'une fonction de préfet en charge de la lutte contre les cybermenaces auprès du Ministre de l'intérieur. Aussi nécessaires et justifiées soient-elles, toutes ces mesures particulièrement visibles, par leur pertinence et, espérons-le, par leur efficacité, donnent une vision particulièrement anxiogène de la transformation numérique. Or, et c'est là un paradoxe sur lequel il convient de s'interroger, et qu'il faudra résoudre pour le dépasser, la sécurité numérique est la condition sine qua non de la confiance sans laquelle il n'est pas de réelle croissance possible dans et par le numérique.

Les espaces stratégiques communs

Pour ce qui nous concerne, nous appréhendons le cyberespace comme l'un des cinq espaces stratégiques communs, espaces qui appellent une certaine forme de régulation internationale, mais qui doivent demeurer libres des appropriations des États ou d'intérêts privés.

Le concept d'espace stratégique commun remonte loin dans l'histoire de l'humanité. À partir du moment où les hommes ont vécu en sociétés organisées, ils ont été confrontés à des ressources dont l'emploi optimal au profit de la collectivité nécessitait des règles différentes de celles de la propriété privée ou de l'accès sans entrave. C'est ainsi que depuis des temps très anciens, et jusqu'à une date récente, les paysans de France exploitèrent collectivement ce que l'on nommait les prés communaux pour y faire paître leurs troupeaux. Ce thème du « commun » connaît un regain d'intérêt depuis une vingtaine d'années. Ainsi, Elinor Ostrom, professeure de sciences politiques aux Etats-Unis, a obtenu en 2009 le prix Nobel d'économie pour ses travaux portant sur la gestion collective des biens communs. Elle a montré comment de nombreuses collectivités, à travers la planète et l'histoire, ont su trouver les moyens d'une gestion économiquement optimale de leurs biens communs, notamment à travers

md3d-fotlia.com

Une régulation de ce nouvel espace stratégique dépend des intérêts d'acteurs aux motivations divergentes.

l'élaboration de ce qu'elle nomme des arrangements institutionnels. Les espaces stratégiques communs relèvent d'une catégorie un peu particulière des communs. Ce sont des espaces offrant des ressources qui doivent être gérées de manière optimale au profit de l'ensemble de l'humanité. Les auteurs qui se sont intéressés à la question s'accordent à ce jour pour en identifier cinq : l'espace extra-atmosphérique, l'espace aérien, l'espace maritime, l'espace fréquentiel et enfin le cyberespace. Ce dernier est d'une nature un peu différente des quatre premiers. D'abord, il n'est apparu dans cette catégorie que de manière très récente, à partir de la fin des années 90, et plus sûrement vers 2005. Ensuite, ce n'est pas un espace naturel. Il a été entièrement conçu par l'homme, par ses machines informatiques de différentes natures qu'il a interconnectées entre elles, qui continue de le faire croître de manière quasi-exponentielle. Enfin, c'est le seul de ces espaces stratégiques communs qui ne fasse pas l'objet d'une réelle régulation internationale.

Le cyberespace, un espace stratégique commun un peu particulier

Si les quatre premiers espaces stratégiques communs sont gérés par des institutions spécialisées des Nations Unies, le cyberespace ne l'est pas. De nombreux acteurs s'opposent fermement, parfois pour des raisons opposées, à l'émergence d'une autorité de régulation supranationale ayant la légitimité nécessaire pour faire émerger un droit international public du cyberespace. Dès 2003, pourtant, les Nations Unies ont ouvert la discussion dans le cadre des Sommets mondiaux sur la société de l'information, et par la création en 2005 du Forum sur la gouvernance d'Internet. Aujourd'hui, plusieurs enceintes internationales ou régionales, pérennes ou conjoncturelles, centrent leurs débats sur ce sujet, sans parvenir à dégager un consensus, dans un contexte de politisation croissante en raison de l'enjeu majeur que représente la question de la gouvernance du cyberespace.

Une absence caractéristique de vision commune du cyberespace

Pour simplifier à grands traits, trois tendances principales s'affrontent. Celle défendue par les États-Unis, qui entendent privilégier une approche multi-acteurs, essentiellement économique d'ailleurs, avec une influence réduite des États. Celle que prône la Chine, visant au contraire à faire des États, dans un cadre onusien, les acteurs exclusifs de la régulation du cyberespace. Enfin, celle défendue par le Brésil, mais aussi dans une moindre mesure par l'Union européenne, lesquels cherchent une voie médiane entre les deux positions précédentes. Chacune de ces postures est, bien entendu, sous-tendue par des considérations géopolitiques qui dépassent largement la question de la gouvernance mondiale du cyberespace. Le débat est engagé depuis plus de 10 ans. Il n'a guère progressé, si ce n'est, d'une part l'acceptation, du bout des lèvres, par les États-Unis de se défaire de la tutelle de l'ICANN[1] et d'autre part le creusement de fossés béants entre des positions apparemment irréconciliables.

(1) Société de droit californien à but non lucratif dont la principales mission est d'administrer les ressources numériques d'Internet, telles que l'adressage IP et les noms de domaines de premier niveau (TLD)

Vers une forme numérique de la tragédie des communs ?

Ces divergences profondes sur le statut de la régulation future du cyberespace pourraient entraîner la mort de cet Internet ouvert et libre, en partie fantasmé, que nous croyons connaître, et qui correspondait au rêve des pionniers du début des années 90. Il faut bien comprendre que l'Internet n'est que la partie émergée de l'iceberg numérique. Les palinodies des puissances se feront au détriment d'une multitude d'acteurs. On se retrouve dans une version moderne

de la « *tragédie des biens communs* ». Celle-ci décrit la compétition pour l'accès à une ressource commune, menant à un conflit entre différents intérêts individuels et l'intérêt collectif dont la conséquence rationnelle est un résultat perdant-perdant. Elle a été caractérisée par Garrett Hardin dans un article publié dans la revue Science en 1968. C'est d'ailleurs en partie sur la base des travaux de Hardin qu'Elinor Ostrom avait développé les siens.

D'une manière ou d'une autre, cette « *tragédie* » devra être surmontée, par les États d'abord, qui disposent seuls, dans le contexte actuel, de la légitimité pour faire émerger un droit protecteur des libertés démocratiques dans le cyberespace. Une convention internationale, suivant le modèle de celle de Montego Bay de 1982 qui a doté les espaces maritimes d'un statut robuste, serait probablement en mesure de jeter les bases d'un droit international public du cyberespace. Une telle démarche correspond à l'émergence de la pensée démocratique, que résument parfaitement les propos de Lacordaire : « *Entre le fort et le faible, entre le riche et le pauvre, c'est la liberté qui opprime et la loi qui affranchit* ». Concernant notre capacité à maîtriser notre avenir numérique, notre vie de citoyen du cyberespace, entre les puissances numériques, nous citerons pêle-mêle les GAFAM[2], la NSA, les nombreux États peu soucieux des libertés individuelles voire certaines autorités administratives de nos États démocratiques, et chacun de nous, il en est exactement de même : la liberté opprime et la loi affranchit.

(2) Google, Appel, Facebook, Amazon, Microsoft…

La noosphère

Pour aller plus loin, avec le cyberespace, et c'est une question que nous nous posons, ne sommes-nous pas en train d'assister, très concrètement, à la matérialisation de la noosphère ? La noosphère, ou sphère de la connaissance, est un concept introduit en 1922 par Pierre Teilhard de Chardin. Pour Teilhard de Chardin, l'histoire de la terre se déroule en trois phases. Au cours de la première phase s'est façonnée la lithosphère, la sphère des masses inertes. Sur celle-ci, s'est ensuite développée la biosphère, la sphère du vivant à laquelle, dans un ultime développement, appartient l'espèce humaine. La noosphère constituerait pour Teilhard de Chardin une troisième phase, en enveloppant les deux premières dans une sphère de la pensée. Comment appréhender la noosphère ? Il est significatif que la notice de wikipédia, consacrée à la noosphère de Teilhard de Chardin, se termine par une histoire de la construction du cyberespace.

Le terme de cyberespace est polysémique : espace de liberté pour les uns, espace de conflictualité pour les autres. Il peut être perçu comme un espace artificiel et anthropogène ou comme une sphère de la pensée. Nous retiendrons, pour notre part, la notion d'espace stratégique commun qui nous paraît la plus fertile et la plus positive. Elle correspond, en tous les cas, au projet que nous développons avec le Centre des Hautes Études du Cyberespace (CHECy).

L'AUTEUR

Henri d'Agrain a été directeur des systèmes d'information et autorité de cyberdéfense de la Marine. Il quitte la Marine en 2013. Il dirige une société de conseil, Small Business France, qui accompagne les PME innovantes vers la commande des grands comptes publics et privés. Il est également directeur général du Centre des Hautes Etudes du Cyberespace (CHECy). Il est membre, en tant que personnalité qualifiée, de la commission parlementaire en charge des questions numériques et postales, la Commission supérieure du service public des postes et des communications électroniques (CSSPPCE).

Les structures de données
fictives utilisées en ingénierie sociale

par **THIERRY BERTHIER** et **BRUNO TEBOUL**

Le cyberespace n'échappant pas encore à la nature humaine, les fausses données créées par l'usager malveillant font naturellement partie du tsunami numérique. Leur production s'accélère de manière systémique et provoque aujourd'hui de violentes turbulences dans un environnement hautement connecté, fragile et instable. L'article explore l'écosystème des fausses données en décrivant les mécanismes fonctionnels des principaux cas d'usage.

THIERRY BERTHIER

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

BRUNO TEBOUL

Directeur Scientifique, R&D et Innovation Groupe Keyrus,
Chaire Data Scientist de l'Ecole Polytechnique

En 2020, le volume mondial des données numériques produites par l'homme et ses machines atteindra les 44 zettaoctets (soit 44 000 milliards de Go). Cette production exponentielle augmente fortement avec le déferlement des objets connectés et engendre de nouveaux défis d'exploitation toujours plus complexes à relever. À l'image d'une ressource naturelle, la donnée numérique peut être de bonne ou de mauvaise qualité et ce sont bien ses qualités qui engendrent sa valeur. La véracité d'une donnée figure dans la liste des désormais classiques 6 V caractérisant le big data : Volume, Variété, Vélocité, Visibilité, Valeur et Véracité. Tout en restant très relative au contexte sur lequel on l'évalue, cette véracité conditionne l'ensemble de la chaîne de traitement informationnel tout comme les décisions qui en résultent.

Véracité de la donnée, approches logique et systémique

La véracité d'une donnée demeure relative au contexte et à l'instant d'évaluation. Dans la suite de l'article, une donnée numérique D désignera un ensemble fini de mots binaires. Ces mots sont écrits à l'aide des bits 0 et 1 et sont "interprétables" par les systèmes sur lesquels ils sont stockés. La véracité d'une donnée D s'évalue alors à un instant t sur un contexte C bien défini. Elle peut être formalisée par une fonction Véracité (D, t , C) qui renvoie 1 (oui) si la donnée est vraie à l'instant t sur le contexte C et 0 (non) si elle est fausse. Ainsi, la donnée (il est 7 heures à ma montre) est vraie deux fois dans la journée et fausse le reste du temps. De même, la donnée (la température extérieure est supérieure à 40 degrés) peut être vraie dans une ville et fausse dans un autre lieu à un instant précis. Lorsque l'on cherche à évaluer la véracité d'une donnée, il est important d'en connaître l'émetteur. La question "Qui a créé cette donnée ?" renseigne souvent sur sa véracité. Lorsque l'origine d'une donnée est parfaitement connue et qu'elle n'a pas été modifiée depuis sa création, il devient possible de la certifier à l'instant t sur un contexte fixé. Mais bien souvent, l'observateur ne dispose pas d'information sur l'origine de cette donnée. Il doit donc faire le pari que l'émetteur est "légitime" et que la donnée n'a pas été modifiée par un hacker. Les métadonnées qui accompagnent la transmission d'une donnée fournissent de l'information utile à l'évaluation de sa véracité. Pourtant, en tant que données numériques, elles peuvent elles-mêmes subir des transformations ou des détournements dans le cadre d'une attaque informatique et perdre ainsi toute véracité. Ainsi, un simple tweet de 140 caractères s'accompagne de 31 métadonnées qui représentent plus de 90 % de l'information transmise... Le *ratio* "volume d'une donnée sur le volume de ses métadonnées" montre que l'information systémique (c'est-à-dire créée par les systèmes qui accompagnent une donnée d'origine humaine) est en forte croissance. L'internet des objets accélère d'ailleurs cette tendance avec une prévision de production de données issues des objets connectés s'élevant à 27 % du volume mondial en 2020. Qu'elle soit directement produite par l'homme ou d'origine systémique, la donnée peut subir des modifications malveillantes qui la transforment alors en fausse donnée ou en donnée fictive. Construite de toutes pièces et à l'image d'une donnée légitime, la donnée fictive est destinée à tromper l'utilisateur ou le système qui la collecte. Elle est parfois associée à un usager "fantôme" sous la forme de profils fictifs créés sur les réseaux sociaux.

Mécanismes des structures de données fictives

On distingue plusieurs grands cas d'usage des structures de données fictives avec pour chacun d'entre eux des objectifs bien définis et des architectures

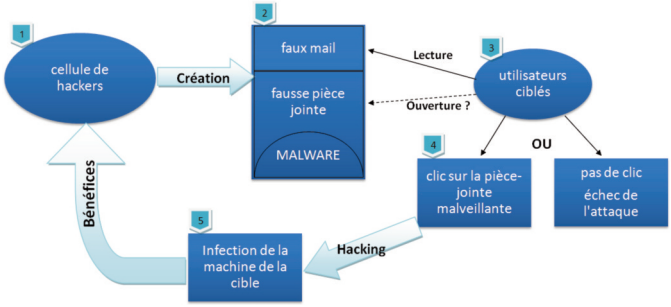


FIG. 1 - MÉCANISME DU "POUSSE AU CLIC"

adaptées à ces objectifs. Nous choisissons de décrire plus précisément quatre situations typiques : les fausses données de hacking de type "pousse au clic"; les structures de données fictives sophistiquées à objectif d'influence; les fausses données injectées par hacking dans une base légitime afin de tromper les exploitants de cette base; les fausses données créées pour alimenter et tromper les systèmes de collecte dans le but de maintenir le niveau de "privacy" de l'utilisateur.

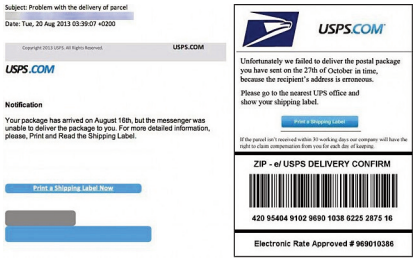


FIG. 2 - UN FAUX MESSAGE D'UPS AVEC LIEN MALVEILLANT

Les fausses données de hacking de type "pousse au clic"

Cette première situation s'inscrit dans la phase initiale d'ingénierie sociale préparatoire à une cyberattaque. Dans la majorité des cas, il s'agit pour l'attaquant d'envoyer un courrier électronique malveillant contenant une fausse information "admissible" pour les futures cibles et une pièce jointe infectée par un malware (Fig.1).

FIG. 3 - UN FAUX MESSAGE DE MISE À JOUR D'UNE APPLICATION AVEC LIEN MALVEILLANT

En fonction du crédit que l'utilisateur ciblé accorde au courrier, il choisit d'ouvrir ou non la pièce jointe. S'il décide de cliquer sur le fichier attaché, il déclenche l'exécution d'un code malveillant qui va s'installer sur sa machine. Le courrier envoyé par l'attaquant imite souvent un message légitime d'une autorité connue, d'une administration ou d'un service commercial fiable. C'est le degré de similarité avec ce modèle de message légitime qui conditionne le clic de la cible sur le lien (Fig.2 et 3). Si le degré de complexité du montage est en général assez limité, il faut pourtant que l'attaquant apporte du soin à la construction de la donnée d'imitation. L'usager quant à lui est de plus en plus

informé et sensibilisé aux dangers des clics sur des liens douteux, ce qui impose des efforts croissants du côté du faussaire. Enfin, l'exploitation des biais cognitifs en tant que composantes du facteur humain de la cybersécurité intervient fortement dans les mécanismes de "pousse au clic". Le biais de confirmation déclenche souvent à lui seul le clic dangereux.

Les structures de données sophistiquées à objectif d'influence

Dans ce cadre, les architectures déployées par l'attaquant sont souvent sophistiquées, volumineuses, hétérogènes et globalement cohérentes. Elles sont conçues selon un cahier des charges bien précis et selon un objectif d'influence parfaitement défini. Les structures de données fictives peuvent être construites pour s'inscrire dans la durée ou au contraire pour une durée de vie très courte mais suffisante pour réaliser l'objectif d'influence. On parlera dans ce cas de structures éphémères efficaces en fonction de l'échelle temporelle associée à l'objectif. Ainsi, l'opération de manipulation des cours de bourse de l'action Twitter réalisée le 14 juillet 2015 est emblématique : un site internet baptisé bloomberg.market a été créé de toutes pièces en copie du site officiel de l'agence de presse américaine www.bloomberg.com/markets. La charte graphique du site fictif imitait parfaitement le site original, seule l'adresse était différente. Le 14 juillet, une dépêche annonçe un projet d'OPA sur Twitter comprenant une offre d'achat de 31 milliards de dollars alors que la valeur du groupe atteint à peine les 25 milliards. À 11 h 39, l'instant de publication de la fausse dépêche sur le site fictif, le cours de bourse de Twitter s'envole de 5,2 % pour atteindre cinq minutes plus tard les 38,82 dollars. Une dizaine de minutes plus tard, le porte-parole de Bloomberg publie sur le site officiel le démenti « *cet article était un faux et est paru sur un site bidon qui n'est pas affilié à Bloomberg !* ». Aussitôt, la spéculation cesse et le cours de l'action retrouve son niveau d'origine. La dizaine de minutes a suffi à créer une forte volatilité et permettre aux attaquants d'effectuer des opérations extrêmement lucratives sur l'action Twitter. La SEC, le gendarme de la bourse américain a ouvert une enquête sur une manipulation de cours. Un second exemple concerne l'opération iranienne de cyberespionnage Newscaster-NewsOnLine qui s'est appuyée sur la construction d'une infrastructure de données fictives complexe afin de cibler des personnalités politiques américaines, des officiers supérieurs, des dirigeants de sociétés liées à la Défense. Un site web d'information a été créé dans la durée, supervisé par une rédaction d'une vingtaine de journalistes fictifs, tous très actifs sur les réseaux sociaux afin d'installer la confiance et de piéger ensuite des centaines de cibles et installer des logiciels espions sur leurs ordinateurs.

Les mécanismes qui régissent ces opérations passent en général par trois phases dont la durée varie en fonction des objectifs de l'attaque :

1- Convaincre les futures cibles que l'information transmise est vraie en installant la confiance.

2- Influencer les cibles afin qu'elles exécutent un certain nombre d'actions en lien avec l'objectif de l'attaquant sur l'espace physique et sur le cybersespace.

3- Tirer les bénéfices de ces actions.

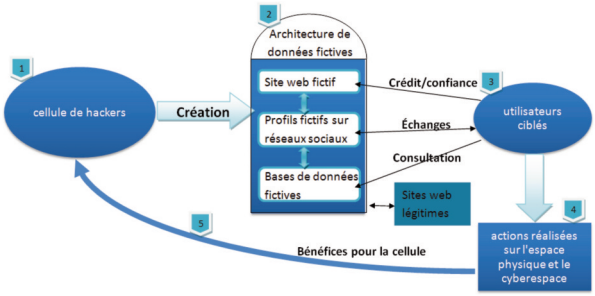


FIG. 4 - MÉCANISME DES DONNÉES FICTIVES À OBJECTIF D'INFLUENCE

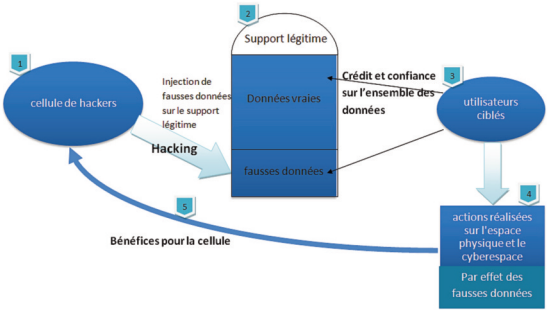


FIG. 5 - MÉCANISME D'INJECTION DE FAUSSES DONNÉES DANS UNE BASE LÉGITIME

L'injection par hacking de fausses données dans un support légitime

L'opération consiste à prendre le contrôle total ou partiel par hacking d'une base de données légitime puis d'y injecter un sous-ensemble de données fictives. Noyées dans la masse, elles doivent apparaître comme légitimes aux yeux des utilisateurs de la base. Cette technique qui s'apparente à de la stéganographie est pratiquée depuis l'antiquité et se révèle souvent très efficace pour fausser l'analyse et l'interprétation d'un ensemble de données. L'affaire Clearstream qui date de 2004 fournit un bon exemple de ce type de manipulation. De fausses données impliquant plusieurs personnalités politiques avaient été injectées dans un vrai listing (une base de données) afin de les discréditer définitivement. Désormais, ce sont les bases de données massives (big data) qui peuvent subir des injections malveillantes afin de tromper les systèmes automatisés de collecte et d'analyse.

Gavage d'un système avec de fausses données afin de préserver sa vie privée

Contrairement aux trois précédentes situations, celle-ci ne relève plus du hacking mais de la diffusion volontaire de fausses données concernant sa propre personne vers un système automatisé de collecte. L'objectif principal de l'utilisateur est de ne pas divulguer ses données

personnelles à un système qu'il juge trop intrusif. Il fait donc le choix de transmettre de fausses données au système avec lequel il interagit. Cette tendance tend à se généraliser. Selon le rapport Symantec 2015 sur la protection des données privées, 57 % des Européens se déclarent inquiets quant à la sécurité de leurs informations personnelles; 81 % estiment que leurs données ont de la valeur (>1000 euros) et 31 % n'hésitent plus à communiquer de fausses données pour protéger leurs données personnelles. Il est fort simple aujourd'hui de tromper les applications Android avec de fausses données. Ainsi, Xprivacy est un outil qui permet de nourrir les applications Android avec de faux contacts, de fausses coordonnées géographiques, de faux dictionnaires user, de faux presses papiers, de faux historiques d'appels, de faux SMS…. Le site FakeNameGenerator permet quant à lui de construire des bases de données sous divers formats (MS SQL, MySQL,IBM DB2, Oracle…) de 50 000 identités cohérentes incluant l'identité, l'âge, l'adresse, le métier et d'autres informations personnelles.

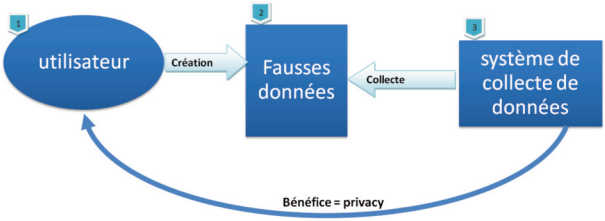


FIG. 5 - GAVAGE D'UN SYSTÈME DE COLLECTE POUR PRÉSERVER SA VIE

La donnée fictive intervient désormais comme composante initiale de l'attaque informatique. Elle constitue à ce titre l'un des principaux outils de l'arsenal d'ingénierie sociale. La détecter suffisamment tôt permettrait de bloquer de nombreuses cyber-agressions avant qu'elles ne deviennent effectives, quel que soit leur degré de complexité. Il faut développer pour cela des plateformes algorithmiques pertinentes, capables de mesurer de manière probabiliste le niveau d'acceptabilité et de véracité d'une donnée pour le système qui la collecte et qui l'exploite. Il s'agit là d'un défi majeur pour les futurs data scientists.

L'AUTEUR

Bruno Teboul
Directeur Scientifique, R&D et Innovation du groupe Keyrus,
. membre de la Gouvernance de la Chaire Data Scientist de l'Ecole Polytechnique
. Enseignant-chercheur à l'Université Paris-Dauphine.

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.

La sécurisation des données confidentielles itinérantes

par JEAN-LUC GEMO

Les outils et les services d'échange et de stockage de données(1) sont aujourd'hui devenus indispensables à la diffusion d'informations professionnelles et privées. Cependant, ils sont loin de garantir la confidentialité de nos données en toutes circonstances dans un réseau plus que jamais exposé à une cybercriminalité montante(2).

La question de la circulation des données sensibles est aujourd'hui une problématique prioritaire aussi bien à l'échelle individuelle, qu'entrepreneuriale (grandes entreprises publiques ou privées) et nationale : l'utilisation massive des appareils personnels dans un cadre professionnel(3), couplée à l'usage de plus en plus systématique de services de stockage et de partage d'informations en ligne, place désormais les données hors du contrôle des services informatiques. Cette situation pose de nouvelles questions quant aux mesures de sécurité à adopter face à la fuite d'informations et à la prolifération de terminaux non sécurisés, sachant que ces tendances sont en train de devenir des standards.

JEAN-LUC GEMO

Co-fondateur de Forecomm et de la solution BlueFiles

Qu'il s'agisse d'erreurs involontaires, de vol, de piratage ou d'espionnage, les affaires concernant des failles de sécurité informatique nous parviennent quotidiennement par la presse, témoignant de la propagation croissante des cybermenaces. Nous envoyons tous les jours des centaines d'informations et

(1) Clouds, messageries, sites de stockage de données en ligne, clés USB, etc.

(2) Citation tirée de l'article "Cybercriminalité : la France particulièrement vulnérable » : http://www.europe1.fr/faits-divers/cybercriminalite-la-france-particulierement-vulnerable-2426983

(3)BYOD: Bring Your Own Device.

Les solutions doivent tenir compte de la multiplicité des opérateurs, des vecteurs des données et des pratiques des utilisateurs.

de fichiers sur le réseau, que ce soit dans un cadre privé ou professionnel. Confiants dans les systèmes que nous utilisons quotidiennement pour stocker ou partager des informations, nous n'imaginons pas que nos données courent des risques majeurs lors de leur itinérance. Rien n'est plus dangereux qu'un sentiment de sécurité illégitime : il réduit notre vigilance et minimise le caractère confidentiel des informations que nous transmettons ou recevons.

Transmission de données : des habitudes dangereuses

Nous échangeons ainsi quotidiennement un nombre croissant de données, insouciants des cybermenaces dès que les systèmes de diffusion ou de stockage se trouvent dans un environnement physique proche (clés USB, disques durs externes, *etc.*),

(4) "Parmi les utilisateurs du stockage de données dans le « cloud », 49% disent ne pas s'inquiéter de savoir où elles se trouvent, malgré les risques associés. 93 % des utilisateurs ignorent où se situent « physiquement » leurs données personnelles." http://www.opinion-way.com/pdf/sondage_opinionway_pour_lima_-_les_francais_et_le_stockage_de_donnees_numeriques_-_mai_2015.pdf

sont des utilitaires reconnus (services de cloud, messageries de type Outlook ou Gmail,...) ou que les destinataires sont des personnes de confiance[4].

Daniel Ventre, titulaire de la chaire de cybersécurité de Saint-Cyr, nous le rappelle : « *Tout ce qui est connecté est vulnérable*[5] *. Que nous déployions d'importants systèmes de sécurité ou que nous menions de nombreuses séries de tests […]: une faille reste toujours possible* ».

(5) http://www.lepoint.fr/editos-du-point/jean-guisnel/cybersecurite-une-faille-reste-toujours-possible-22-04-2015-1923282_53.php

(6) http://www.cnetfrance.fr/news/les-geants-du-web-open-bar-pour-la-nsa-39791199.htm

(7) http://www.nextinpact.com/archive/70009-apple-icloud-securite-cles-chiffrement.htm

Les services de messagerie et de partage de données en ligne se chargent de stocker, d'envoyer et de recevoir des informations mais la confidentialité de vos données n'est pas leur cœur de métier, comme nous l'a montré l'affaire PRISM[6].

L'exemple de la société Dropbox[7] est éclairant sur ce point : vos données, chiffrées avec une clé privée sont, techniquement, « sécurisées » mais pas confidentielles. L'entreprise pourrait conserver une copie des clés de

chiffrement pour ses techniciens[8]. Par ailleurs, ses serveurs de stockage étant hébergés aux USA, vos données se retrouvent soumises aux lois américaines. Ces dernières prévoient d'ailleurs depuis le Patriot Act[9] que les prestataires de services en ligne puissent bénéficier d'un accès total à vos données. Certains s'autorisent ainsi à « *examiner, déplacer, refuser, modifier ou supprimer vos contenus sans préavis et en toute discrétion*», s'ils sont jugés contraires aux conditions d'utilisation[10]. Or, si nous pouvons avoir une confiance raisonnable dans les entreprises et les services de renseignements étatiques de notre pays, qu'en est-il des services étrangers ? N'oublions pas que les sièges de la plupart des prestataires de services en ligne que nous utilisons ne sont pas situés dans l'Hexagone.

Bien souvent sous-estimés, voire ignorés par la plupart des utilisateurs, les risques sont pourtant bien réels, comme l'attestent de nombreuses affaires récentes de fuite de données[11], de mise à disposition malencontreuse de données confidentielles des dossiers publics[12], de vol de données sécurisées en masse[13], de piratage des données privées par des grands groupes[14] ou encore de démission due à la publication frauduleuse d'emails sensibles.

(8) http://www.nextinpact.com/archive/70009-apple-icloud-securite-cles-chiffrement.htm

(9) http://www.lemonde.fr/les-decodeurs/article/2015/01/12/le-patriot-act-une-legislation-d-exception-au-bilan-tres-mitige_4554570_4355770.html

(10) « Cette loi autorise les services de sécurité à accéder aux données informatiques détenues par les particuliers et les entreprises, sans autorisation préalable et sans en informer les utilisateurs. » https://fr.wikipedia.org/wiki/USA_PATRIOT_Act

(11) http://www.zataz.com/fuite-de-donnees-internes-pour-easyjet/

(12) Affaire Bluetouff : http://www.itespresso.fr/affaire-bluetouff-droits-homme-invoques-defendre-blogueur-96609.html

(13) http://www.20minutes.fr/societe/1672275-20150825-divorces-suicides-extorsion-fonds-piratage-ashley-madison-vire-drame

(14) http://www.numerama.com/139645-t-vodaphone-pirate-les-enregistrements-telephoniques-d39une-journaliste.html

(15) Opérateur d'Importance Vitale

(16) http://www.lesechos.fr/30/03/2015/lesechos.fr/0204266819340_cybersecurite---nouvelles-obligations-pour-les-operateurs-d-importance-vitale.htm

(17) http://www.lesechos.fr/tech-medias/hightech/0203324340121-la-cybersecurite-un-marche-juteux-qui-fait-des-emules-651507.php

Des circuits sécurisés aux données sécurisées

De nombreuses entreprises (OIV particulièrement[15]) sont aujourd'hui obligées d'investir dans de coûteux systèmes de protection pour assurer la sécurité de leurs données[16] : pare-feu, antivirus, outils de sécurisation des données, « *Security Operation Center* » et autres services de cybersécurité auraient ainsi coûté plus d'un milliard d'euros aux sociétés françaises en 2013[17].

La plupart de ces services protègent des circuits de données fermés : ils vous permettent de stocker, de transmettre et de recevoir des informations et des fichiers en toute sécurité à l'intérieur d'un réseau interne (par exemple, sur votre poste de travail, *via* un service de cloud corporate ou de messagerie interne). Bien qu'efficaces, ils imposent de nombreuses

contraintes à leurs utilisateurs : configuration matérielle spécifique, réseau de stockage et de diffusion unique à déploiement limité, complexité opérationnelle, mise en œuvre laborieuse... La principale faille de ces systèmes de protection n'est pourtant pas fonctionnelle mais humaine[18]. Si l'information est effectivement protégée dans le strict cadre interne, l'usage massif des technologies mobiles, l'essor du télétravail et l'adoption massive de services de stockage et de transfert en ligne externe bouleversent la circulation des données. Ces nouvelles tendances induisent de nombreuses failles de sécurité informatique car les services gratuits sur Internet ne chiffrent pas les données en continu, les terminaux personnels ne sont généralement pas protégés (même à minima) des menaces présentes sur le réseau, constituant de véritables portes ouvertes aux hackers qui en profitent pour s'introduire dans les systèmes professionnels. Des informations dites sensibles voyagent ainsi tous les jours de terminaux en terminaux, risquant à chaque instant d'être perdues, interceptées, corrompues par des tiers (malveillance, pirate informatique…) ou des entités malveillantes (malwares, softwares, virus…).

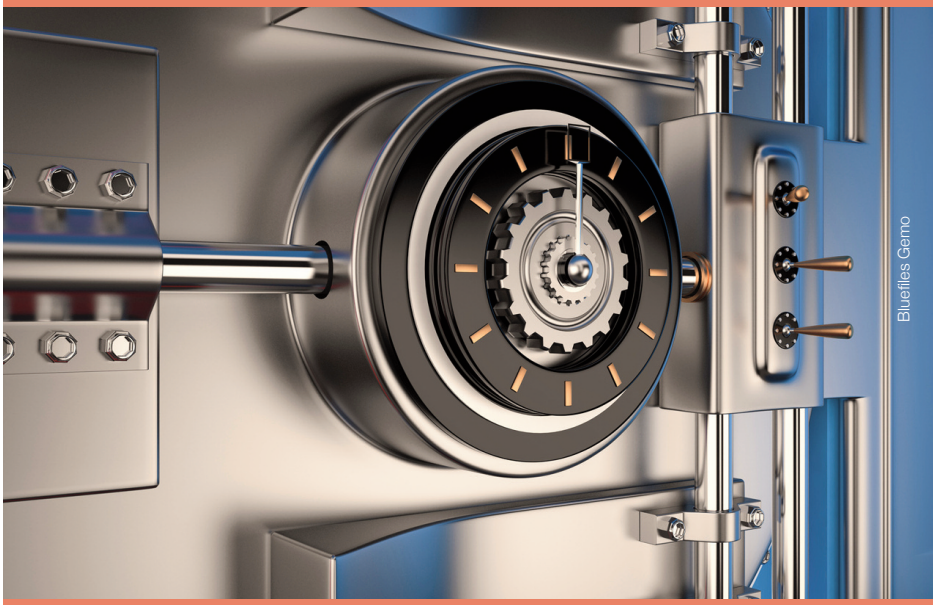
(18) http://page.arubanetworks.com/rs/arubanetworks/images/SecuringGenMobile_%20RunningtheRiskReport.pdf

Les circuits sécurisés privés (cloud privé, intranet…) sont maintenus et mis à jour régulièrement par des professionnels sans mauvaises intentions mais qu'en est-il des données partagées avec des postes qui se trouvent hors des circuits fermés ? C'est le cas du partage de fichiers avec des partenaires, des consultants ou tout simplement l'envoi d'emails vers des services informatiques dont la stratégie de sécurité est inconnue. Le nombre d'employés prenant des risques inconsidérés en envoyant de simple emails vers l'extérieur (appel d'offre, contrat, plan, *etc*.) et en utilisant des services en ligne gratuits[19], pour des raisons de productivité et d'impératifs opérationnels, est encore extrêmement élevé.

(19) Dropbox, WeTransfer, Gmail, etc.

Les informations placées sur des clés USB ou des disques durs sont moins connectées mais tout aussi exposées car ces objets ne nécessitent généralement pas de mots de passe pour accéder à leur contenu. Leur utilisation expose les données qui y sont stockées : vol du matériel, ordinateur familial infecté, récupération frauduleuse, *etc.* C'est également le cas d'une utilisation « raisonnée » d'un employé emportant des données pour travailler à domicile.

On le voit clairement, nos impératifs opérationnels et professionnels surpassent trop souvent notre sens des responsabilités face à la confidentialité de certaines données que nous échangeons ou que nous manipulons. De plus, nous ne sommes pas à l'abri de la malveillance : un collaborateur indélicat, un ancien employé malveillant sont



Une protection et un chiffrement de la donnée qui permettent une itinérance sécurisée.

toujours susceptibles de faire sortir nos données des circuits sécurisés – à l'instar de Bradley Manning[20].

(20) http://www.lemonde.fr/technologies/article/2013/08/21/bradley-manning-condamne-a-35-ans-de-detention_3464430_651865.html

De nombreuses entreprises songent ainsi à réorienter leur stratégie de cybersécurité en axant leurs efforts sur la protection de la donnée elle-même de façon à ce que leurs fichiers soient protégés en cas d'itinérance quel qu'en soit le support, le mode de stockage ou l'outil de transmission.

Maîtrise des données : un enjeu majeur

Face au nombre croissant de cyberattaques[21] et à la multiplication des données et des failles, nous sommes obligés de faire évoluer nos stratégies de cybersécurité sous peine de voir nos savoir-faire et nos compétences spoliés et « offerts » à la concurrence : perte d'avantages concurrentiels, de confiance des investisseurs, de revenus, difficultés commerciales et problèmes de réputation sont directement liés au degré de maîtrise

(21) http://www.01net.com/actualites/la-france-cible-privilegiee-des-cyberattaques-avancees-619046.html

de nos données. Un système de sécurité défaillant ou la sous-évaluation des risques liés à la cybercriminalité peuvent avoir de graves conséquences à l'échelle de l'entreprise voire à celle de la nation (affaire Snowden sur la surveillance massive et internationale des utilisateurs d'Internet[22], le site Wikileaks[23] ou plus récemment l'affaire des données « échappées » de Sony Pictures[24]).

(22) http://www.lemonde.fr/pixels/article/2015/06/02/deux-ans-apres-ses-revelations-les-premieres-victoires-d-edward-snowden_4645293_4408996.html

(23) http://www.lemonde.fr/pixels/article/2015/08/11/wikileaks-s-allie-a-varoufakis-pour-faire-fuiter-le-texte-du-traite-de-libre-echange-transatlantique_4720797_4408996.html

(24) http://www.bloomberg.com/news/articles/2015-06-19/wikileaks-posts-more-documents-from-sony-pictures-hacking

ALLER PLUS LOIN

Développée par une entreprise française, BlueFiles est une solution à la problématique de la l'échange de données sensibles. Une imprimante virtuelle (BluePrinter) crée une version chiffrée, non modifiable et versionnée des fichiers (.doc, .xls, .ppt, .dwg… et tout autre format logiciel disposant d'une commande d'impression) . La solution comporte un système d'identification de chaque destinataire et un panel d'options avancées de sécurisation (Restriction d'accès par utilisateur ou période, limitation d'ouverture aux appareils connectés. Blocage de l'impression). Les fichiers sécurisés (.blue) peuvent être diffusés via l'ensemble des canaux de diffusion classiques. La donnée étant chiffrée en local, un fichier .blue est donc illisible pour un prestataire de service en ligne comme pour un spyware ou un hackeur. Ils ne peuvent être déchiffrés que dans l'application sécurisée BlueReader (Application gratuite) qui contient un système de double authentification (email + code d'activation – valable 1h). Les paramètres de sécurité d'un fichier .blue peuvent être modifiés en temps réel : restriction d'accès, blocage de l'impression, non-conservation d'une copie locale... Le contrôle des données itinérantes reste permanent. BlueFiles possède également une fonction de traçabilité des données qui permet de suivre en temps réel l'utilisation des fichiers (localisation, ouvertures, plateforme de lecture…).

www.mybluefiles.com

Une science des données
pour une guerre de l'information

par JEAN-PAUL PINTE

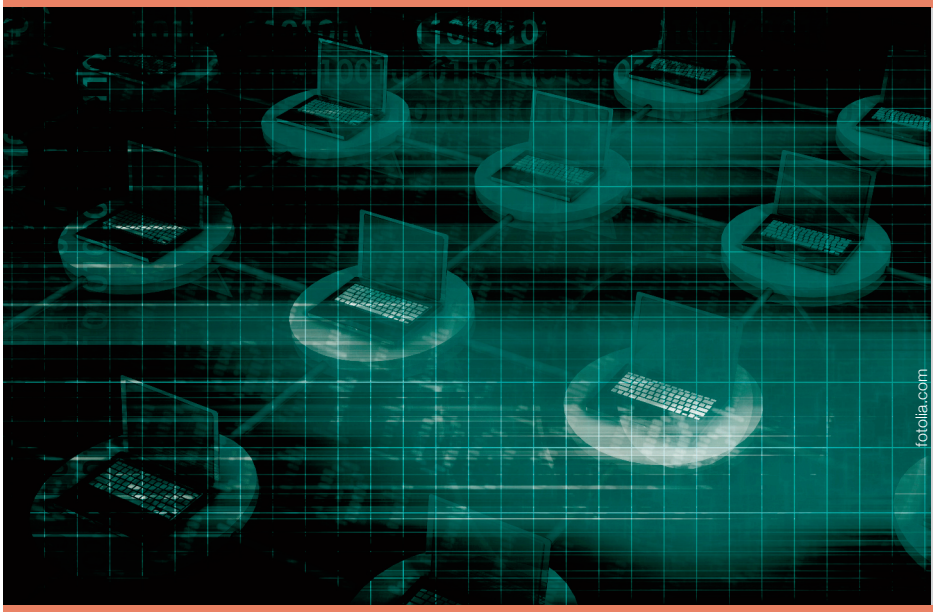
Notre société est aujourd'hui gouvernée par des algorithmes ou calculateurs que l'homme a créés et qui en retour le construisent. Pendant longtemps le pouvoir d'accéder à l'information stratégique a relevé d'une certaine élite ou de pouvoirs attribués par l'État à des instituts dans le cadre d'études précises et de veille stratégique. Aujourd'hui ce n'est plus le cas.

Chacun de nous peut à son niveau accéder à des informations utiles sur le rayonnement de sa vie privée et professionnelle sur la toile. Cette capacité est même devenue une urgence pour tout citoyen ou toute entreprise qui souhaite maîtriser et protéger son environnement informationnel, humain et matériel. En ce qui concerne la cybercriminalité, le cyberterrorisme nous nous dirigeons même vers une science prédictive de l'information dont la mise en place s'imposerait de manière urgente suite aux derniers événements de janvier et de novembre 2015. Mais tant de territoires sur la toile restent inexplorés …

JEAN-PAUL PINTE
Maître de conférences
Université catholique de Lille

Ces règles et instructions qui peuvent résoudre des problèmes

Nos vies sont désormais numériques voire algorithmiques. On voit ainsi poindre avec ces algorithmes une science sociale ou des données qui consisterait à étudier la production, l'analyse et la consommation de l'information. Ces séries d'instructions que sont les algorithmes opèrent via des calculs dans le Big Data et l'Open Data. Elles permettent aujourd'hui d'obtenir des résultats pour prévoir nos besoins, nos souhaits informationnels, mais aussi détecter nos tendances voire même maintenant prédire le (cyber) crime. Ces quantités de données que constituent les



Le maillage des objets entre eux rend difficile les investigations relatives au stockage des données et à la surveillance des échanges illégaux.

algorithmes nous poussent même à leur faire de plus en plus confiance. Les infonomistes, ceux qui pour qui le métier est l'infonomics, utilisent cette science et sont capables au même titre que des Etats et des entreprises spécialisées de chiffrer le monde.

Dominique Cardon, sociologue des réseaux se questionne même dans son dernier ouvrage sur ce à quoi rêvent ces algorithmes [1] pour nos vies à l'heure du Big Data.

(1) Dominique Cardon, A quoi rêvent les algorithmes ? : Nos vies à l'heure des Big Data, Editions du Seuil et de la République des Idées, 2015

Il est loin le temps où Internet était encore sommable. Aujourd'hui extraire de l'information et de la connaissance de ce déluge de données dépasse largement les capacités de tout être humain. Le stockage des données n'est plus la grande difficulté. Aujourd'hui, il est surtout question d'extraction de données, en termes de pertinence et de discernement, avec l'aide d'algorithmes efficaces. Les résultats des requêtes obtenus d'un moteur de recherche sont aussi le fruit d'algorithmes. Les publicités qui s'affichent ne sont plus du domaine de l'aléatoire. Il va falloir apprendre à vivre avec ces algorithmes tout en mesurant que ceux-ci peuvent être le

fruit de manipulations. Par exemple, rien ne vous empêche de vous retrouver un jour la cible des services de renseignement suite à une recommandation d'un tiers qui vous inciterait à cliquer sur un lien voire si vous tapez un mot-clé vous amenant dans le cyberespace vers des liens non recommandables mais tracés par ces services.

Toutes ces transactions et manipulations ne sont pas toujours du ressort de l'humain. Il y a ici presque une part de déshumanisation et d'assujettissement lorsqu'il s'agit de surveiller par exemple l'apologie du terrorisme sur des espaces de microblogging comme Twitter où il est possible de robotiser les tweets ! Dans le domaine de la santé, de manière plus utile, on a pu prédire des épidémies de grippe rien qu'en surveillant sur Google le questionnement de personnes atteintes de la maladie ou d'autres -en doute de symptômes - simplement en agrégeant les requêtes formulées sur le moteur de recherche et les commentaires émis sur des espaces collaboratifs d'écriture.

Les architectures distribuées restent à explorer…

A l'heure de l'infobésité et des mégadonnées, la question de classifier et d'organiser l'information n'a jamais été aussi présente. Le discernement de l'information dans cette masse informationnelle se pose aujourd'hui avec acuité. Les algorithmes fabriquent peu à peu notre existence numérique mais ce n'est pas tout. Il existe d'autres exemples d'architectures distribuées[2] qu'il convient d'investir aujourd'hui pour approfondir des recherches stratégiques.

(2) Cécile Méadel, Francesca Musiani (Coord), Abécédaire des architectures distribuées, Presse des Mines, Paris, 2015

Internet en est un des meilleurs exemples puisqu'il ne possède aucun nœud central. Les architectures distribuées reposent sur la possibilité d'utiliser des objets qui s'exécutent sur des machines réparties sur le réseau et qui y communiquent par messages.

Rappelons cependant qu'Internet n'est pas le Web et qu'à ce titre des outils, comme ceux de l'anonymisation, ont leur place dans le décor des réseaux distribués et de la recherche approfondie puisqu'ils protègent le citoyen et offusquent des opérateurs mal intentionnés. Parmi ces derniers, on trouve le plus souvent des proxys de type HTTP/SOCKS ou encore des réseaux privés virtuels (VPN) ou encore TOR (The Onion Router). Ce dernier tend à être de plus en plus surveillé ces derniers mois ce qui limitera progressivement l'anonymisation de ses utilisateurs.

Le nomadisme informationnel se développe

Les applications nomades, contenues sur les Smartphones, tablettes et autres écosystèmes numériques, sont aussi devenues des outils intelligents. La captation des données relatives aux échanges de manière distribuée, via ces outils, en mode pair-à-pair, par des cyberdélinquants, peut constituer de bons terrains d'investigation pour les services en charge de la surveillance.

Les technologies Bluetooth et IRDA, dont l'échange se fait par infrarouge, représentent les premières fonctionnalités de pair-à-pair, mobile et sans fil, et permettent d'échanger des données en direct et sans intermédiaires. Les techniques de télécommunication radio courte distance inventées par Ericsson (Réseaux Mesh), il y a plus de vingt ans, vont également dans le sens de la mobilité distribuée. Le logiciel "Commotion" qui permet de créer des réseaux MESH a ouvert la voie à de nouvelles applications telles que les jeux, la cartographie participative, VoIP locale et la diffusion d'informations, etc.)

Les "réseaux peer to peer", qui permettent aux gros fichiers d'être distribués, le "Darknet", avec ses communautés Internet privées et le "cloud computing", qui permet le stockage de documents sur Internet plutôt que sur les ordinateurs individuels, sont autant de lieux où il sera nécessaire d'investiguer. Toutefois, sur ces réseaux, les données seront cryptées et configurées pour fonctionner avec de nouveaux appareils tels les objets connectés, laissant peu ou aucune trace des données sous-jacentes. L'enjeu est grand car on estime que le nombre d'objets connectés en circulation à travers le monde s'élèvera entre 50 et 80 milliards d'ici 2020 !

Consoles de jeux, crypto-monnaies et autres technologies

Il n'y a rien de surprenant à ce que l'on utilise aujourd'hui une console de type PS4 pour communiquer entre personnes. De nombreuses applications sur les Smartphones font déjà l'usage de cette fonctionnalité. La plupart des jeux ont aussi des systèmes de messagerie instantanée qui nécessiteraient une surveillance. De même, les pressions sur le GamePad ne peuvent être décelées ni interprétées si une codification est définie au préalable par les joueurs ou les communicants sur la console. Les systèmes de voix sur IP de PlayStation, comparés aux autres formes traditionnelles de communication, seraient plus difficiles à surveiller par les enquêteurs et on pourrait même imaginer que les derniers attentats auraient pu être organisés *via* ces consoles en communiquant sans parler ou taper un seul mot. La technologie et le logiciel "off-the-shelf" permettent aussi

de crypter la voix de téléphone et les messages texte sur mobiles. Il permet aussi de rester en contact comme ce fut le cas lors des attentats de Bombay.

Basé sur un protocole Peer To Peer, le Bitcoin vise à offrir une solution alternative à la monnaie réelle. Il est donc une manière d'effectuer des transactions, via une communication entre les utilisateurs, sans recourir aux rouages et contrôles d'une banque réelle. Récemment, lors d'attentats, il a même été évoqué le financement très probable d'organisations instigatrices d'actes terroristes via le logiciel Bitcoin. D'autres crypto-devises, plus sophistiquées, comme Etherum permettent de créer à partir d'une plateforme d'autres applications grâce à un langage de programmation (Touring complete).

Ainsi, les cyber-délinquants auraient de plus en plus recours à la technologie, y compris Google Earth et Street View, pour planifier leurs attaques. Ils utilisent aussi des dispositifs de cryptage plus sophistiqués comme la stéganographie, déjà utilisée en 2001. Cette technique vise à faire passer inaperçu un message dans un autre message mais aussi à intégrer un texte dans une image. La stéganographie se distingue de la cryptographie qui s'attache à protéger des messages en assurant leur confidentialité, authenticité et intégrité.

Il est aujourd'hui encore plus question pour notre société d'une véritable gouvernance de l'Internet et d'un nouveau paradigme en ce qui concerne les compétences informationnelles. Alors que tout s'agite autour de nous, la difficulté d'intégrer la notion de guerre de l'information, chère à l'intelligence économique, au monde du renseignement semble encore constituer un frein.

L'AUTEUR

Jean-Paul Pinte, Docteur en Information Scientifique et Technique, est Maître de conférences à l'Université Catholique de Lille et spécialiste de la veille et de l'intelligence compétitive qu'il enseigne dans plusieurs masters en France et à l'étranger.
Cyber-criminologue et spécialiste de la fouille de données, Il enseigne la cybercriminalité dans plusieurs Masters en France. Il est expert scientifique au Conseil supérieur de la formation et de la recherche stratégiques (CSFRS), membre expert de l'Association Internationale de Lutte Contre la Cybercriminalité (AILCC), de l'Académie de l'intelligence Economique et du FIC (Forum Internationa de cybercriminalité) depuis sa création.
Titulaire d'un certificat en management des risques criminels et terroristes des entreprises, délivré par l'EDHEC et l'INHESJ, ses compétences et son statut de Lieutenant-colonel de gendarmerie (RCC) l'amènent à intervenir à l'Ecole de Guerre à Paris, à l'Ecole Nationale de Magistrature, dans la formation continue du personnel des tribunaux ainsi qu'à l'Institut National des Hautes Etudes de Sécurité et de Justice (INHES J).
Il a écrit de nombreux articles dans des revues spécialisées comme la Revue pour la science et a publié plusieurs articles dans la Revue de la Défense Nationale ainsi que dans la Revue de la Gendarmerie Nationale. Il et est le co-auteur, avec Myriam Quéméner, d'un ouvrage intitulé Cybercriminalité des acteurs économiques : risques, réponses stratégiques et juridiques aux Editions Hermes-Lavoisier en 2012. Il a dirigé un ouvrage sur l'identité numérique dans les Cahiers du Numérique des Editions Hermes-Lavoisier (Vol 7/1 — 2011). En mai 2014 est sorti son dernier ouvrage coordonné chez Hermés-Lavoisier intitulé Enseignement, préservation et diffusion des identités numériques.
Il est enfin l'auteur du blog bien connu sur la cybercriminalité, la sécurité et l'ordre public sur internet.
http://cybcrcriminalitc;wordpress.com

Dans quel univers
évolue le véhicule connecté ?

par FRANCK MARESCAL et DARIO ZUGNO

Une étude de l'agence HAVAS, effectuée en début d'année 2015, montre que 71 % des automobilistes estiment que le véhicule est l'objet connecté le plus attendu. Les bénéfices espérés sont nombreux que cela soit pour la préparation à l'avance d'un voyage, le développement de systèmes collaboratifs entre conducteurs ou l'usage de nombreuses aides pour faciliter la conduite... On peut penser que cette évolution rapide des technologiesembarquées, dont on ne parlait pas ou très peu il y a une année encore, va révolutionner notre vie d'automobiliste mais cette belle médaille a un revers.

FRANCK MARESCAL

Colonel de gendarmerie, chef de l'observatoire central des systèmes de transport intelligents

DARIO ZUGNO

Chef d'escadron de gendarmerie, affecté à l'observatoire central des systèmes de transport intelligents

A travers une succession de questions, une description rapide d'un véhicule connecté et l'appréciation de son besoin dans notre société, nous analyserons les menaces qui pèsent de plus en plus sur le véhicule connecté. Nous verrons alors comment le sécuriser d'un point de vue technique, juridique et conceptuel. Nous aborderons enfin la posture de la gendarmerie nationale dans ce domaine.

Comment définir un véhicule intelligent et connecté ?

Le véhicule est considéré comme intelligent par ses technologies embarquées qui permettent de faciliter la conduite et d'apporter plus de confort ou de sécurité dans un esprit de développement durable. Déjà, les ADAS (*Advanced Driver Assistance Systems*)

Syda Productions

Une connexion de prime abord réservée à des fonctions de sécurité et de perception de l'environnement.

intègrent des systèmes d'aide comme le régulateur de vitesse. De nouveaux dispositifs voient le jour, qu'ils soient connectés au monde extérieur ou pas. D'ores et déjà proposés sur des modèles haut de gamme, ils seront au minimum en option, voire en série, dans tous les véhicules d'ici 5 années. Il s'agit globalement de systèmes préventifs d'accident (freinage d'urgence par la détection automatique de piétons ou d'obstacles, détection du manque de vigilance du conducteur ou de franchissement de ligne blanche, systèmes pouvant agir sur le comportement du conducteur), d'assistance au conducteur (suivi de ligne automatiquement sur autoroute, intégration intelligente du smartphone dans le véhicule, réalité augmentée, détection des panneaux de signalisation, conduite semi-autonome dans les bouchons, meilleur parcours proposé) ou collaboratif (partage de données, par ex. le lien V2V - véhicules à véhicules - dans une zone pour prévenir de danger).

Pour fonctionner, ces systèmes intelligents nécessitent des capteurs pour appréhender l'environnement plus ou moins lointain du véhicule. Des caméras de vision avant ou fixant le conducteur sont embarquées, avec des dispositifs ultrasons, des radars et des lidars (scan en 3D) en complément, sans oublier la connectivité vers l'extérieur apportant des informations de localisation, de trafic et d'événements à anticiper. Ceux-ci sont mis en œuvre par des calculateurs (appelés ECU : *Electronic Control Unit*), qui agissent aussi sur les organes de

fonctionnement classiques du véhicule (direction, moteur, freinage, gestion de l'habitacle, divertissement, localisation, verrouillage centralisé, téléphonie main libre, ...) reliés entre eux par un réseau de transfert de données (CAN : Controller Area Network). Une prise OBD-II (On Board Diagnostic), permettant d'accéder directement au CAN pour un diagnostic et l'entretien et du véhicule, complète ces technologies.

La connexion vers l'extérieur est assurée par de multiples voies, en particulier les puces téléphoniques, le Bluetooth, la prise OBD, bientôt le WIFI.

L'ensemble de ces technologies interconnectées entre elles, la fusion de ces données et la prise de décision automatique sont le vrai challenge pour aboutir demain au véhicule autonome de confiance, garantissant le niveau de sûreté et de sécurité conforme aux attentes et aux enjeux sociétaux et économiques.

L'automatisation de la conduite a été définie selon 5 niveaux d'autonomie par le consortium SAE[1], association internationale d'ingénieurs et d'experts dans divers domaines de l'industrie. Au dernier Congrès mondial des Systèmes de Transport Intelligents, l'institut français VeDeCom a fait une présentation de son savoir-faire avec un véhicule de niveau 4, le plus abouti des démonstrations.

(1) SAE : SAE international (les lettres n'ont pas de signification), anciennement Society of Automotive Engineers

L'évaluation de la nécessité d'une connexion dans un véhicule

La mise en place du système d'appel d'urgence e-call par l'ensemble des états européens est fixée au plus tard au 1er mars 2018. Ce dispositif permettra de transmettre automatiquement des informations à une plate-forme, par appui sur un bouton d'aide ou en cas d'accident, qui évaluera l'assistance à mettre en place. Un contact téléphonique pourra alors être pris avec l'habitacle du véhicule. Un dispositif presque équivalent est déjà proposé par des constructeurs mais il n'est pas encore obligatoire.

De nombreuses autres fonctionnalités nécessitent d'être connectées. Il s'agit par exemple des services de localisation pour recevoir la circulation routière environnante et la capacité de mettre à jour la cartographie, tout en envoyant des données anonymisées vers un serveur de gestion. La surveillance du véhicule en cas de vol est aussi une possibilité offerte et l'information peut être transmise à un smartphone. Enfin, la mise à jour logicielle (dite *over the air*) à distance est aussi une caractéristique des véhicules modernes, ou le deviendra très vite.

En outre, le projet collaboratif SCOOP, en cours d'expérimentation sur 5 zones en France, permettra à quelques milliers de véhicules de communiquer entre eux par

le biais de réseaux sans fil, en particulier le WIFI G5, afin de faciliter leurs déplacements grâce à des informations envoyées automatiquement entre eux ou avec un gestionnaire de voirie et ainsi d'améliorer la sécurité routière.

Ces exemples non exhaustifs montrent tout l'intérêt du véhicule communicant.

Le véhicule connecté est un système menacé

Le nombre de cyber-attaques visant des entreprises a augmenté de 38 % dans le monde ces douze derniers mois et de plus de 50% en France avec 21 incidents grave par jour (source Pricewaterhousecoopers du 15/10/2015). Ces attaques se font *via* le réseau informatique avec souvent des pertes financières importantes. L'informatique est omniprésente dans un véhicule récent où l'on dénombre jusqu'à 80 ECUs (*Electronic Control Unit*) qui exécutent 60 millions de lignes de code et échangent jusqu'à 25 Go de données par heure sur le bus de communications interne, le CAN. Les véhicules connectés sont donc tout autant menacés.

Chaque année se tiennent des conférences (Blackhat) et des conventions (DefCon) aux États-Unis réunissant des professionnels de la sécurité des systèmes d'information et des hackers. Elles donnent lieu à de multiples interventions sur des sujets liés au piratage informatique, à des concours divers et à des démonstrations toutes plus impressionnantes les unes que les autres : piratage d'un fusil connecté qui a manqué toutes les cibles choisies, prise de contrôle de caméras de surveillance d'une habitation pilotées par un smartphone, actions à distance sur un véhicule...

Au cours de ces dernières années, la communauté des pirates informatiques a montré à plusieurs reprises qu'il est possible de compromettre la cybersécurité des véhicules. Ceci est d'autant plus préoccupant qu'il s'agit de la compromission de la sécurité des passagers ou d'autres usagers de la route.

A l'été 2015, trois événements ont défrayé la chronique aux Etats-Unis avec la prise de contrôle à distance d'une Jeep Cherokee, d'un Model S de Tesla, ainsi que d'une Chrysler Corvette piratée par l'envoi d'un simple SMS sur le boîtier, relié au CAN par la prise OBD, provoquant la coupure du système de freinage. De nombreuses publications scientifiques appuient ces exemples.

La prise de conscience de cette problématique existe mais est assez récente. La défense canadienne a par ailleurs lancé un appel d'offre très sérieux en octobre 2015 pour trouver le hacker capable de protéger ses véhicules et de trouver les vulnérabilités et les mesures de sécurité adéquates à mettre en place.

Globalement, la Stratégie Nationale pour la sécurité du numérique présentée le 16 octobre 2016 vise à lutter contre des menaces bien identifiées touchant entre autres les individus et les objets connectés, sous l'égide de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information – SGDSN) dont un mode d'action important est le fait « d'agir ensemble ».

Quels sont les dangers identifiés consécutifs à un piratage

Les vecteurs d'attaques pour pénétrer sur les systèmes embarqués des véhicules sont nombreux et peuvent s'expliquer par un manque de procédures d'authentification, de contrôle, de cryptage des données ou même par des vulnérabilités logicielles. A l'image de tout système informatique complexe, l'intrusion peut venir de dispositifs qui seraient mal sécurisés comme le data center d'un constructeur, la prise USB, le Bluetooth, le WIFI, le réseau CAN, la prise OBD ou la puce téléphonique. D'autres vulnérabilités potentielles existent aussi via un smartphone relié au véhicule, une montre connectée, une clé intelligente, ou encore la valise diagnostique des réparateurs.

Les menaces engendrées sont alors de deux ordres.

A - Les risques liés à la sécurité :

- Déni de service (perturbation du dispositif V2V, déconnexion de fonctions de localisation, aides à la conduite hors d'usage)
- Intimidation (actions de commandes sans contrôle du conducteur)
- Demande de rançon (le véhicule est rendu hors d'usage temporairement)
- Terrorisme (accident, interception, arme par destination)

B - Les risques liés au respect de la vie privée :

- Vols de données personnelles
- Manière de conduire
- Écoute téléphonique (kit main libre, e-call)
- Localisation du véhicule (en temps réel ou historique)
- Surveillance vidéo (caméra frontale nécessaire au freinage d'urgence, ou caméra conducteur de surveillance de la vigilance)

La sensibilité du risque est proportionnelle à la vraisemblance de la menace et à l'impact suscité. On peut imaginer l'émoi dans la population si ces menaces devaient arriver à une grande échelle ou dans un transport collectif. L'ensemble des acteurs liés au véhicule a donc tout intérêt à les anticiper.

Le véhicule connecté peut-il être sécurisé ?

La norme ISO 26262 traite de la sûreté fonctionnelle des véhicules mais n'est pas

La sécurisation des fonctions connectées oblige à prendre en compte dès la conception du système d'information du véhicule son adéquation aux normes habituelles en informatique.

adaptée à sa sécurisation contre le risque Cyber. La norme ISO 27001 traitant du Système de management pour la sécurité de l'information (SMSI) et reflétant l'état de l'art au niveau international permet de gérer la sécurité des actifs informationnels. La sécurité du véhicule connecté, ordinateur à quatre roues, doit donc s'en inspirer pour obtenir une protection appropriée contre la perte de disponibilité, de confidentialité et d'intégrité. Pour ce faire, il est opportun de surveiller et d'évaluer l'efficacité des mesures de sécurité, d'identifier les risques émergents et le cas échéant d'améliorer les mesures de sécurité. Cela sous-entend la prise en compte d'un vaste éventail de menaces.

Ainsi les préconisations fournies par l'ISO 27002 (code de bonnes pratiques pour les SMSI) et par l'ISO 27005 (gestion de risques liée à la sécurité informatique) permettent une appréciation des risques par son analyse et son évaluation.

Toutefois la sécurité de l'information n'est pas toujours prise en compte dès la conception et l'élaboration des systèmes d'information. L'intégration après coup de la sécurité s'avère difficile et coûteuse.

Des initiatives existent pour améliorer la sécurité. Le projet collaboratif AUTOSAR[2] vise à standardiser et à optimiser les

(2) AUTOSAR : AUTomotive Open System Architecture (www.autosar.org)

(3) SESAMO : Security and Safety Modelling (www.sesamo-project.eu)

processus de communication interne et les logiciels embarqués. Le projet européen SESAMO[3] qui vient de se terminer apporte aussi des bases sur le double aspect sécurité et sûreté.

Aux États-Unis, la société Intel a créé récemment un conseil de la sécurité informatique du véhicule connecté (ASRB[4]) rassemblant des experts de l'industrie automobile dans le monde entier, plus particulièrement chargé des systèmes de cybersécurité. Ces chercheurs effectueront des tests et des vérifications et seront en mesure de pouvoir codifier les bonnes pratiques et d'adresser des recommandations et des solutions de cybersécurité, un ingrédient essentiel dans la conception de chaque automobile des générations futures. Intel fournira des plateformes avancées de développement permettant de mener ces recherches.

(4) Intel ASRB : Intel Automotive Security Review Board

L'amélioration de la sécurité pourra s'effectuer en agissant sur deux leviers complémentaires que sont la sensibilisation des concepteurs (constructeurs automobiles, équipementiers, starts-up) à l'origine du produit et celle de l'utilisateur pour les rendre exigeants en matière de sécurité.

Enfin, le gouvernement français a lancé, dans le cadre des Plans pour la Nouvelle France Industrielle, des initiatives visant notamment à fédérer des actions de recherche sur le véhicule autonome et connecté et conforter la confiance numérique. L'Institut de Recherche Technologique SystemX, a lancé début 2015, avec le pôle de compétitivité Systematic, la mise en œuvre d'une plateforme expérimentale CHESS (*Cyberecurity Hardening Environment for Systems of Systems*) et d'un projet de recherche associé EIC (Environnement pour l'Intégration et l'interopérabilité en Cybersécurité), avec un appui très fort de l'ANSSI et de quelques industriels. L'objectif est d'évaluer le couplage de technologies de cybersécurité à travers des cas d'usages innovants dans le domaine des SmartGrids, de l'Usine du Futur, du Transport Connecté et Autonome et des nouveaux services de l'Internet des Objets. Le projet de recherche traite également des aspects économiques, des impacts assurantiels et de la dimension juridique et réglementaire de la cybersécurité.

Le véhicule connecté doit-il être protégé d'un point de vue juridique ?

Il s'agit d'une question épineuse qui ne manquera pas de faire débat dans un futur plus ou moins proche. Aujourd'hui le contexte juridique du véhicule et de son conducteur est relativement simple et devrait être complété.

Au niveau civil :

- le régime de la responsabilité du fait personnel (art 1382 du Code Civil) ou de celui des choses que l'on a sous sa garde (art 1384 du Code Civil).

- le droit du respect de sa vie privée (art 9 du Code Civil) et à la protection des

données à caractère personnel (loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

Au niveau pénal :

- l'intimité de la vie privée d'autrui (art 226-1 du Code Pénal), le véhicule étant considéré comme une annexe du domicile privé.

- les atteintes aux systèmes de traitement automatisé des données (STAD – art. 323-1 et suiv.) comme le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données (et par extension dans le système informatique d'un véhicule), d'introduire frauduleusement des données, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient, est réprimé par la loi.

En outre, le chef d'entreprise a une obligation générale de sécurité et des obligations légales en cas de fuite d'information lorsque celles-ci contiennent des données à caractère personnel.

Avec l'installation d'un enregistreur EDR dans le véhicule qui pourrait consigner les paramètres de conduites, mais également des vidéos par les caméras embarquées, il reste à savoir s'ils pourraient être utilisés par différents acteurs intéressés par ces données, tels que les assureurs, la justice et les forces de l'ordre en cas de sinistres graves mais également pour de simples contrôles.

(5) Les véhicules communicants nécessitent-ils de nouvelles réglementations ? Par Bernard FLURY-HERARD et Hervé de TREGLODE – juin 2015

Enfin, un rapport[5] du Conseil Général de l'Environnement du Développement Durable (CGEDD) dresse des pistes de réflexion et des recommandations pour améliorer la sécurité des systèmes embarqués.

La posture de la gendarmerie nationale

Afin d'anticiper ces vulnérabilités pour limiter dès que possible leurs conséquences et de profiter des opportunités pour le service de la gendarmerie nationale (dans l'amélioration de ses modes d'action par exemple), un observatoire central (OCSTI[6]) a été créé en juin 2015. Il a pour objectifs :

(6) OCSTI : Observatoire Central des Systèmes de Transport Intelligents – gendarmerie nationale

– de disposer d'une vision globale du domaine des transports intelligents, et au-delà des objets connectés, en assurant une veille technologique poussée (en France et à l'étranger) ;

– de recueillir du renseignement criminel dans le domaine des STI auprès des unités territoriales de la gendarmerie, de l'analyser et d'effectuer des propositions en matière de sûreté ;

– de développer et d'entretenir un réseau de correspondants afin d'expliquer les problématiques de la gendarmerie et de renforcer les partenariats existants entre les divers acteurs des Transports Intelligents en les faisant bénéficier de notre expertise dans certains domaines ;

– de suivre les groupes de Travail inter-administrations ;

– de s'impliquer dans l'expérimentation de projets pilotes ;

– de communiquer ses travaux ou ses réflexions via une lettre trimestrielle et un rapport annuel ;

– d'organiser un séminaire international regroupant l'ensemble de ses correspondants.

L'Observatoire accompagne donc les acteurs du domaine des Transports par un suivi rigoureux de l'évolution des technologies et de la réglementation. Dans son rôle de prévention, l'OCSTI sensibilise les constructeurs et équipementiers et propose ses analyses.

Faut-il prévoir une législation ?

Au même titre que n'importe quel dispositif électronique ou informatique, un véhicule connecté embarque de nombreux systèmes numériques et doit être protégé pour assurer sa sécurité de fonctionnement ou pour interdire le vol de données personnelles. Les risques énumérés plus haut le montrent bien.

Il ne paraît pas indispensable de légiférer si les standards de la sécurité informatique sont suivis par tous les acteurs du domaine des transports. Les concepts de « *security by design* » et de « *cyber résilience dans les ITS* » (consensus international qui semble s'être dégagé lors du dernier congrès mondial des ITS - *Intelligent Transportation System*) sont des guides cohérents et nécessaires. La prise de conscience et l'anticipation sont indispensables.

Ainsi, des recommandations devraient suffire à l'image de celles données par la NHTSA-USA « National Highway Traffic Safety Administration » [7][8] ou par sa stratégie clairement affichée un an plus tard[9], la feuille de route du ministère des Transports allemand[10] en septembre 2015 ou les standards apportées par le consortium international SAE[11]. Encore faut-il qu'elles soient élaborées rapidement (profil de protection, spécifications), soit par l'administration, soit par un conseil de standardisation technique du domaine des Transports, puis bien évidemment publiées et suivies (avec une évaluation par exemple). En complément, la transparence du code source informatique et des algorithmes est nécessaire pour évaluer en tant que de besoin la sécurité par des organismes mandatés. Ce concept, repris de plus en plus dans les réflexions, est pris en compte par le gouvernement dans la loi pour une république numérique.

(7) A Summary of Cybersecurity Best Practices – octobre 2014

(8) Risk Management Framework Applied to Modern Vehicles – octobre 2014

(9) NHTSA ans Vehicle Cybersecurity – juillet 2015

(10) Strategy for automated and connected driving – Federal ministry of transport and digital infrastructure – sept 2015

(11) Cybersecurity guidebook for cyber-physical automotive systems J3061 – janvier 2014

Aux États-Unis, des sénateurs ont jugé que ces recommandations n'étaient pas assez prises en compte comme le montre une analyse du cabinet de conseil

(12) Cybersecurity : automakers remain passive as government takes action – août 2015

(13) Security and Privacy in Your Car Act of 2015

américain FROST & SULLIVAN[12], et un projet de loi a été déposé au Congrès. Il s'agit du « SPY CAR ACT of 2015 » [13].

Le développement aujourd'hui rapide du véhicule connecté et sa large diffusion posent de nombreuses questions pour lesquelles nous avons tenté d'apporter une réponse.

D'autres enjeux devront aussi être relevés comme celui relatif à la préservation de la preuve pour que la justice puisse mener une enquête en cas d'intrusion dans le système numérique du véhicule (norme ISO 27037). Les constructeurs ont l'obligation de laisser à la disposition de la justice un état du système, une copie des « logs » ou de toute information numérique en lien avec une intrusion. Il s'agit peut être alors dès maintenant de repenser complètement l'architecture informatique du réseau interne du véhicule pour le simplifier et le rendre plus sécurisé et ainsi probablement plus efficace.

Dans quelques années, le véhicule autonome sera la déclinaison la plus avancée du véhicule connecté et d'autres interrogations apparaissent déjà dans le domaine éthique, psychologique et technique. L'exigence et le comportement des consommateurs de ce type d'automobiles seront aussi des facteurs structurants.

La cryptologie au cœur de la cybersécurité : enjeux et choix

par **BERTRAND WARUSFEL**

Une dimension peu connue de la transformation numérique est l'importance croissante que les technologies cryptographiques ont prise et le rôle qu'elles jouent dans la sécurisation de nos systèmes d'information. Les évolutions récentes du cadre juridique européen et les nouveaux besoins du marché vont certainement induire un recours accru aux outils cryptographiques.

La science du chiffre a quitté les lieux clos des enceintes militaires et diplomatiques pour s'insinuer dans tous nos moyens de traitement et de transmission de l'information, ce qui a imposé au fil des décennies une révision radicale du cadre technique et juridique de leur utilisation.

BERTRAND WARUSFEL

Professeur de droit
Université de Lille (CRDP-ERDP)

S'agissant de la France, nation de mathématiciens et puissance militaire et diplomatique jalouse de son indépendance, il a été assez long et difficile de changer de paradigme. Assimilés jusqu'en 1986 à des matériels de guerre dont la production, le commerce et l'exportation étaient fortement encadrés, les systèmes cryptographiques ont connu pendant une quinzaine d'années une période transitoire durant laquelle leurs fournisseurs souhaitant diffuser en France ou exporter leur production devaient se soumettre à des contraintes fortes de déclaration ou d'autorisation préalable auprès du Premier ministre[1].

Ce n'est, en effet, qu'en 2004 que l'article 18 de la loi sur la confiance dans l'économie numérique a définitivement

(1) Voir notamment B. Warusfel, "Dix ans de réglementation de la cryptologie en France : du contrôle étatique à la liberté concédée", Annuaire français de relations internationales, n° 1, 2000 (http://www2.droit.parisdescartes.fr/warusfel/articles/reglcrypto_warusfel.pdf).

reconnu que « *l'utilisation des moyens de cryptologie est libre* » et que le commerce sur le territoire national des produits « *n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité* » (c'est-à-dire qui mettent en œuvre en particulier des fonctions de chiffrement) ne serait plus soumis qu'à un régime de déclaration préalable simplifiée.

Au-delà de ces règles domestiques, la France - comme tous ses partenaires de l'Union européenne - a continué à appliquer les prescriptions issues de l'Arrangement de Wassenaar qui lui impose de contrôler l'exportation de tous les produits de chiffrement ayant une taille de clé symétrique supérieure à 56 bits.

Mais cette libéralisation du régime des moyens cryptologiques ne s'est pas traduite pour autant par un développement rapide de leur usage par les consommateurs, voire même par les entreprises. En effet, tant s'agissant des systèmes d'authentification et de signature que des produits de chiffrement assurant la confidentialité des données, des problématiques différentes ont longtemps freiné leur essor.

Des services de confiance mieux encadrés

L'utilisation de la cryptographie asymétrique (dite à clé publique) pour des fonctions d'authentification et de contrôle d'intégrité a donné naissance à des applications de signature électronique, capables de certifier à la fois l'identité du signataire et l'absence d'altération du document signé. Sur cette base technique, de nombreux pays – et particulièrement ceux de l'Union européenne – ont construit une législation donnant force juridique aux engagements contractuels et aux documents signés électroniquement. C'est ainsi que la directive européenne du 13 décembre 1999 a institué un cadre juridique harmonisé pour les signatures électroniques, entraînant derrière elle les États-membres.

C'est ainsi que la France fut l'un des premiers à modifier son vénérable Code civil en adoptant le 13 mars 2000 une loi consacrant l'assimilation d'une preuve électronique à la preuve littérale par écrit exigée par le droit civil et prévoyant la possibilité, sous certaines conditions techniques, de reconnaître à une signature électronique les effets d'une signature manuscrite. Son décret d'application du 30 mars 2001 et différents arrêtés d'application complétèrent ce dispositif et précisèrent (conformément à la directive) les exigences techniques et méthodologiques en la matière : notamment le caractère sécurisé de la signature et des moyens logiques et physiques mis en œuvre, ainsi que le recours à un certificat électronique qualifié.

Cette révolution juridique aurait dû induire une révolution des usages, en favorisant

notamment la dématérialisation de nombreuses pratiques contractuelles ou encore en poussant les prestataires de services en ligne à recourir à des moyens de signature pour renforcer l'authentification de leurs usagers et le contrôle d'accès à leurs services. À l'exception de quelques applications professionnelles dans des secteurs spécifiques (par exemple l'authentification des avocats pour accéder à l'échange dématérialisé avec les tribunaux, ou encore la signature par les notaires d'actes authentiques électroniques), ces avancées juridiques restèrent largement sous-utilisées.

Plusieurs raisons se sont sans doute conjuguées pour cela : un niveau d'exigences trop élevé en matière de sécurisation des dispositifs de signature, le manque de standardisation et d'interopérabilité entre les différentes solutions, le coût des procédures de certification ou encore l'existence de solutions alternatives pour gérer la preuve dans un univers dématérialisé[2].

(2) Par exemple par le recours à une « convention de preuve » permettant d'organiser contractuellement un régime probatoire entre les parties à une transaction sans recourir à la signature électronique.

Toujours est-il qu'après quinze ans d'application plutôt décevante de la directive de 1999, l'Union européenne l'a abrogée et lui a substitué le règlement du 23 juillet 2014 sur l'identification électronique et les services de confiance. Souhaitant faciliter aux citoyens européens l'accès transfrontalier aux services numériques (et donc leur éviter d'être confrontés à des exigences d'authentification nationales divergentes), le législateur européen a instauré non seulement un mécanisme de reconnaissance mutuelle des schémas d'identification électronique nationaux mais aussi un régime juridique couvrant différents « services de confiance », dont celui de certification électronique et de signature (auquel s'ajoutent l'horodatage, le cachet électronique ou encore le recommandé électronique et l'authentification de site Internet).

A cette occasion, le nouveau règlement a opéré, discrètement mais sûrement, un important glissement. Alors que la directive de 1999 reposait sur une logique très libérale qui présumait que la seule initiative privée ferait émerger des prestataires de service de certification et des services de signature efficaces (ce qui n'a finalement pas été le cas), le nouveau texte soumet tous les nouveaux services de confiance au contrôle obligatoire de l'autorité nationale de sécurité (en France l'ANSSI). Il est un contrôle *a priori* s'agissant des prestataires de services qualifiés[3] et un contrôle a posteriori pour les prestataires de services non qualifiés qui feraient l'objet de réclamations[4]. De la seule (et apparemment inefficace, en l'espèce) régulation par le marché, nous voici

(3) Articles 17 et 20 du règlement.

(4) Article 17.2 (b).

Un contrôle qui est passé de la sphère libérale du marché à une compétence publique de souveraineté numérique.

passés à un encadrement par les autorités nationales de sécurité, ce qui paraît plus cohérent avec le fait que ce sont ces mêmes services de confiance qui contribuent ensuite à l'authentification des usagers auprès des services publics en ligne.

On peut donc espérer que ce nouveau cadre, plus directement contraignant puisqu'il repose sur un règlement et non sur la transposition d'une directive, va entraîner le développement d'une offre de produits et de services qui sécuriseront l'identité numérique des personnes et des entreprises.

Pour autant – et comme le relève justement le règlement[5] – il faudra que l'on conjugue cette identification renforcée avec les légitimes préoccupations de protection des données personnelles. On connaît en effet le paradoxe qui veut qu'un renforcement trop important de l'authentification et de la traçabilité des personnes puisse fragiliser les droits individuels, et plus particulièrement le droit à la vie privée et la protection des données qui y est rattachée[6].

(5) Voir son considérant 11 et son article 5.

(6) Notons d'ailleurs que le législateur a récemment profité de la nouvelle loi relative au renseignement pour rappeler dans le code de la sécurité intérieure la garantie légale du « respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile » (nouvel article L801-1 CSI créé par la loi du 24 juillet 2015).

Les choix nécessaires en faveur d'un bon usage du chiffrement des données

Le paysage est tout à fait différent lorsque l'on se tourne vers les technologies de

chiffrement. Par nature, celles-ci sont considérées comme pouvant apporter une garantie technique efficace aux préoccupations de données personnelles et de protection des secrets (qu'ils soient d'ordre privé, économique, voire d'intérêt public). C'est au contraire leur capacité à rendre moins détectables les personnes et les transactions qui suscite encore des inquiétudes liées aux impératifs de répression pénale ou de sécurité nationale. Pourtant là encore, nous pensons que les évolutions technologiques et politiques de ces dernières années rendent incontournable des choix forts.

On sait que les États occidentaux ont longtemps cherché à confiner l'utilisation des moyens de chiffrement à certains acteurs régaliens ou à certaines entreprises très exposées à la concurrence internationale, tout en s'efforçant d'en limiter la diffusion sur le marché et dans le public. Ce fut, comme on l'a dit, le cas de la France qui a maintenu ces technologies sous un strict contrôle national (en les soumettant à autorisation, au-delà d'un certain niveau de taille de clés symétriques : 40 puis 128 bits), laissant ainsi du temps aux services spécialisés français pour se doter de moyens de cryptanalyse en relation avec les nouvelles capacités de calcul que la micro-informatique et les équipements mobiles mis à la portée du plus grand nombre.

Ce fut plus encore l'objet des efforts incessants des agences fédérales américaines dans une lutte d'autant plus ardue que les États-Unis sont la nation leader des technologies de l'information et que leur Constitution consacre dans son 1er amendement le droit au « *free speech* »(7). On se souvient en particulier des annonces officielles par la Maison-Blanche du projet Clipper Chip en 1993-1994, basé sur un composant spécial de chiffrement qui aurait permis aux autorités fédérales d'accéder aux données en clair pour les besoins des enquêtes judiciaires ou de la sécurité nationale des États-Unis(8). C'est aussi la National Security Agency (NSA) qui avait convaincu l'organisme fédéral de normalisation (NIST) de standardiser une version de l'algorithme de chiffrement DES à 56 bits plutôt que dans sa version d'origine plus puissante à 64 bits.

Plus encore, ce sont les révélations de Richard Snowden en 2013 qui ont montré à quel point la NSA avait agi de manière détournée pour tenter par tous les moyens de réduire la puissance de

(7) Pour une décision judiciaire américaine emblématique de l'opposition entre les intérêts de sécurité nationale (en l'espèce, issus des réglementations ITAR traitant du commerce des matériels de guerre) et la liberté d'information s'agissant de la divulgation d'un algorithme de chiffrement, voir la décision Bernstein v. US DoJ, Cour fédérale du 9ème circuit, n° 97-16686 du 5 juin 1999 (http://www.eff.org/files/filenode/bernstein/19990506_circuit_decision.html).

(8) Pour une critique américaine du projet par un des grands cryptologues américains, voir W. Diffie, The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology, 11 mai 1993 (http://www.epic.org/crypto/

chiffrement des produits utilisés sur le marché. Suspectée d'avoir manipulé les équipes du NIST, la NSA a, par exemple, été très directement montrée du doigt dans un rapport rédigé par une équipe d'experts réunis par le NIST qui a révélé notamment ses efforts pour standardiser un algorithme cryptographique Dual_EC_DRBG qui comportait une fragilité secrète[9].

(9) NIST Cryptographic Standards and Guidelines Development Process Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology, Juillet 2014 (http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf)

L'ampleur de ces pratiques visant à réduire les capacités de chiffrement des usagers et des entreprises au seul bénéfice des moyens d'interception des services de renseignement a créé un doute immense dans l'opinion et a révélé l'ambiguïté fondamentale qu'il y avait à confier à la même entité la protection de la sécurité informatique et le travail de renseignement technique et de cryptanalyse (ce qui est le cas de la NSA, comme du GCHQ britannique, mais qui n'existe pas en France où l'ANSSI assure la cybersécurité sans être impliquée dans la cryptanalyse offensive).

Cela conduisit le groupe de travail réuni par le Président Obama après le scandale Snowden à recommander le soutien à la création de standards de chiffrement, l'abandon de toute tentative de fragiliser les moyens de chiffrement disponibles sur le marché et de « *promouvoir un usage plus important du chiffrement qu'il s'agisse des données en transit ou stockées dans le cloud ou dans des serveurs* »[10].

(10) Liberty and Security In a Changing World – Report and Recommandations of the President's Review Group on Intelligence and Communications Technologies, 12 décembre 2013, p. 22.

Plus généralement, les organisations internationales et les mouvements de défense des droits civiques commencent à considérer la capacité de chiffrer comme l'un des moyens de préserver non seulement la vie privée des citoyens mais plus encore la liberté d'expression et de communication. C'est dans ce sens qu'un récent rapport du rapporteur spécial pour la promotion et la protection du droit à la liberté de l'information, David Kaye, a été publié par les Nations-Unies en mai 2015[11]. Il recommande en particulier que les États mettent en place des politiques favorables à l'usage du chiffrement et des techniques d'anonymisation et qu'ils « *n'adoptent des restrictions que sur la base d'une analyse au cas par cas et qui satisfasse à des impératifs de légalité, de nécessité, de proportionnalité et de légitimité des objectifs poursuivis* ».

(11) David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ONU, Conseil des droits humains, 39e session, 22 mai 2015.

On peut en effet considérer aujourd'hui qu'il existe des menaces majeures qui nécessitent de promouvoir activement une pratique usuelle du chiffrement : risque de captation et de réutilisation indue des données personnelles (plus

particulièrement par les plateformes et autres intermédiaires du Net), risque d'espionnage numérique pratiqué par les services étrangers ou par des officines privées agissant notamment à des fins de concurrence économique déloyale ou de fraude cybercriminelle, mais encore utilisation des technologies de surveillance massive pour réduire les libertés démocratiques (en particulier dans les États autoritaires). Il faut également prendre en compte que des systèmes d'information ne préservant pas fortement la confidentialité de leurs données internes de configuration (mots de passe, fichiers de contrôle des accès, …) constituent autant de failles individuelles qui contribuent à fragiliser la sécurité des réseaux et à propager toutes sortes de vecteurs d'insécurité numérique.

Le recours à des moyens de chiffrement est devenu d'autant plus nécessaire que le *cloud computing* engendre une perte de maîtrise des données, qu'elles soient personnelles ou professionnelles. Abandonnant le contrôle physique de ses ressources d'information, l'usager doit pouvoir les protéger davantage en en renforçant la sécurité intrinsèque. Dès lors le chiffrement et le contrôle d'intégrité s'imposent comme réponses indispensables aux risques intrinsèques de l'externalisation de l'information dans le nuage.

Face à ces exigences de cybersécurité mais aussi de protection des libertés fondamentales, on constate une réaction surprenante mais révélatrice de certains responsables du renseignement et des enquêtes judiciaires. Dans leur article du New York Times d'août 2015, visiblement piloté par le procureur new-yorkais C. Vance qui l'a contresigné, son homologue de Paris ainsi que le procureur de la Cour suprême espagnole et le chef de la police londonienne ont agité le spectre d'une impuissance des autorités judiciaires devant le chiffrement des données stockées sur les smartphones[12]. Au-delà du caractère assez caricatural des arguments et des exemples invoqués, cet article manifeste plus une manœuvre de lobbying (pour influer unilatéralement sur la décision publique) qu'une réflexion d'intérêt général qui effectuerait une véritable balance entre les intérêts publics divergents.

(12) Cyrus R. Vance Jr., François Molins, Adrian Leppard & Javier Zaragoza, « When Phone Encryption Blocks Justice », New-York Times, 11 août 2015.

Or c'est bien de cela qu'il s'agit aujourd'hui. Faut-il pour préserver les capacités de renseignement et d'enquête judiciaire décourager, voire dissuader, les entreprises et les citoyens de rechercher à préserver leurs données et leurs systèmes d'information grâce au chiffrement de leurs communications et de leurs fichiers ? Faut-il considérer que le renforcement de la cybersécurité justifie, au contraire, qu'une politique publique

veille à promouvoir et à normaliser une offre de sécurité de l'information ?

A notre sens, on peut penser qu'entre l'affaiblissement du niveau de sécurité numérique d'un État ou d'une économie et le risque de moindre puissance des outils de renseignement et d'investigation numérique, c'est désormais le second risque qu'il faut accepter d'affronter en s'efforçant d'en limiter les effets (notamment par la poursuite des investissements dans les outils de cryptanalyse, utilisables également par les autorités judiciaires en cas de besoin[13]).

Faire le choix inverse, consistant à désarmer les citoyens et les entreprises face au détournement de leurs données et à l'essor incontrôlé d'applications *big data* très intrusives tout en développant par ailleurs les moyens d'authentification et de traçabilité, reviendrait à instaurer durablement une insécurité numérique qui porterait fortement atteinte à l'équilibre que toute démocratie doit assurer entre la sécurité collective et les droits et libertés individuelles.

(13) Les articles 230-1 et suivants du Code de procédure pénale permettent, s'agissant d'enquêtes sur des infractions punies d'au moins deux ans d'emprisonnement, d'avoir recours « aux moyens de l'État soumis au secret de la défense nationale » (c'est-à-dire à des capacités classifiées de cryptanalyse).

L'AUTEUR

Bertrand WARUSFEL est Professeur de droit à l'Université de Lille (CRDP-ERDP). Il enseigne notamment le droit des nouvelles technologies et de la sécurité des systèmes d'information. Co-auteur de l'ouvrage Lamy Droit du numérique, il est également avocat au barreau de Paris, administrateur de l'Association française de droit de la sécurité et de la défense (AFDSD) et membre du conseil scientifique de l'INHESJ.

Sécurité et partage des données de santé en milieu hospitalier

par **FRANCIS DAUL**

Note de la rédaction : Le CHRU de Nancy s'est engagé tôt dans un processus de sécurisation et de partage des traitements et des données entre techniciens et praticiens de santé. Francis Daul a bien voulu nous faire part de son expérience en répondant à nos questions.

Quels sont vos principaux objectifs de sécurité pour le système d'information hospitalier ?

Les trois objectifs majeurs de sécurité du système d'information hospitalier sont la disponibilité, l'intégrité et la confidentialité des données. Pour garantir la continuité des soins, les données doivent être disponibles 24h/24, 7j/7 et rapidement accessibles. Depuis la dématérialisation du dossier patient, le praticien s'appuyant désormais sur le système d'information pour la prise en charge de son patient, il doit avoir l'assurance que les données sont fiables. La donnée de santé fait partie du domaine de la vie privée (article 9 du code civil « *Chacun a droit au respect de sa vie privée* »). Elle est protégée par le secret professionnel (ou secret médical), confidentielle, sensible et exige une protection renforcée. La violation du secret médical est punie d'un an d'emprisonnement et de 15 000 euros d'amende (code pénal article 226-13).

FRANCIS DAUL

Ingénieur
Responsable d'Exploitation
Direction du Système d'Information - CHRU Nancy

Au-delà des indispensables logiciels et matériels de sécurité, la sécurité des données impose une démarche qualité permanente qui nécessite l'information, la sensibilisation et l'implication de tous les professionnels de santé.

Romolo Tavani - fotolia.com

L'architecture des systèmes informatiques de santé doit concilier le partage des données entre praticiens et le respect de données privées.

Comment gérez-vous les droits d'accès au système d'information hospitalier ?

L'accès aux données personnelles de santé doit être restreint à l'équipe de soins qui prend en charge le patient pour une pathologie ou un épisode de soins. La prise en charge des patients est souvent multidisciplinaire, en particulier en milieu hospitalier (service d'imagerie, laboratoire de biologie, plateaux techniques comme les blocs opératoires, services de soins). Réussir à concilier l'obligation de respect de la confidentialité des données avec leur partage qui est essentiel pour la coordination des soins nécessite, sur le plan technique, l'octroi de droits d'accès conformes à l'activité des professionnels de santé et à leur affectation au sein de l'établissement.

Bien entendu, les droits d'accès ne doivent en aucun cas entraver les soins, c'est pourquoi les procédures de « *bris de glace* » permettent en cas d'urgence d'attribuer des autorisations temporaires. Ces « *bris de glace* », comme tous les accès aux données, sont tracés puis analysés.

Dans notre établissement hospitalier, qui compte 9 000 employés et huit hôpitaux répartis sur deux sites, les mouvements de personnel sont nombreux, notamment du fait de l'activité universitaire. Cela nécessite une gestion des accès centralisée et automatisée.

Le CHRU de NANCY a été pionnier dans la mise en œuvre d'un IAM (*Identity Access Management*) en milieu hospitalier : dès 2006, le CHRU s'est engagé dans un projet de constitution

d'un annuaire central d'identités, alimenté directement par les logiciels de gestion des ressources humaines et de gestion de la structure de l'hôpital.

Cet annuaire utilise les modèles RBAC (*Role Based Access Control* : modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès repose sur le rôle que l'utilisateur joue dans l'entreprise) et OrBAC (*Organization Based Access Control* : c'est un modèle qui est basé sur l'organisation de l'entreprise).

Ainsi les droits d'accès sont attribués sur deux critères, le rôle ou le métier du professionnel de santé et son affectation au sein de l'établissement. C'est ensuite un méta-annuaire qui provisionne les comptes et autorisations d'accès dans les différents logiciels du système d'information.

Ce système centralisé permet la création, la modification et la suppression automatique des comptes et autorisations dès que le mouvement du personnel est acté dans le logiciel de gestion des ressources humaines. Bien entendu, ce système ne peut alimenter que les logiciels métier compatibles avec le provisionnement automatique des comptes et autorisations. Nous travaillons avec les éditeurs pour faire évoluer leur logiciel dans ce sens.

Enfin, des revues (contrôles) de droits d'accès sont réalisées régulièrement.

Comment authentifiez-vous les utilisateurs ?

En 2010, le CHRU a mis en œuvre sa carte d'établissement multiservices qui permet le passage des barrières, l'accès aux locaux, l'accès aux distributeurs automatiques de vêtements, l'accès à la fonction monétique pour les selfs, les distributeurs de repas et bien sûr l'accès au système d'information hospitalier. Ces cartes personnalisées (elles comportent le nom, le prénom, la photo et la fonction de l'agent) intègrent plusieurs technologies pour être compatibles avec les différents systèmes d'accès. Pour les connexions depuis l'extérieur du CHRU nous déployons une solution de type OTP (*One-time password*).

Quels sont les partenaires extérieurs avec lesquels vous échangez des données et comment sécurisez-vous ces échanges ?

Il faut rappeler tout d'abord une règle générale et essentielle : tout partage de données de santé nécessite l'accord préalable du patient, qui doit être informé et peut s'opposer à ces transmissions d'informations.

L'évolution de l'hôpital (diminution de la durée d'hospitalisation, augmentation de l'activité de soins ambulatoires) impose le développement de l'interopérabilité du système hospitalier avec les partenaires du CHRU pour accompagner le parcours du patient.

Le SIH communique en permanence avec les partenaires institutionnels du CHRU (l'Établissement français du sang, l'Observatoire régional des urgences, la Caisse pPrimaire d'assurance maladie, les différentes mutuelles, la Trésorerie générale, etc.), les médecins de ville et le Dossier Médical Personnel. La mise en œuvre prochaine des Groupements hospitaliers de territoire (GHT) développera cette interopérabilité entre tous les établissements qui leur sont rattachés pour atteindre l'objectif d'un système d'information convergent. Pour ses échanges, le CHRU a fait le choix de la solution ENOVACOM suite V2 qui lui permet de tracer, sécuriser (Identification, Authentification, Signature, Chiffrement, Gestion des habilitations) et modéliser ses processus d'échanges.

Concernant les échanges avec la médecine de ville, nous utilisons essentiellement deux systèmes de messagerie sécurisée :

- Apicryt, qui est historiquement le système de messagerie médicale sécurisée le plus utilisé par les médecins de ville dans notre région.

- MSSanté : l'ASIP Santé, en collaboration avec les Ordres des professionnels de Santé (médecins, pharmaciens, chirurgiens-dentistes, sages-femmes, masseurs-kinésithérapeutes, pédicures podologues) a initié un projet de messagerie sécurisée de santé nationale afin de faciliter les échanges sécurisés entre les professionnels de Santé. Le CHRU de Nancy déploie l'architecture nécessaire pour être également opérateur de la messagerie MSSanté.

Le dossier patient informatisé est interconnecté à ces deux messageries pour l'envoi de courriers aux médecins traitants.

Comment gérez-vous la traçabilité des accès et actions sur le système d'information hospitalier ?

De l'appel du patient au SAMU jusqu'à l'administration du médicament, l'essentiel des actes hospitaliers est tracé dans le système d'information. Les traces d'accès et actions produites par les différents logiciels sont archivées. Elles sont restituées à la demande, notamment dans le cas d'un recours légal.

Face au nombre important d'événements générés par l'ensemble des composants du système d'information, les hôpitaux se dotent d'outils qui permettent de les collecter, les archiver, les gérer et les corréler. Ces outils type SIEM (Security Information and Event Management) sont munis de moteurs de corrélation qui permettent de relier plusieurs événements qui conduisent à l'ouverture d'un incident de sécurité et à l'alerte du Responsable de la sécurité du système d'information et du correspondant informatique et libertés.

Quelles sont les démarches qualité en cours qui contribuent à l'amélioration de la sécurité du système d'information hospitalier ?

Dès 2007, la Direction du Système d'Information s'est engagée dans une démarche qualité qui repose sur le

référentiel des bonnes pratiques ITIL[1]. Cinq processus ont été démarrés : la gestion des incidents, des problèmes, des changements, des configurations et la gestion des niveaux de services. Tous ces processus contribuent fortement à la disponibilité et l'intégrité des données.

(1) ITIL (Information Technology Infrastructure Library pour "Bibliothèque pour l'infrastructure des technologies de l'information") est un ensemble d'ouvrages recensant les bonnes pratiques ("best practices") pour la gestion des services informatiques (ITSM), édictées par l'Office public britannique du Commerce (OGC). L'adoption des bonnes pratiques de l'ITIL par une entreprise ou par une collectivité lui permet d'assurer à ses clients (internes comme externes) un service répondant à des normes de qualité préétablies au niveau international. C'est donc un label de qualité proche des normes de l'ISO.

(2) http://www.has-sante.fr/portail/jcms/fc_1249882/fr/certification-des-etablissements-de-sante

Par ailleurs, plusieurs démarches qualité, la certification des comptes, le programme hôpital numérique, la certification HAS[2], l'agrément d'hébergeur de données de santé qui sont impulsées par la Haute autorité de santé, l'Agence des systèmes d'information partagés de santé et les Agences régionales de santé contribuent à l'amélioration de la qualité et de la sécurité. Ces démarches, qui sont toutes convergentes, conduisent à uniformiser les pratiques professionnelles, à formaliser les procédures et mode opératoires, à organiser les audits réguliers et à produire les indicateurs de qualité et d'activité qui permettent de mesurer l'efficience du système d'information hospitalier.

L'analyse permet d'identifier les situations à risques et de prioriser les actions qui permettront d'en minimiser l'impact sur le système d'information. L'analyse de risque est imposée par la loi informatique et libertés (article 30). Nous nous appuyons sur EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) développée par l'Agence Nationale de la Sécurité des Systèmes d'information qui est l'une des méthodes la plus répandue.

Notre système d'information hospitalier compte plus de 200 briques applicatives (logiciels). Le logiciel étant au cœur du système d'information, il est difficile d'assurer la sécurité des données sans le concours des éditeurs qui doivent produire des logiciels conformes aux exigences de disponibilité, d'intégrité et de confidentialité.

Depuis 2013 l'Agence des systèmes d'information partagés de santé travaille à l'élaboration d'un référentiel de certification des logiciels destinés aux hôpitaux. En 2015, la publication du référentiel de qualité hôpital numérique (issu d'un travail collaboratif entre les fédérations hospitalières, les industriels du secteur, l'Agence Nationale d'Appui à la Performance, le COFRAC - Comité français d'accréditation - et les représentants des organismes certificateurs) et l'ouverture du guichet de certification qualité hôpital numérique constituent une avancée considérable pour la qualité des logiciels hospitaliers.

Comment garantissez-vous la disponibilité de la donnée ?

Pour se prémunir d'un sinistre ou d'un acte malveillant nous répliquons de façon

synchrone toutes les données critiques entre nos deux Datacenter distants de 7 km et interconnectés par deux chemins de fibre différents. Le dernier recours en cas d'altération d'un système ou d'une base de données reste la sauvegarde. Le CHRU a mis en œuvre un système centralisé de sauvegarde également réparti sur ses deux salles informatiques, toutes les sauvegardes étant également répliquées de façon asynchrone entre les deux sites. Des algorithmes de déduplication des données sauvegardées permettent d'en optimiser le stockage.

Le poste de travail étant la porte d'accès au système d'information, il doit être banalisé pour garantir la disponibilité et la sécurité de l'information. Les données et les processus critiques doivent être hébergés dans les Datacenters.

Qui sont les principaux acteurs impliqués dans la sécurité des données ?

La sécurité du système d'information doit avant tout être une préoccupation pour tous les professionnels de santé. Le personnel hospitalier, dont les informaticiens, doit respecter au quotidien les bonnes pratiques et procédures qui visent à garantir la sécurité du système d'information (renouvellement des mots de passe, verrouillage des sessions, vigilance lors de la navigation sur internet et le relevé de messagerie). Chacun s'engage à respecter ces bonnes pratiques en signant la charte à son arrivée dans l'établissement. L'État est un acteur majeur puisqu'il fixe le cadre de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S).

Au sein de l'établissement, le responsable du traitement reste le garant de l'application de la PGSSI pour son périmètre de responsabilité. Le Responsable de la sécurité des systèmes d'information de l'établissement définit et met en œuvre la politique de sécurité des Systèmes d'information (PSSI), il diagnostique et analyse les risques, sensibilise le personnel, conseille la Direction Générale, organise des audits et contrôle l'application de la PSSI. Il est un partenaire essentiel de la Direction du Système d'Information pour la mise en œuvre et le suivi des démarches qualité. Le Correspondant « Informatique et Libertés » qui a pour mission d'assurer le respect des obligations légales de la loi informatique et libertés, relative au traitement des données à caractère personnel et plus particulièrement des donnés de santé, est également un acteur essentiel pour garantir le droit des patients.

L'AUTEUR

Francis DAUL Ingénieur Responsable d'Exploitation anime la démarche qualité de la Direction du Système d'Information du CHRU de Nancy depuis 2007.
Il développe l'industrialisation de la production et cultive l'approche orientée service en s'appuyant sur le référentiel ITIL (Information Technology Infrastructure Library).

Le consommateur,
victime ou héros des systèmes CRM ?

Entretien avec CHRISTOPHE BOUGEREAU

L'avènement du big data et des objets connectés sonne le glas des interprétations plus ou moins sérieuses sur l'enjeu de la donnée client et de sa sécurité. Désormais il est établi que cette donnée devient un élément constitutif du capital d'une société par les intérêts économiques que son exploitation révèle et ensuite, dans sa dimension sécuritaire, par sa confidentialité. Dans les deux cas la gestion de la relation client qui justifie et qui légitimise au quotidien l'exploitation de la donnée client, est au centre du débat et en cela mérite une analyse critique.

CHRISTOPHE BOUGEREAU

Maitre de conférences associé en marketing relationnel (Université Bretagne Sud IUT) et consultant en stratégie client (Dirigeant fondateur de Maison Du Client)

Maître de conférences associé en marketing relationnel (Université Bretagne Sud IUT) et consultant en stratégie client (Dirigeant fondateur de Maison Du Client), Christophe Bougereau revient pour la revue sur les enjeux d'une solution de Customer Relationship Management[1].

(1) Customer Relationship Management en Anglais (CRM) soit Gestion de la Relation Client (GRC) est une stratégie par laquelle l'entreprise vise à comprendre, à anticiper et à gérer les besoins de ses clients actuels et potentiels.

Revue - La multiplication des programmes relationnels et des initiatives de e-commerce nous invite à revenir sur le principe général de la relation client par solution logicielle. Pouvez-vous nous rappeler le contexte qui a conduit au développement de ces solutions et nous dresser une cartographie des solutions essentielles sur le marché ?

Le commerce a longtemps été associé à la notion réductrice de transactions : le vendeur transmet un message associé à

un produit ou un service avec la volonté de convaincre le plus grand nombre. Cette communication unilatérale, de la marque vers le consommateur, s'appuie sur un postulat fort : la rareté de l'offre au regard d'une demande forte et en croissance. Les années 80/90 et le rééquilibrage « besoin-offre » ont quelque peu corrigé cette vision en introduisant la notion de rapport « qualité/prix ». La mise à disposition d'un produit ne pouvait plus suffire, il fallait désormais que celui-ci respecte des critères attendus par le client. L'idée maîtresse des marques restait cependant fondée sur l'idée que les consommateurs constituaient une cible homogène et passive dans l'attente de la vérité détenue par les marques.

Cette idée est aujourd'hui dépassée, tout au moins pour les économies occidentales, par un état de fait : dans une économie proche de la décroissance, l'offre est à ce jour largement supérieure à la demande. De fait, le produit ou le service ne peut exister que dans la mesure où il s'adresse à une attente identifiée. Aujourd'hui le marketing est bel et bien devenu une affaire de «relations » et les marques qui réussiront dans le futur sont celles qui parviendront à tisser des liens de plus en plus personnels avec leurs clients au travers d'un parcours client spécifique où l'expérience client prendra tout son sens.

Pour aller plus loin il faut s'intéresser aux travaux menés par Procter & Gamble dans les années 90 sur le concept de « moments de vérité ». L'industriel avait alors identifié le FMOT (First Moment Of Truth). Un stimulus (principalement issu des médias classiques comme la télévision) pousse le consommateur vers le magasin. Le premier contact avec le produit ou service qui s'y opère est à l'origine du déclenchement d'une intention d'achat. Cet achat est alors suivi d'un usage : le Second Moment of Truth (SMOT). En 2010, Google rebondit sur cette approche et l'adapte à l'ère digitale en introduisant « le nouveau modèle mental du marketing » : le ZMOT c'est-à-dire le « Zero Moment Of Truth ». Ce moment particulier où le consommateur est en recherche d'information, notamment via les moteurs de recherche et les réseaux sociaux, vient se placer entre le stimulus et le premier contact avec le produit dans un magasin (physique ou en ligne). Simultanément Google a proposé la notion d'UMOT (Ultimate Moment of Truth). Il s'agit dans ce cas du partage sur la toile de l'expérience vécue par le client via notamment les réseaux sociaux.

A cette succession linéaire de moments de vérité, le concept de « Permanent Moment Of Truth » semble aujourd'hui plus pertinent. Les clients sont en permanence susceptibles d'agir, pour ou contre la marque, via des supports proposés par la marque mais également au travers de médias complétement

indépendants, interactifs et accessibles immédiatement, en premier lieu le mobile. Un tel contexte est à rapprocher des situations de crise bien connues dans l'univers de la production industrielle. Comment être en alerte et capter les signaux les plus faibles de façon à proposer la réponse appropriée ? Une solution serait de passer par la mise en place de « Customer Rooms » à l'image des « War Rooms ». Dans ces espaces se cristallisent différentes typologies de clients et de pilotages associés qui embrassent leurs effectifs, leur satisfaction et leur valeur.

Capter ces signaux faibles nécessite une réelle organisation de l'écoute client dans un mode omnicanal. De cette écoute, associée à une capacité de collecte, de tri et d'organisation de l'information pertinente, découlera une création de valeur. Une entreprise qui recueille des données « brutes », quelles que soient les sources, les trie, les exploite et les enrichit. Elle crée de la connaissance client qui donne des opportunités de prises de paroles pertinentes et par conséquent plus efficaces en matière de retours sur investissement. Nous pouvons parler de prises de paroles CCCS : Cohérentes (quel que soit le canal, le discours est le même), Coordonnées (les différentes prises de paroles interagissent de façon à construire une histoire), Convergentes (les différentes informations échangées intègrent un système central comme un datawarehouse) et Synchronisées (partagées en temps réel dans un écosystème informationnel ou système CRM).

Dans le contexte des organisations complexes, la difficulté consiste à collecter et à organiser les données dans une « Customer Data Base » unique alors même que les sources sont potentiellement hétérogènes, non structurées et générées en grande partie par des individus à forte autonomie avec un faible « référentiel commun ». L'enjeu est essentiellement organisationnel et managérial. Cet entrepôt de données doit bénéficier d'une alimentation croisée avec les autres briques du système CRM : l'outil de relation commercial (le terminal de paiement en boutique ou la tablette pour les commerciaux), l'outil de centre de contact (les échanges à distances), l'outil de gestion automatique des campagnes marketing (Electronic Marketing Automation) et les outils analytiques et de reporting (Datamining).

Revue : Dans ce contexte quelles sont les opportunités et enjeux du Big Data

Pour améliorer leur connaissance client et notamment appréhender le vécu client dans le cadre de son parcours d'achat, les entreprises s'intéressent de plus en plus aux données externes : les conversations sur le web, les commentaires rédigés sur les sites d'avis,

sur les forums de discussions, sur les réseaux sociaux. Ces données externes constituent une grande partie du Big Data et sont potentiellement riches d'expériences racontées de façon spontanée.

Face à cette profusion d'informations non structurées, l'entreprise peut être mise en difficulté. Ainsi le principal enjeu du big data, c'est d'être capable de faire le tri parmi toutes les données disponibles : mieux vaut 5.000 commentaires correctement qualifiés plutôt que 100.000 inexploitables car hors sujet. Pour cela il convient de prendre de la hauteur et de hiérarchiser les enjeux et les priorités.

Consolider l'ensemble des informations aisément accessibles constitue la première étape d'une approche globale qui pourra s'ouvrir à d'autres sources d'information d'un omnicanal élargi aux réseaux sociaux. Pour l'entreprise, l'enjeu consiste à ne pas se disperser en se concentrant sur son cœur de métier et en favorisant une vision claire des étapes successives.

Cette connaissance client sera profitable par la suite tout au long du processus relationnel. À titre d'illustration, Arnaud Bouchard, directeur associé en charge de l'entité «expérience client» chez Cap Gemini Consulting, a mis en évidence les plaintes des internautes du fait de la non prise en compte de la connaissance client dans les programmes de fidélité. Si les consommateurs veulent toujours que leur fidélité soit récompensée, ils ont surtout besoin de «reconnaissance» et à ce titre réclament une vraie interaction avec la marque. Les marques doivent donc apprendre à considérer les engagements affichés sur les réseaux sociaux, les commentaires sur les produits achetés, le nombre de visites dans un magasin, les réponses aux questionnaires de satisfaction ou encore le téléchargement d'une application pour smartphone. La data ainsi partagée constitue pour le client une opportunité d'être pris personnellement en compte par l'entreprise et par conséquent de recevoir des offres personnalisées. En partageant une partie de ses données personnelles, le client devient héros du système CRM.

Le dispositif relationnel devenu très complexe nécessite d'être dorénavant piloté et organisé autour de solutions logicielles globales intégrant quasi nativement toutes les dimensions d'un CRM. Sur ce terrain les 4 leaders (Salesforce, Oracle, Microsoft et SAP) ont ces dernières années consolidé leur place et distancent largement les autres solutions qui se distinguent généralement sur des niches de métiers en intégrant des spécificités ignorées jusqu'à maintenant par les généralistes.

Revue - Pouvez-vous mentionner les intérêts pour une entreprise de bénéficier de cette solution ?

Les solutions logicielles ont pour objectif de placer la donnée client au cœur du système d'information. Elles visent une parfaite connaissance des clients, de leur profil, de leur valeur de manière à mieux identifier leurs besoins et développer des démarches sécurisées en matière de commerce, de communication, de fidélisation et de prospection. Les autres impacts constatés de ces outils sont généralement la facilité d'usage et les gains de productivité.

Un système CRM performant permet de développer au sein de l'entreprise une approche transversale où les échanges seront faciles et sécurisés. Échanges vers l'externe bien évidemment mais également en interne de façon à s'assurer du respect de la confidentialité de certaines données. À ce titre, la maîtrise du portefeuille clients d'une entreprise est un acte crucial non négociable et les stratégies de différenciation et de personnalisation voulues par les entreprises en renforcent la nécessité.

Collecter et organiser la donnée permet de créer de la connaissance client et assure un avantage concurrentiel pour tous ceux qui sont en mesure d'exploiter intelligemment cette information. Pour autant, il ne s'agit pas de confondre outil et stratégie. Le système CRM n'est qu'un ensemble d'outils. Certes très performants s'ils sont bien intégrés, ils ne construisent pas de parcours client et identifient encore moins les moments de vérité.

Par conséquent, pour créer une véritable valeur ajoutée et éviter l'arrêt de tels projets, l'entreprise doit, précédemment à tout choix technique, formaliser expressément ses besoins métiers ainsi que les enjeux réglementaires et sécuritaires associés. En cela la solution logicielle impacte directement les dimensions organisationnelles et les processus métiers.

Revue : La collecte des informations personnelles dans le cadre d'un CRM est-elle sécurisable ? Le risque n'est-il pas de faire du client une victime du CRM ?

Il faut garder à l'esprit que tout système informatique peut être « hacké », piraté (Tanguy de Coatpont, directeur général de Kaspersky Lab France et Afrique du Nord). Dès qu'un système informatique est, d'une manière ou d'une autre, connecté à internet ou à un autre réseau informatique, des individus malveillants peuvent y pénétrer et y dérober des informations. Toutefois ces actes de piraterie nécessitent un véritable investissement (connaissance informatique et moyens humains) que ne justifie pas nécessairement une base de connaissance client.

Même si comme nous venons de le voir, la force et la puissance d'une solution logicielle de relation client résident dans sa capacité à exploiter un maximum de données, il faut relativiser les risques. D'un point de vue des systèmes CRM et des sécurités associées, il faut veiller à distinguer les données pertinentes d'un point de vue marketing ventes, destinées à être conservées et valorisées dans le temps, des données transactionnelles (au premier rang desquels figurent les comptes bancaires) qui doivent eux faire l'objet d'une exploitation momentanée, réglementée et associée à une sécurité normalisée.

A ce stade, l'entreprise doit être en mesure de calibrer le niveau de criticité de ses différentes données et des applications associées. Pour cela, elle doit être capable d'estimer l'impact financier que pourrait avoir un sinistre ou un incident sérieux et le degré de probabilité qu'il survienne. En fonction des niveaux de risques ainsi établis, il faut alors proposer des niveaux de sécurité appropriés, donc différents, selon les usages. C'est la bonne voie pour trouver l'équilibre entre une sécurisation indispensable de certaines données et une exploitation de la connaissance client nécessaire au développement d'une relation client de plus en plus individualisée et personnalisée.

L'explosion des datas associée à la généralisation de solutions logicielles « cloud » invite bien évidemment à un examen critique de la sécurité des données, mais d'un point de vue stratégie d'entreprise c'est la pertinence même de cette accumulation qui doit être challengée. Sans stratégie, sans vision, il n'est pas nécessaire d'investir dans des solutions logicielles coûteuses car parfois le bon sens et le pragmatisme peuvent suffire.

D'un point de vue client, le risque est un usage maladroit et non respectueux par l'entreprise de ses données qui conduirait par exemple à une sursollicitation commerciale. Devenu victime de ces solutions, le client serait amené à prendre des décisions drastiques qui mettraient en cause la rentabilité même du dispositif relationnel mis en place.

Une solution logicielle CRM doit, de fait, être considérée comme une opportunité dans l'installation d'une relation bienveillante, respectueuse et pérenne entre l'entreprise et ses clients.

LEAPS, 1er programme d'incubation et d'accélération dédié à la cybersécurité

par CAROLINE LIMER

LEAPS, Lille Euratechnologies Acceleration Program for Security, a pour vocation d'accélérer la création et le développement de startups sur un marché de la cybersécurité en pleine expansion, et, par-delà, participer à positionner l'Europe comme leader sur ces enjeux majeurs de société.

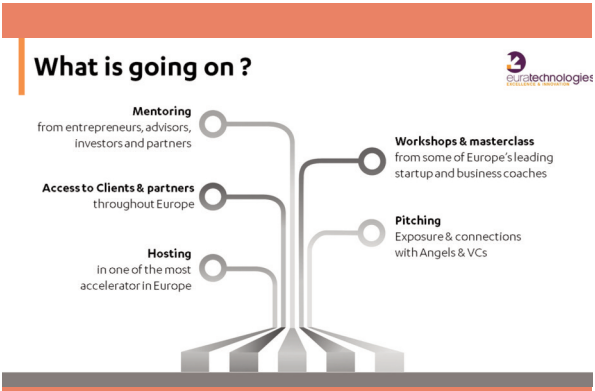
L'idée est partie d'un constat simple : sur 10 projets rejoignant un incubateur ou un accélérateur en France, combien aujourd'hui ciblent le marché de la cybersécurité et de la confiance numérique ? Estimé à 155,74 milliards de dollars en 2019 par Markets & Markets, trop peu d'entrepreneurs choisissent ce secteur en pleine croissance. Pourtant, les failles informatiques se multiplient et font apparaitre la nécessité de développer des solutions sur ce marché, pour les entreprises comme pour les particuliers.

CAROLE LYMER
Euratechnologies

Une filière en plein essor

« *L'industrie européenne de la Confiance Numérique est toujours en émergence face aux leaders déjà confirmés venus d'autres continents, comme les Etats-Unis et Israël. Cette filière est composée d'une pléiade de petites et moyennes entreprises qui peinent à atteindre une taille critique. Nos entreprises développent souvent des produits très innovants pour lesquels la mise sur le marché peut être laborieuse et difficile.* » Pierre Calais, CEO/Président at Stormshield.

Ce phénomène s'explique en partie par l'absence d'un écosystème favorable au développement de ces entreprises : les structures d'accompagnement rompues aux enjeux de cybersécurité sont bien moins nombreuses que sur d'autres marchés comme le web ou



Un objectif : l'émergence de success stories.

l'e-commerce par exemple. En Israël, c'est tout un écosystème qui s'est structuré autour de tech-champions : incubateurs, accélérateurs, fonds d'investissements, centres de recherche et universités, sans oublier le soutien gouvernemental et les collaborations avec les grands groupes etc. Les relations et les interconnexions inter-entreprises sur le territoire sont primordiales et sont à l'origine de nombreuses externalités positives : les synergies y sont stimulées, les mises en relations sont simplifiées et les partages d'expériences favorisés.

Une filière aux besoins spécifiques

L'avènement de leaders européens nécessite de former toutes les compétences liées au développement de leur business : marketing, communication, commercial, etc. de façon à booster la mise sur le marché de produits développés. On ne communique pas sur des produits de « *confiance numérique* » comme on le ferait sur d'autres produits.

Par ailleurs, les entreprises doivent également pouvoir trouver les financements, clef de voûte essentielle à leur développement. Depuis le début de l'année, les levées de fonds dans le secteur s'enchainent partout dans le monde, signe de la vitalité d'un marché estimé à 170 milliards de dollars en 2020[1]. En août dernier, la startup Tanium finalisait une levée de près de 120 millions de dollars auprès d'investisseurs américains : combien de startups peuvent espérer lever de tels fonds en Europe ?

(1) Markets&Markets

Conscients de la valeur des produits et services développés par les entreprises du secteur, les investisseurs européens commencent à se positionner et un réel mouvement de structuration du marché est en marche. Ce mouvement prendra probablement quelques années encore pour être réellement abouti.

Enfin, la filière de la cybersécurité doit opérer un changement d'image pour pouvoir attirer les nouvelles générations. A tous les niveaux et postes, la cybersécurité peine à recruter. Si ce

phénomène est en partie dû à une croissance importante des entreprises et donc un nombre de recrutements supérieur aux nombres de diplômés, la richesse des métiers proposés est souvent méconnue. Le constat s'applique également aux entrepreneurs.

LEAPS : Le tremplin pour accélérer son business en Europe

Conscient de ces enjeux, EuraTechnologies souhaite accompagner le développement de leaders européens de la Cybersécurité à travers un programme d'accompagnement unique en France.

« *Nous souhaitons montrer à tous ceux qui envisagent de créer une startup que la cybersécurité est un marché stratégique tout en étant accessible. Le développement de produits innovants adaptés aux usages est essentiel pour accompagner la transformation digitale de notre société toute entière. Le numérique est une chance pour tous seulement si on assure les conditions de la confiance. C'est pour ces raisons que nous lançons le programme d'accélération LEAPS.* » Raouti CHEHIH, Directeur Général d'EuraTechnologies

LEAPS c'est avant tout une promesse : celle de se développer dans plusieurs pays européens en peu de temps. Il vise à faciliter cette étape et soutenir ainsi l'européanisation de la filière. L'internationalisation est souvent une étape cruciale pour l'évolution d'une entreprise. LEAPS a pour vocation de susciter des vocations et l'envie d'entreprendre dans la cybersécurité, mais également d'attirer en France ou en Europe des startups prometteuses qui souhaitent s'y développer. Les utilisateurs, que ce soient des entreprises, des administrations ou le grand public, pourront choisir des solutions européennes pour assurer leur sécurité numérique.

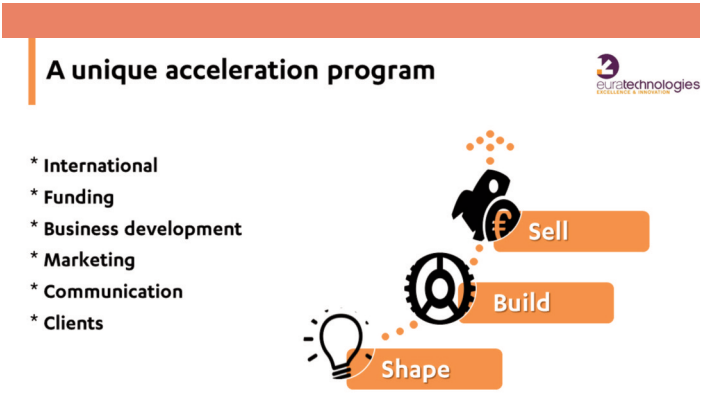
Le Nord-Pas de Calais haut lieu de la « confiance numérique »

Enfin, LEAPS permet à EuraTechnologies de capitaliser et de mettre au profit des startups l'expertise et savoir-faire acquis grâce à l'animation de la filière régionale de la Cybersécurité, à travers le ClusterCN&CS, et la co-organisation de plusieurs FIC.

La région Nord-Pas de Calais est devenue en quelques années un véritable hub de la Cybersécurité en France et dans une partie de l'Europe. Les jeunes pousses, accompagnées par LEAPS, trouveront à Lille le soutien d'une filière dense et dynamique. De nombreuses entreprises du ClusterCN&CS se sont d'ailleurs positionnées pour apporter leurs compétences et solutions aux jeunes pousses qui intègrent EuraTechnologies.

La méthode

Suite à un process de sélection basé sur des critères aussi variés que l'offre de



Un objectif : l'émergence de success stories.

produits ou de services, le marché, la technologie, le positionnement concurrentiel, le modèle économique, l'équipe, les prévisions financières, l'état d'avancement du projet est réalisé grâce au soutien d'un jury de professionnels.

En 90 jours, les startups sont challengées sur tous les aspects de leur stratégie d'entreprise et confrontées à des feedbacks d'experts et d'utilisateurs basés partout en Europe. Du « *product market fit* » à la stratégie RH, les participants seront invités à aller au bout de leur projet. Le programme réuni de prestigieux experts internationaux du business de la cybersécurité qui mettront à profit leurs track-records au profit de 5 startups de la première promotion du programme, issues de différents pays d'Europe.

Originaires d'Europe et des Etats Unis, les mentors viendront du monde entier pour accompagner les participants à travers des workshops, boot camps, formations, pitching…

La domotique ou une connectivité à maîtriser

par **PIERRE PERGET**

Le paradigme du domicile privé, par essence inviolable selon le droit à valeur constitutionnelle, est bouleversé par l'intégration dans l'habitat d'une ouverture sur le monde par la connectivité.

La domotique concerne les techniques d'intégration dans l'habitat d'automatismes en matière de sécurité, de gestion de l'énergie, de communication, etc. Elle est aujourd'hui simple à installer, interopérable et évolutive. Elle rend l'utilisateur autonome et totalement maître de sa maison. Le marché est en pleine expansion et concerne désormais un public non-initié. La domotique ne peut plus se distinguer des objets connectés qui la composent. Les applications dépassent la seule notion de confort car la sécurité des personnes et des biens en constitue, par essence, une finalité.

PIERRE PERGET
Lieutenant de Gendarmerie, commandant la brigade de recherche de Lunel

Les fonctionnalités de l'habitat intelligent se diversifient au gré des évolutions technologiques mais elles ne sont pas sans risques pour les utilisateurs. Elles suscitent une adaptation du droit compte tenu du risque de contentieux, notamment lié à l'accroissement exponentiel du nombre d'objets connectés.

Des applications davantage limitées par l'imagination que par des contraintes techniques

Dans cette partie, nous développerons quelques applications relatives à la vie quotidienne

La lutte contre les appropriations frauduleuses

En 2014, l'ONDRP[1] recense 15 978 faits constatés de vols simples sur chantiers. Ce constat alarmant incite

fotolia.com

Une connexion sur un univers domestique qui doit être sécurisée.

(1) Source ONDRP: Crimes et délits constatés par la Police et la Gendarmerie nationales FRANCE ENTIÈRE entre 2009 et 2014

(2) « Radio Frequency IDentification », en français, « Identification par Radio Fréquence ». Cette technologie permet d'identifier un objet, d'en suivre le cheminement et d'en connaître les caractéristiques à distance grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet.

la Fédération française du bâtiment (FFB) à se tourner vers de nouvelles solutions technologiques. L'emploi des puces connectées RFID[2] s'avère convaincant. Un chantier de 47 logements à Bondy (93), d'une durée de 20 mois, s'achève sans qu'aucun vol n'ait été à déplorer en dépit de nombreuses tentatives d'intrusion. Le procédé technologique RFID employé sur ce type de chantier fonctionne avec plusieurs puces électroniques placées sur des objets susceptibles d'être dérobés. Dès que l'un de ces capteurs détecte un déplacement anormal, l'information est relayée à un appareil centralisateur présent sur chantier. Ce dernier est installé hors de portée d'éventuels malfaiteurs. L'alerte est ensuite communiquée à une station de télésurveillance. Les agents de sécurité s'assurant ainsi de la réalité d'une intrusion et provoquant éventuellement l'intervention des forces de l'ordre.

Lutte contre les atteintes aux bâtis

La lutte contre le risque incendie dans les habitations est une priorité du ministère de l'Intérieur (loi n° 2010-238 du 9 mars 2010). Ce texte rend obligatoire l'équipement d'au moins un Détecteur autonome avertisseur de fumée (DAAF) par logement. Il alerte les occupants d'une habitation qu'un incendie les menace. Pour pallier l'éventualité de l'absence de résidents pouvant agir pour

empêcher la destruction du bien, des sociétés comme HomeWizard proposent un DAAF connecté[3]. Ce dernier est à même d'envoyer une notification via internet sur smartphone ou tablette, de l'alerte incendie. Il est également possible d'associer une ou plusieurs caméras IP, dans une intégration domotique globale. Ce perfectionnement revêt l'avantage de pouvoir vérifier la réalité de l'alerte et de provoquer l'action les services de lutte contre l'incendie en cas de départ de feu réel. Le système de caméra enregistre de précieux indices pouvant aider à élucider les causes objectives du sinistre et déterminer les responsabilités. Une sauvegarde des données dans le Cloud se révèle d'un intérêt majeur pour conserver hors des locaux sinistrés les données obtenues avant destruction des capteurs.

(3) http://www.homewizard.fr/domotique-pack-surveillance-homewizard.html

La géolocalisation et la sécurité personnes

La disparition inquiétante d'enfants est un phénomène éminemment traumatisant. Selon la commissaire Sophie Robert, de l'Office central de la répression des violences aux personnes (OCRVP), chaque année en France 50 000 enfants disparaissent. Toutes ces disparations ne sont pas crapuleuses car 49 000 d'entre elles sont des fugues à l'issue desquelles les enfants sont retrouvés sains et saufs. En 2012, 439 mineurs ont été enlevés par l'un des parents, souvent suite à une rupture. Pour leur faculté à pouvoir être géolocalisés, les objets connectés peuvent s'avérer d'une aide précieuse pour faciliter la réalisation des recherches délicates dès réception de l'alerte.

Une société américaine a développé un objet connecté dont la fonction est de surveiller les déplacements et les fonctions vitales de l'enfant. D'une valeur de 169 dollars américains, il se présente sous la forme d'un gros bouton que porte l'enfant sur son vêtement. Son alimentation par pile, lui confère une autonomie de deux mois. Il relève automatiquement et concomitamment les données suivantes : la respiration, le rythme cardiaque et la position (allongée sur le ventre ou sur le dos). L'appareil détecte aussi les chutes.

Couplé à une application informatique développée pour ordinateur, tablette ou smartphone, l'objet alerte les parents ou les personnes en charge de l'enfant de toute anomalie sans délai. Mais l'utilité de cet appareil ne s'arrête pas à ce monitoring de l'état de santé de l'enfant. Une fonction « proximité », basée technologiquement sur la géolocalisation, permet d'alerter le parent de l'éloignement de l'enfant et de suivre son déplacement. Cette caractéristique peut clairement jouer un rôle déterminant pour aider à la résolution d'enlèvements ou de fugues, ou tout du moins, en faciliter le dénouement favorable. Au-delà de ces quelques exemples issus d'une offre

pléthorique de connectivité en matière de sécurité, il apparaît que des risques pèsent sur une stratégie de sécurité basée sur les avancées de l'internet des objets.

Le risque utilisateur

Les systèmes de traitement automatisés de données sont souvent dotés de solutions technologiques efficaces permettant de contrer la plupart des risques informatiques. Le facteur humain est une source de danger. Par là s'entendent l'utilisation de mots de passe simplistes, la mauvaise configuration d'un pare-feu, la non mise à jour de l'antivirus … Les pouvoirs publics et en premier lieu les administrations en charge de la sécurité intérieure gagnent à promouvoir les bonnes pratiques sur internet. L'Agence nationale de la sécurité des systèmes d'information (ANSSI), affirme[4] que « *L'application des mesures d'hygiène préconisées par l'ANSSI, auxquelles le Centre de cyberdéfense a contribué en apportant son expérience opérationnelle, permettrait d'éviter plus de 80 % des attaques informatiques rencontrées.* » La majeure partie du contentieux pénal afférent à la connectivité peut se voir infléchir par des mesures préventives. L'agence parle « d'hygiène ». Les bonnes pratiques informatiques sont plébiscitées par l'ANSSI en 2015, comme l'était l'hygiène bucco-dentaire en 1979, quand le Comité Français d'Éducation pour la Santé expliquait dans une publicité télévisée pourquoi il fallait se brosser les dents[5].

(4) Source : http://www.ssi.gouv.fr/particulier/principales-menaces/comment-de-premunir-de-ces-menaces/

(5) Source : http://www.ina.fr/video/PUB3216389084

Les orages solaires

La NASA (*National Aeronautics and Space Administration*, agence spatiale gouvernementale des Etats-unis), publie sur son site internet [6] le fait qu'une gigantesque tempête solaire a bien failli toucher la terre le 23 juillet 2012. Selon l'agence américaine, il s'en est fallu de quelques semaines pour que la terre subisse un retour au XVIII[e] siècle. Selon le Space Weather Prediction Center[7] (SPWC, centre de prédiction météorologique spatial), qui est également une agence scientifique officielle du gouvernement des États-Unis, les tempêtes solaires peuvent avoir de graves impacts sur les transmissions satellitaires, dont le guidage par satellite (GPS, pour *Global Positioning System*), le transport du courant électrique haute tension et les communications radio hautes fréquences. Les objets connectés utilisent ces technologies et seraient annihilés par une telle perturbation électromagnétique.

(6) Source: http://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/

(7) Source: http://www.swpc.noaa.gov/impacts/

Un risque de pénurie de terres rares

Ces dernières recèlent des minerais à propriété magnétique, indispensables à la

fabrication de nombreux composants électroniques. Les tractations géopolitiques, principalement tournées vers la zone arctique, pour s'accaparer les plus grandes réserves mondiales, n'auront qu'un effet retardateur sur la pénurie en minerais. D'après les réflexions de Damien Degeorges[8], docteur en sciences politiques, il s'avère que la Chine, est en position de quasi-monopole. Les grandes puissances sont donc contraintes à une stratégie de diversification, basée ou non sur une politique écologique de recyclage.

(8) Damien Degeorges, Terres rares, enjeu géopolitique du XXIe siècle, édition l' Harmattan, 2013

Le brouillage des objets connectés

Les objets connectés présentent aussi des vulnérabilités intrinsèques, comme les attaques par déni de service dont la plus préoccupante est le brouillage d'ondes électromagnétiques. Si un sportif entend sécuriser ses déplacements en forêt par le port d'un bouton d'alerte connecté, il n'en sera rien si un agresseur est porteur d'un brouilleur d'ondes électromagnétiques, certains étant vendus avec une portée efficace de 30 mètres qui peut être amplifiée. Les grands avantages de ce procédé de déni de service sont la facilité d'emploi, la discrétion, la nécessité de connaissances techniques sommaires et une installation du système possible dans la durée.

Il est ainsi techniquement possible de neutraliser le bracelet de surveillance électronique d'un détenu, de contrer les dispositifs de géolocalisation mis en œuvre par la police judiciaire ou d'empêcher à distance la fermeture d'une automobile pour s'accaparer son contenu. D'un point de vue opérationnel, les forces de sécurité intérieure doivent pouvoir identifier ces appareils pour en réprimer l'usage. Le but est de déceler ces objets lors des perquisitions pour les saisir dans le cadre des articles L33-3-1 et L39-1 du code des postes et communications électroniques. Le risque pénal lié à l'usage d'un brouilleur d'ondes est de 6 mois d'emprisonnement et 30 000€ d'amende.

À ce titre, l'article 29 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, codifié à l'article 132-79 du code pénal, prévoit une aggravation globale des peines pour l'usage d'un moyen de cryptologie pour préparer, commettre ou faciliter la préparation ou la commission d'un crime ou d'un délit. Sanctionner l'usage d'un brouilleur d'ondes électromagnétiques selon des dispositions analogues renforcerait la cohérence de la répression.

La protection des personnes électrosensibles

Au-delà de la protection des données à caractère personnel afférentes à l'utilisation des objets connectés[9], la multiplication du trafic radioélectrique dû à l'augmentation exponentielle du nombre des objets

(9) Au titre de la loi 78-17 du 6 janvier 1978, dite loi informatique et liberté.

connectés peut générer un problème de santé publique.

Au mois de juillet 2015, un jugement du Tribunal du contentieux de l'incapacité de Toulouse atteste, expertise médicale à l'appui, qu'une plaignante souffre d'un grave handicap lié à l'hypersensibilité aux ondes électromagnétiques. Il existe un risque de proportionnalité entre l'augmentation du trafic radioélectrique dû à l'avènement de l'internet des objets et le nombre de personnes électrosensibles.

Un contentieux juridique naissant

La société TrendNet, Inc[10] se voit mise en cause par des consommateurs qui se plaignent des défauts de sécurité de ses appareils. Il s'agit d'une entreprise qui fabrique, conçoit et vend des périphériques réseaux tels que des routeurs, des modems et notamment des caméras IP destinées à la vidéo-surveillance des lieux privés. Elle indique que les caméras sont protégées par des paramètres de sécurité par défaut, en l'espèce, l'emploi d'un mot de passe qui est associé à un nom d'utilisateur. Seule cette identification permet l'accès aux flux vidéos et audio, qui sont alors émis en direct. Le 12 janvier 2012, un hacker découvre une faille de sécurité qui concerne l'utilisation des caméras IP et accède au flux vidéo sans passer par les éléments de sécurité précités. Cet état de fait a entraîné des centaines de connexions rendues publiques sans que cela soit autorisé par les détenteurs légitimes des caméras.

(10) https://en.wikipedia.org/wiki/In_re_TRENDnet,_Inc.

La *Federal Trade Commission* (FTC)[11] indique que la société TrendNet a agi en violation des dispositions de la section 5a du *Federal Trade Commission Act* (section relative aux activités commerciales déloyales) pour avoir prétendu que toutes les mesures avaient été prises pour assurer aux consommateurs que les caméras IP pouvaient être raisonnablement utilisées comme moyen sécurisé pour surveiller des espaces privés du domicile ou d'un lieu de travail.

(11) Il s'agit d'une agence indépendante gouvernementale, laquelle a été créée par le Federal Trade Commission Act en 1914. Son rôle est de veiller à la protection du consommateur américain par l'application du droit de la consommation, mais aussi de contrôler les pratiques de concurrence déloyale. Ainsi, elle lutte contre la fraude et les tromperies. En somme, il s'agit sensiblement de l'équivalent américain de la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) en France. (FTC)

L'enjeu est d'éviter un contentieux massif résultant de la mise sur le marché d'objets connectés non fiabilisés. Il apparaît que la clé de la sécurisation globale de l'internet des objets réside dans les procédés de normalisation industrielle et l'application du droit de la consommation.

Il est clair que la norme industrielle se substitue ou devance la loi pour encadrer les exigences de sécurité et de compatibilité des objets connectés. L'outil de normalisation est cohérent et en adéquation avec la portée mondiale d'internet.

En France, la norme industrielle est un critère d'évaluation de la sécurité générale des produits telle qu'elle est définie au sein du code de la consommation (article L221-1). Mais par interprétation stricte, cette obligation de sécurité est entendue au sens où le produit doit, dans les conditions normales d'utilisation, présenter la sécurité à laquelle on peut légitimement s'attendre pour ne pas porter atteinte à la santé des personnes. Le produit ne doit pas s'enflammer, générer des courts-circuits ou des émanations dangereuses … Cette disposition peut difficilement faire l'objet d'une interprétation par analogie visant à étirer le texte jusqu'à prendre en compte, au titre de l'obligation générale de sécurité des produits, la protection de la vie privée et la sécurité des données à caractère personnel. En cela, une nouvelle conceptualisation du texte s'impose. Par ce biais, il est concevable qu'à l'avenir, la Direction Générale de la Concurrence de la Consommation et de la Répression des Fraudes (DGCCRF), au motif que l'objet connecté méconnaît les normes en vigueur au regard du respect de la vie privée et des données à caractère personnel puisse, par décret ministériel et après avis de la commission de la sécurité du consommateur, retirer du marché, ou exiger la mise en conformité des systèmes insatisfaisants.

UNE TECHNOLOGIE QUI VA MODIFIER DANS LA DECENNIE NOTRE RAPPORT AU MONDE REEL

La réalité augmentée est une interface entre des éléments virtuels et le monde réel avec une interaction en temps réel.

Outre des adaptations grand public, qui visent l'adéquation à un produit par une mise en situation virtuelle, il existe de nombreuses applications professionnelles. Elles ont une plus-value indéniable dans les domaines de la formation et de la maintenance industrielle.

Si la mobilisation des données personnelles utiles à une expérience de RA est déjà encadrée par la loi, leur détournement pour une utilisation négative, visant à fausser des qualités substantielles de produits ou à dénaturer un processus de décision, serait grave et sanctionnable. Le droit de propriété intellectuelle en matière de cadres 3D de maintenance industrielle, notamment en présence de sous-traitants, la gestion d'une contextualisation en matière publicitaire ou de points de vente virtuels ouvrent la voie à une nouvelle législation.

Réalité augmentée
et place des données

par GRÉGORY MAUBON

On entend de plus en plus parler de la « réalité augmentée » et elle est même reconnue comme un axe de développement privilégié de l'industrie par le Gouvernement français. Dans cet article, nous reviendrons sur ce qu'est précisément la réalité augmentée et, après quelques exemples sur son usage, nous nous focaliserons sur ses liens avec le monde de la data.

Introduction sur la Réalité augmentée

Bien que le terme soit à la mode depuis quelques années, la réalité augmentée existe depuis bien plus longtemps. On estime que le premier dispositif, créé par Ivan Sutherland, est apparu en 1968 à Harvard. La technologie s'est principalement développée en laboratoire jusqu'en 1999 où la création de la compagnie française Total Immersion a signé les débuts de la réalité augmentée grand public. Une autre étape majeure fut franchie en 2007 avec la mise sur le marché de l'Iphone par Apple. Cet appareil possédait toutes les composantes technologiques pour faire de la réalité augmentée mobile et a considérablement développé le nombre d'utilisateurs.

GRÉGORY MAUBON
Consultant expert
Co-fondateur de RA'pro

Définition

La Réalité augmentée (RA) est un domaine transverse qui utilise de nombreuses technologies différentes. Elle permet de contextualiser des données et peut être considérée comme une interface entre des éléments virtuels et le monde réel. Une expérience de RA possède les trois caractéristiques suivantes : combiner le monde réel et des données virtuelles, en temps réel, être interactif en temps réel (une modification dans le monde réel entraîne

MiddleVR Improve Reality.

Des applicatifs qui recouvrent des techniques de merchandising et des mises en situation directes pour former le choix du consommateur.

un ajustement des données virtuelles) et utiliser un environnement en trois dimensions. Bien que de nombreux exemples soient liés à la vision, la réalité augmentée peut « augmenter » n'importe lequel des cinq sens.

Les interfaces

Plusieurs types d'interfaces sont utilisables aujourd'hui pour vivre une expérience de réalité augmentée. Les ordinateurs classiques sont les plus anciennes mais restent une valeur sûre pour mettre en place des dispositifs fixes dans des lieux publics. LEGO présente, par exemple, dans ses magasins une borne composée d'un écran, d'une caméra et d'un ordinateur pour permettre aux consommateurs de visualiser le modèle contenu dans une boîte en réalité augmentée. Depuis 2007 et l'apparition de l'Iphone, le smartphone (puis la tablette) est devenu l'interface privilégiée de la RA, grâce à son utilisation mobile, sa diffusion dans le grand public et le développement des réseaux de connexion 3G puis 4G. Le smartphone a, en particulier, permis une utilisation simple des applications de géolocalisation. On peut dire qu'il a apporté la RA sur le terrain.

Aujourd'hui, des interfaces de type lunettes et casques sont en cours de développement, en particulier pour les applications professionnelles où l'usage des deux mains est indispensable. La France est d'ailleurs en pointe dans ce domaine avec des entreprises comme Laster Technologies (Paris) et Optinvent (Rennes). La technologie des lunettes est encore un peu jeune pour se diffuser largement mais on estime qu'elle sera mature dans 2 à 3 ans. On peut trouver également des systèmes projectifs pour s'affranchir du matériel porté par l'utilisateur. Diotasoft, par exemple, propose un système de contrôle de position sur des pièces aéronautiques de ce type.

Les domaines d'utilisation

On peut distinguer deux grands domaines d'utilisation de la réalité augmentée avec des contraintes de mises en œuvres différentes : le grand public avec des applications plutôt orientées vers le marketing et la communication, le monde professionnel où la demande de retour sur investissement est plus présente.

Les applications grand public sont très nombreuses et couvrent de larges domaines comme le jeu, l'aménagement de la maison, la mode, la beauté ou les loisirs. Voici quelques exemples d'applications reconnues dans le domaine de la réalité augmentée. Le catalogue IKEA est

augmenté sur ses trois dernières éditions (2014 à 2016). Il sert de marqueur à une application qui permet de placer virtuellement des meubles à l'intérieur d'une habitation. L'origine de l'utilisation de la réalité augmentée vient d'une constatation simple : 70 % des acheteurs de meubles ne connaissent pas les dimensions de leur appartement et 14 % se trompent de dimensions au cours d'un achat (source IKEA). La réalité augmentée permet donc de réduire le nombre de retours de marchandises.

L'Oréal a lancé en 2014 une application pour permettre de tester un maquillage avant l'achat grâce à la réalité augmentée : le Make-up Genius. L'application fonctionne en utilisant le visage comme marqueur et superpose en temps réel sur l'écran du smartphone, qui devient une sorte de miroir, les différents maquillages choisis par l'utilisatrice. Il s'agit de tester rapidement et simplement des produits, ce qui pourrait se faire en boutique mais avec plus de contraintes. Il n'y a pas de résultats publiés sur les taux d'achat mais les tests que nous avons réalisés à RA'pro nous montrent que l'intention d'achat est fortement stimulée.

Warbot est une application beaucoup moins connue que les deux précédentes mais elle est particulièrement intéressante car dédiée à stimuler l'achat. Elle a été créée en 2013 par AugmentedPixels. L'application reconnaît une boîte de jouet (le marqueur) et, à travers une tablette, lance un petit jeu qui permet de gagner un coupon de réduction pour le jouet en question. C'est un cycle très intelligent puisqu'il rend le jouet « visible » dans un linéaire de magasin surchargé et accompagne l'utilisateur jusqu'à l'achat.

Les applications professionnelles sont tellement nombreuses qu'il est difficile d'en donner une vue exhaustive. On peut tenter comme précédemment de les classer en grandes familles. Une grande partie se classe dans les simulations pour l'apprentissage. La réalité augmentée a un avantage sur la réalité virtuelle, elle utilise le monde réel comme environnement et rend donc plus crédibles les situations. Voici quelques exemples en situation de formation.

Renault utilise de la réalité augmentée pour former des opérateurs à la réparation de véhicules qui ne sont pas encore construits.

Les étudiants en médecine de la Sheffield Hallam University utilisent un mannequin « augmenté » pour répéter leurs gestes. À la différence d'un mannequin classique, le SimMan interagit à partir de séquences vidéos, filmées avec des acteurs, superposées directement sur son visage. Les étudiants sont ainsi dans des conditions de stress beaucoup plus proches de la réalité des soins.

L'armée de Terre française étudie dans le cadre du programme « Scorpion » des systèmes individuels de réalité augmentée pouvant, entre autres, être utilisés dans l'entraînement au combat.

Très proches de la formation, on trouve des usages de la réalité augmentée en assistance à des gestes techniques. Dans

cette situation, la technologie apporte une aide visuelle à un opérateur dans l'accomplissement d'une tâche connue et encadrée par une procédure, qu'il détienne ou non des compétences dans celle-ci. BMW travaille par exemple depuis des années sur un système utilisant des lunettes de réalité augmentée capables de reconnaître directement un moteur et de proposer des processus classiques de réparation « pas à pas ». Mitsubishi Electric expérimente un système similaire aux Etats-Unis pour assister les techniciens dans la réparation *in situ* des dispositifs de climatisation.

Comme il existe beaucoup de modèles différents et qu'il est impossible d'emporter les manuels d'utilisation, le technicien peut reconnaître le module de climatisation grâce à un smartphone ou une paire de lunettes et lancer des procédures de réparations « classiques ». Le programme CAMDASS (Computer Aided Medical Diagnostics and Surgery System) de L'ESA est un autre exemple. Il s'agit dans ce cas d'un système d'aide aux gestes médicaux d'urgence pour les astronautes qui seront chargés des missions de longue durée. En cas de traumatisme durant le voyage, ils ne pourront faire appel à aucune aide extérieure. CAMDASS pourra donc assister un astronaute dans une opération de chirurgie complexe sur un de ses camarades.

Quelle est la place de la donnée ?

Nous avons vu que les données sont la matière première des expériences de réalité augmentée. La RA est donc bien une interface particulière entre les données et les personnes, une manière de visualiser de l'information contextualisée donc plus simple à comprendre. Cette technologie trouve toute sa place à l'heure où tout le monde parle de BigData et où de plus en plus de données sont accessibles pour le particulier. On peut se demander si l'usage de la réalité augmentée engendre des risques particuliers autour de l'usage des données. La question est complexe car nous avons globalement peu de recul dans ce domaine.

Les données « sources »

La récolte de données est déjà encadrée par la loi. L'utilisation en réalité augmentée de points de géolocalisation, de formes de visage, d'images ou de tout autre élément n'a rien de particulier. Les règles de captation, de croisement de base de données, de droit d'auteur, de droits patrimoniaux, d'informations préalables, de droit de modification s'appliquent normalement.

La réalité augmentée n'a pas non plus de lien naturel avec la « qualité » des données. La véracité, la précision, la valeur de la donnée sont des questions qui se posent en amont des expériences de RA. Évidemment, les conséquences de l'utilisation de « mauvaises » données sont potentiellement plus graves car l'action se passe ici en temps réel. On ne rapporte pas encore de cas de détournement ou de falsification de données volontaire dans des expériences de RA, mais on comprend que la phase de validation est une étape critique de certains processus.

Le seul point qui pourrait poser quelques problèmes est celui de la propriété intellectuelle des modèles 3D dans le cadre, par exemple, d'un système de maintenance de machines complexes. En effet, de telles machines sont composées de nombreuses pièces provenant de multiples sous-traitants. Chacun étant propriétaire des modèles 3D de ces pièces, les réunir dans un même système peut s'avérer ardu. Dans ce cas cependant la réalité augmentée est plutôt le catalyseur du problème, et non sa cause.

La contextualisation

La contextualisation des données dans le monde réel entraîne des questions plus spécifiques à la réalité augmentée. On peut prendre comme exemple l'application « No Ad » produite en 2014 par un collectif new-yorkais pour remplacer les publicités du métro de New-York par des œuvres d'art (en réalité augmentée à travers un smartphone). L'application porte-t-elle atteinte aux marques présentes sur les publicités ou à l'annonceur ? Peut-on parler de détournement de support ? Plusieurs autres cas ont été rapportés ces dernières années au point de faire apparaître le mot d'« ARsquatting ». Ils restent cependant de portée limitée car ils nécessitent l'installation d'une application et une démarche volontaire. Dans un futur proche où la majorité des personnes utiliseraient quotidiennement des lunettes de réalité augmentée, la situation serait toute autre.

Le droit de l'air

Autre exemple de contextualisation problématique des données, l'utilisation virtuelle de l'espace public ou de l'espace privé. La réalité augmentée permet en effet de placer virtuellement une image, une vidéo, un modèle 3D ou même un magasin à n'importe quel endroit de la planète (En Chine, le site Yihaodian spécialisé en e-commerce a lancé des boutiques virtuelles de cette manière). On imagine facilement quel type de conflit cela peut engendrer !

La réalité augmentée est une technologie qui commence à prendre sa place dans de nombreux domaines. Fortement dépendante des données (en amont) et des interfaces matérielles (en aval), elle entre tout juste dans une période de maturité et de stabilité. On peut supposer que, dans les 5 ans qui viennent, elle va bouleverser de nombreux secteurs de notre économie et même de notre vie quotidienne.

L'AUTEUR

Grégory MAUBON, animateur et conférencier, est un consultant expert en réalité augmentée et usages numériques. Il est à l'origine en 2008 du site www.augmented-reality.fr et a co-fondé en 2010, RA'pro l'association de promotion de la réalité augmentée. Il propose aujourd'hui des prestations pour aider les entreprises et les institutions à définir avec précision leurs besoins en réalité augmentée et les accompagner dans la mise en place de solutions pragmatiques, en adéquation avec les besoins révélés et cohérentes avec le système d'information en place et la communication numérique.

middleVR

UNE NOUVELLE MODALITE DE LA CONCEPTION ET DE LA VALIDATION DE PROCESS INDUSTRIELS

La présence dans le monde virtuel de la RA suscite des émotions et des réactions réelles parfois dictées par l'instinct. Elles trouvent une application mercantile dans les domaines du jeu et du merchandising.

Sur le plan industriel, la RA constitue un outil de conception, de maquettage et de design mais aussi de validation des assemblages, des maintenances et de l'ergonomie des produits. Elle permet un travail collaboratif quelle que soit la position géographique des opérateurs. Sa mise en place progressive, va modifier dans la prochaine décennie un ensemble de pratiques commerciales.

La réalité virtuelle,
un atout commercial et industriel

par SÉBASTIEN KUNTZ

La réalité virtuelle est une technologie permettant d'immerger un utilisateur dans un environnement virtuel au moyen de lunettes 3D. Un peu comme au cinéma en 3D, sauf qu'on est complètement entouré des images et que le monde réel a disparu ! Imaginez-vous téléportés sur une plage paradisiaque, sur Mars, ou encore pour assister à un match de foot en direct dans un autre pays comme si vous y étiez ! À l'école on peut remplacer les cours par des visites de Pompéi, des dissections virtuelles, ou des simulations physiques et chimiques.

Les ingénieurs et architectes s'en servent bien sûr déjà, et le potentiel en formation est énorme.

SÉBASTIEN KUNTZ
Président de MiddleVR

Utilisée depuis plus de 15 ans par les industriels du monde entier (Peugeot, PSA, Airbus, la Nasa…), cette technologie est maintenant accessible au grand public grâce à l'arrivée de nouveaux acteurs tels que Samsung, Oculus (racheté deux milliards de dollars par Facebook en mars 2014), ou HTC.

La réalité virtuelle a de nombreux avantages

Tout d'abord elle est très simple d'utilisation. Ce que vous savez faire dans la réalité, vous saurez le faire en virtuel. Plus besoin de clavier ou souris pour interagir! Si vous voulez vous baisser dans le monde virtuel, baissez votre corps sans avoir à appuyer sur une touche de clavier ou sur un bouton de joystick comme dans les jeux actuels !

Ensuite, la réalité virtuelle provoque des émotions et des réactions réelles ! Si l'on vous met au bord d'une falaise virtuelle, vous aurez le vertige ! Si on vous jette

middleVR

Le cerveau est abusé par son immersion sensorielle ce qui permet l'étude de ses réactions liées à son nouvel environnement.

une balle, vous aurez le réflexe de l'attraper. Tout ceci est vrai même si une partie de votre cerveau sait que l'environnement est virtuel. La partie "animale", instinctive, ne comprend pas que cette falaise n'existe pas vraiment. Pour elle, il y a un danger immédiat qu'il faut éviter, avant toute autre considération philosophique de savoir si ce danger est créé par un ordinateur ou bien réel.

Ce phénomène de se sentir dans un autre monde est appelé "présence", et c'est le cœur de la réalité virtuelle. Si l'on se sent "présent" dans une autre réalité créée par un ordinateur, on oublie le monde réel et on trompe le cerveau. On peut dès lors former l'utilisateur, à des gestes ou à des procédures, visualiser un bâtiment ou un produit avant qu'il n'existe et même guérir certaines phobies !

Une immersion multiforme d'un utilisateur dans la réalité virtuelle

La plus utilisée jusqu'ici par les grands groupes industriels est un système appelé "Cave". Il s'agit d'une pièce d'au moins 3 mètres par 3 mètres, dans laquelle chacun des murs est en réalité un écran 3D, comme au cinéma 3D, sauf que l'image est calculée précisément pour vos yeux en temps réel. Vous avez l'impression qu'un monde en hologramme est présent devant vous.

Depuis deux ans les casques de réalité virtuelle grand public tels que l'Oculus Rift, le HTC Vive, le Samsung Gear VR ou le Playstation VR se préparent pour un lancement mondial. Signe que le marché aiguise les appétits, la startup Oculus Rift a été rachetée par Facebook après seulement 18 mois d'existence pour la somme faramineuse de 2 milliards de dollars.

Le Samsung GearVR a la particularité de ne pas nécessiter d'être branché à un ordinateur. En effet, c'est votre téléphone qui est inséré dans un boîtier, qui calcule et affiche les images, offrant une très bonne immersion pour un prix très

abordable de 100 €. Les casques branchés sur un PC offrent plus de possibilités et devraient coûter autour de 400 €.

Google propose également une alternative appelée Google Cardboard. Le boîtier est en effet en carton, les lentilles en plastique, et le système marche avec une grande gamme de téléphones. Amusant, le système est néanmoins de piètre qualité, provoquant nausées et maux de tête, et ne reflète pas du tout le potentiel incroyable de l'utilité de la réalité virtuelle.

Un outil pour améliorer la réalité

On pense bien sûr en premier lieu aux applications de loisirs : jeux, voyages virtuels et nouveaux moyens de communication. La réalité virtuelle va bien au-delà et elle est déjà utilisée depuis 15 ans comme un outil pour améliorer la réalité.

Les premières applications sont orientées pour les ingénieurs, leur permettant de s'immerger dans leur maquette de voiture, de bateau, d'avion, d'usine… Par exemple Peugeot, Renault, Ford, BMW et tous les fabricants automobile et aéronautique utilisent la réalité virtuelle intensément et y ont investi des millions d'euros. Dassault Aviation n'utilise plus aucune maquette physique pour la création de ses avions. Tout est testé et validé en réalité virtuelle, y compris les procédures d'assemblage et de maintenance.

La réalité virtuelle est un formidable outil pour détecter des erreurs de conception, visualiser des designs alternatifs et d'outil de prise de décision. Auparavant seuls les ingénieurs pouvaient comprendre un plan. Désormais, avec une maquette en réalité virtuelle, tout le monde peut comprendre un prototype, donner son avis et participer à la conception.

On peut même vérifier l'ergonomie d'une chaîne de montage : un mannequin virtuel va permettre de détecter les mauvaises

middleVR

la réalité virtuelle est un outil industriel qui permet la mise en situation dans un univers créé.

middleVR

La réalité virtuelle est un moyen de validation de choix de consommateurs et de l'adéquation du bien à son besoin.

postures de travail générant des troubles musculo-squelettiques, des problèmes de dos, *etc.* !

On retrouve ces mêmes avantages dans l'architecture et le bâtiment : visualiser un projet, pouvoir communiquer autour, impliquer les usagers/habitants et même faire de la concertation pour que les riverains puissent voir l'impact d'un nouveau bâtiment sur leur voisinage.

De manière pragmatique, une personne achète une cuisine, et quand elle l'a reçu elle se rend compte qu'elle ne peut pas atteindre le haut du frigo. Il était évidemment impossible de voir ce problème sur un plan. Si elle avait eu accès à une représentation 3D de la cuisine en réalité virtuelle, elle aurait testé les différents éléments de la cuisine et compris le problème.

La formation est un domaine d'élection de la réalité virtuelle

L'usage le plus passionnant de la réalité virtuelle est la formation : on peut désormais répéter des gestes jusqu'à les maîtriser, simuler des procédures de sécurité en environnement dangereux et bien plus encore. Au début de ma carrière, j'ai travaillé sur des simulateurs de formation par la réalité virtuelle. L'un d'eux permettait de faire des formations sur les wagons de marchandise, les opérateurs devant tous les contrôler avant qu'ils ne partent sur les voies. Les problèmes potentiels sont nombreux et il faut apprendre à les identifier. Grâce à la réalité virtuelle, plutôt que d'être dans une salle de classe et de regarder des images sur un écran, on peut amener le wagon dans la salle de cours! On peut alors simuler tous les wagons, toutes les pannes possibles, dans toutes les situations possibles : de jour, de nuit, sous la pluie, la neige… Cela permet également de dupliquer les sites de formation facilement.

Saint Gobain a également créé une application de formation à la pose d'enduit par projection. Grâce à la réalité

virtuelle, les opérateurs peuvent répéter les gestes de projection jusqu'à obtenir le geste parfait, sans gaspiller un précieux matériau. Les gestes peuvent également être analysés *a posteriori* par le formateur, en indiquant par exemple en fausses couleurs l'épaisseur d'enduit, qui doit être très homogène sur toute une surface. On peut ainsi identifier si le geste accélère ou freine alors qu'il doit être constant. Insistons bien ici sur le fait que la réalité virtuelle n'est pas là pour remplacer le formateur, mais bien pour être un outil lui permettant de proposer des formations plus efficaces.

On peut également citer rapidement les applications en marketing (publicité, événementiel), études de marché pour analyser le packaging d'un produit ou le rayonnage d'un magasin.

L'une des évolutions majeures de la réalité virtuelle est la capacité à être à plusieurs dans ce monde virtuel. Que les différents utilisateurs soient dans le même espace réel ou à l'autre bout du monde, le résultat sera le même : pouvoir voir et être avec d'autres personnes comme si elles étaient physiquement à côté de nous. Pour les ingénieurs ou architectes, cela signifie qu'ils vont pouvoir travailler avec leurs collègues ou clients partout dans le monde sans avoir besoin de se déplacer ! Un formateur pourra former en même temps des élèves quelle que soit leur localisation.

Comme toutes les nouvelles technologies, la réalité virtuelle peut inquiéter. Il peut effectivement y avoir des dérives. Mais ces inquiétudes étaient également présentes pour internet, la télévision, la radio, et même l'imprimerie ! Nous pensons sincèrement que la réalité virtuelle a un potentiel énorme pour améliorer la réalité.

L'AUTEUR

Sébastien Kuntz est le président et fondateur de MiddleVR, entreprise spécialisée en réalité virtuelle.
Il a notamment participé au développement d'applications de formation par la réalité virtuelle à la SNCF et en tant que responsable technique réalité virtuelle chez Dassault Systèmes.
Il est membre du comité d'administration de l'Association Française de Réalité Virtuelle qui regroupe tous les acteurs du domaine en France (Airbus, DCNS, Saint Gobain etc).
Conférencier international, il intervient dans des conférences scientifiques ou industrielles pour sensibiliser les professionnels à la valeur de la VR, ce qui fut le cas notamment lors de la premièrere conférence Oculus Connect à Los Angeles en Septembre 2014.

http://www.middlevr.com

LA CONFIDENTIALITÉ EST INSCRITE DANS LA SÉCURITÉ DE L'INFORMATION

La confidentialité des données est inhérente à certaines professions mais elle est imposée par la loi dans d'autres circonstances. La protection par la loi s'applique aux savoirs et savoir-faire des établissements publics ou privés liés aux intérêts économiques de la nation.

En matière d'actifs dématérialisés, le droit permet également de dissuader et de réprimer différentes formes d'atteinte au secret, tant par des dispositifs pénaux que civils. Outre les classiques applications à la violation du secret professionnel ou à des formes d'abus de confiance, le droit retient la concurrence déloyale.

Une proposition de directive européenne, publiée le 28 novembre 2013, et la proposition de loi du 16 juillet 2014, outre un souci d'harmonisation, montrent une volonté de lutter contre l'appropriation de données commerciales confidentielles.

Panorama juridique
de la confidentialité

par SABINE MARCELLIN

Les entreprises actuelles sont communicantes et collaboratives. Comment concilier cette tendance à la transparence avec la confidentialité des données ? Face à l'évolution de la cybermenace, comment le droit contribue-t-il à la confidentialité ? Quelles sont les obligations légales majeures de secret des affaires en droit français ? Quelles sont les évolutions juridiques attendues ?

Pour l'entreprise ouverte, une part de secret reste nécessaire afin de protéger[1] les actifs immatériels, projets, produits et données personnelles. La confidentialité des données s'inscrit naturellement dans la sécurité de l'information comme la disponibilité, l'intégrité et la traçabilité.

SABINE MARCELLIN

Senior legal counsel & executive director Legal / Corporate Crédit Agricole Corporate & Investment Bank

(1) La protection des informations sensibles des entreprises, Guide pratique du Medef, 2013 (medef.com)

(2) Obligations en matière de sécurité des systèmes d'information, octobre 2015, Forum de Compétences (forum-des-competences.org)

(3) Article 226-13 du Code pénal

Quand le droit oblige au respect de la confidentialité

Au-delà du principe de précaution, protéger la confidentialité de l'information répond, dans certains cas, à des exigences légales et réglementaires. Différents textes législatifs et règlementaires applicables en France créent des obligations[2] de sécuriser le système d'information.

Le secret professionnel est une obligation séculaire

Ce secret, applicable aux médecins à l'origine, est aujourd'hui élargi[3] à tout dépositaire de secret. La formulation actuelle de l'article s'est adaptée à l'organisation plus flexible du monde de l'entreprise « *La révélation d'une*

droits réservés

Des dispositions textuelles variées pour protéger un nouvel objet de droit et économique.

information à caractère secret par une personne qui en est dépositaire soit par état soit par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 1 500 euros d'amende ». Ce mode de protection s'est développé selon les spécialités : secret professionnel de l'avocat, le secret bancaire, *etc.*

D'autres mécanismes juridiques obligent les entreprises à la confidentialité. Parmi les principaux, la protection de la vie privée, longtemps promue par la jurisprudence, a été codifiée dans le Code pénal[4] et le Code civil[5]. Une autre obligation spécifique à la confidentialité des données personnelles provient de la loi n°78-17 modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il s'agit de l'obligation[6] pour le responsable d'un traitement de données à caractère personnel d'en assurer la sécurité et la confidentialité.

(4) Article 226-1 du Code pénal

(5) Article 9 du Code civil

(6) Articles 35 à 38

(7) Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique

(8) TGI de Paris, 21 février 2013, Sarenza c/ Jonathan et autres

La loi relative à la fraude informatique[7], publiée en janvier 1985, dite loi Godfrain, n'impose pas directement aux organisations de mettre en œuvre des mesures de sécurité. Cependant, les magistrats considèrent régulièrement que l'insuffisance de sécurisation d'un système d'information fait supporter à l'entreprise victime de fraude informatique une partie de son propre dommage. Par exemple, dans l'affaire Sarenza[8], cette société

victime de l'introduction d'un tiers dans son fichier clients verra la condamnation du coupable réduite par le Tribunal, du fait de l'insuffisance de sa gestion des identifiants d'accès à sa base.

Les textes régissant la défense nationale

Plusieurs textes régissant la défense nationale obligent les entreprises à sécuriser leurs infrastructures et leurs données. Citons notamment la Protection du potentiel scientifique et technique de la nation (PPST). La PPST est constituée de l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée et au développement technologique de la nation. L'article 410-1 du Code pénal vise à protéger l'accès aux savoirs, aux savoir-faire et aux technologies des établissements publics ou privés localisés sur le territoire national, lorsque leur détournement ou leur captation pourrait porter atteinte aux intérêts économiques de la Nation.

Par ailleurs, La loi de programmation militaire[9] du 13 décembre (LPM), contraint les opérateurs d'importance vitale (OIV) à respecter des règles de sécurité nécessaires à la protection des systèmes d'information. La LPM considère que l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation. La LPM prévoit aussi que les OIV soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité, contrôles qui seront effectués par l'ANSSI (Autorité Nationale de Sécurité des Systèmes d'Information)[10]. Les OIV devront également notifier à l'ANSSI les incidents de sécurité qui affecteraient certains de leurs systèmes d'information.

(9) Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale et décrets n° 2015-350 relatif à la qualification des produits de sécurité et des prestataires de confiance pour les besoins de la sécurité nationale et n° 2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale

(10) Outils méthodologiques pour la sécurité des systèmes d'information, ANSSI (ssi.gouv.fr)

(11) Rapport sur la cybercriminalité, groupe de travail dirigé par Marc Robert, juin 2014, documentation française

Quand la confidentialité est protégée par le droit

Au-delà de l'incitation légale à protéger les informations, le droit permet également de dissuader et de réprimer différentes formes d'atteinte au secret, tant par des dispositifs pénaux que civils. Pour sanctionner spécifiquement la cybersécurité, il existe 248 infractions, selon le rapport Robert[11] publié en 2014.

Protection par le droit pénal

Le droit pénal incite à la protection de certaines informations et permet de sanctionner différentes formes d'atteintes au secret. Citons quelques protections majeures. La révélation d'une information à caractère secret par un dépositaire astreint au secret professionnel, évoqué ci-dessus, est sanctionnée par un an de prison et 15 000 € d'amende[12].

L'atteinte aux données personnelles, outre les sanctions administratives imposées par la CNIL, peut faire également l'objet de sanctions pénales[13].

(12) Article 226-13 du Code pénal

(13) Article 226-16 et suivants du Code pénal

(14) Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique

(15) Loi n°2012-48 du 27 mars 2012 relative à la protection de l'identité

(16) C Cass. Crim, n° 13-83630, 22 octobre 2014

La loi relative à la fraude informatique[14], dite loi Godfrain, a vu les sanctions renforcées en 2012 par la loi relative à la protection de l'identité[15].

Au-delà des règles spécifiques, les magistrats ont également recours à des qualifications classiques pour réprimer l'atteinte à la confidentialité, notamment l'abus de confiance. Cette incrimination peut être retenue pour réprimer les actes de divulgation, si la société victime a préalablement remis à l'auteur de l'infraction un bien pour un usage déterminé et s'il existe un lien contractuel antérieur entre la victime et l'auteur de l'infraction. Lorsqu'un salarié détourne des informations confidentielles en violation d'une charte informatique, la Cour de Cassation[16] a considéré qu'il peut être poursuivi pour abus de confiance. La jurisprudence considère, dans certains cas, que l'atteinte aux informations peut être qualifiée de vol[17] et de recel, cette qualification étant réservée classiquement aux biens matériels. Sans que la liste soit exhaustive, évoquons aussi le secret de fabrique[18] : il protège les procédés de fabrication d'une certaine originalité ayant un intérêt pratique et commercial pour l'entreprise, s'ils sont traités de façon confidentielle.

(17) C Cass. Crim, n° 13-83630, 20 mai 2015

(18) Art. L.621-1 du Code de la propriété industrielle et L 152-7 du Code du travail

Protection par le droit civil

Le droit civil offre une palette de dispositions permettant de protéger les secrets de l'entreprise. Quels sont outils majeurs de protection du secret ?

Le mécanisme de concurrence déloyale peut permettre de sanctionner l'atteinte aux secrets de l'entreprise, si celle-ci peut prouver l'existence à la fois du fait dommageable, du préjudice et du lien de causalité entre eux. Les magistrats ont sanctionné la conservation par un ancien salarié d'un code d'accès confidentiel aux outils informatiques de son ex-employeur, grâce auquel il se renseignait sur la clientèle pour la détourner systématiquement à son profit[19].

(19) C Cass., Crim, décisions du 27 septembre et du 19 décembre 2000

A titre préventif, l'élaboration des contrats, dans les relations de travail ou commerciales, permet d'élaborer des obligations de confidentialité adaptées aux exigences des cocontractants.

Quelle évolution juridique pour le secret des affaires ?

Dans un souhait d'harmonisation et de sensibilisation, une proposition de loi relative au secret des affaires[20] a été enregistrée à l'Assemblée Nationale le 16 juillet 2014. Elle propose une protection juridique du secret des affaires. L'une des conditions est que cette

(20) Proposition de loi relative à la protection des affaires, n° 2139, de MM Bruno Le Roux et Jean-Jacques Urvoas, enregistrée le 16 juillet 2014

information fasse « l'*objet de mesures de protection raisonnables, compte tenu de sa valeur économique et des circonstances, pour en conserver le caractère non public* ». Ce dispositif associe approche civile et pénale pour prévenir et réprimer les atteintes au secret des affaires. Dans sa rédaction, la définition du secret des affaires désigne « *toute information*

- qui ne présente pas un caractère public en ce qu'elle n'est pas, en elle-même ou dans l'assemblage de ses éléments, généralement connue ou aisément accessible à une personne agissant dans un secteur ou un domaine d'activité traitant habituellement de ce genre d'information ;

- qui, notamment en ce qu'elle est dénuée de caractère public, s'analyse comme un élément à part entière du potentiel scientifique et technique, des positions stratégiques, des intérêts commerciaux et financiers ou de la capacité concurrentielle de son détenteur et revêt en conséquence une valeur économique ;

- qui fait l'objet de mesures de protection raisonnables, compte tenu de sa valeur économique et des circonstances, pour en conserver le caractère non public.»

Les modalités de sécurité des informations, objet du secret des affaires, ne sont pas définies par la proposition et restent à l'appréciation de l'entreprise, au regard notamment de sa valeur économique. La proposition a été intégrée dans le projet de loi Macron[21] mais les députés ont supprimé l'amendement polémique sur le secret des affaires, qui menaçait d'entraver le travail d'enquête des journalistes.

(21) Loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques

A Bruxelles, une proposition de directive européenne[22] sur le secret des affaires a été publiée le 28 novembre 2013. Ce texte crée aussi une définition commune du secret d'affaires et met en place des moyens permettant aux victimes de l'appropriation illicite d'un tel secret d'obtenir réparation. Son objectif est de permettre aux juridictions nationales de traiter les affaires d'appropriation illicite d'informations commerciales confidentielles ou de retirer du marché des produits constituant une atteinte à un secret d'affaires.

(22) Proposition de directive n° 2013/0402 du 28 novembre 2013 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites

La confidentialité est protégée par un ensemble de textes aussi vaste qu'hétérogène.

L'AUTEUR

Sabine Marcellin est juriste spécialisée en droit du numérique.
Elle est aujourd'hui juriste dans un établissement financier, après avoir pratiqué le droit comme avocate au Barreau de Paris et au sein d'un éditeur de logiciel.
En 1995, elle a créé le Guide Lamy Droit du numérique et a dirigé sa publication annuelle jusqu'en 2013. Elle est également auditrice (promotion 2014) de la session Sécurité et Justice de l'Inhesj (Institut national des hautes études de la sécurité et de la justice).
Depuis 2014, elle est lieutenant-colonel de la réserve citoyenne de la cyberdéfense de la gendarmerie.

fotolia.com

LE VOL DE DONNEES NE REPOSE PLUS SUR LA SOUSTRACTION DE SON SUPPORT

La prise en compte de l'appropriation frauduleuse de données immatérielles a longtemps buté sur l'appréciation des tribunaux qui ne reconnaissaient pas qu'elles puissent faire l'objet d'un vol et qui liaient cette soustraction à celle de son support.

La sanction d'une utilisation physique des fichiers soustraits, la reconnaissance d'un droit de propriété sur la donnée immatérielle, l'admission que celle-ci pouvait être détachée de son support, forment le cheminement des tribunaux vers la reconnaissance du vol de fichiers informatiques.

La notion de vol-reproduction reste toutefois plus adéquate à celle de vol-soustraction du fait des processus informatiques utilisés et que le propriétaire reste le détenteur de ses données.

La loi 2014-1353, du 13 novembre 2014, marque l'intégration dans le droit de la sanction de cette pratique illégale. L'article 323-3 du code pénal sanctionne l'extraction, la détention, la reproduction et la transmission de données, contre le gré du propriétaire, quel que soit le vecteur utilisé.

Cybermenaces sur les données: comment réprimer le vol du patrimoine informationnel?

par **MYRIAM QUÉMÉNER**

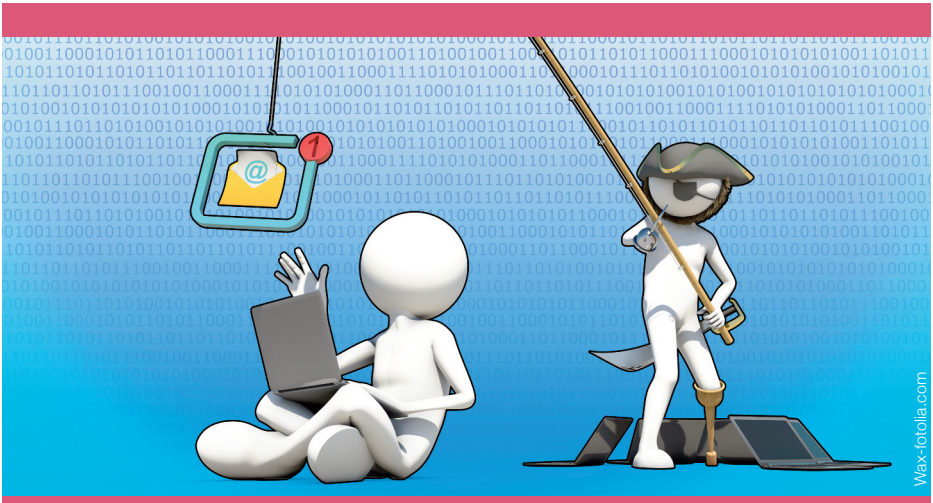
Faux ordres de virement internationaux, fraude aux coordonnées bancaires, fraude au président, l'actualité est riche en matière de « cyberarnaques» qui relèvent en fait d'un phénomène des plus inquiétants, de plus en période de crise économique, à savoir la prédation économique. Ces agissements délictueux aboutiraient au détournement de plusieurs centaines de millions d'euros chaque année en France. Les données personnelles sont aujourd'hui une manne, source de profits, et une richesse déterminante pour les entreprises. Ces informations contenues dans les données informatiques sont devenues des cibles pour la concurrence et les cyberdélinquants.

MYRIAM QUÉMÉNER
Magistrat, Expert pour le conseil de l'Europe Conseiller auprès du préfet chargé de la lutte contre les cybermenaces.

Comment sont réprimées ces cyberarnaques qui sont en fait des vols ou des détournements de données immatérielles ? Si la qualification de vol pouvait apparaître évidente, tel n'a pas été le cas pendant longtemps, la jurisprudence restant globalement très attachée à la notion de chose, objet matériel[1].

(1) Par exemple, les communications téléphoniques (utilisation d'un minitel sans autorisation de l'abonné) constituent des prestations de service non susceptibles d'appropriation et n'entrent pas dans la catégorie des choses visées par l'art. 379 C. Pén. • Crim. 12 déc. 1990

Il est tout d'abord nécessaire de constater que le vol de données numériques a donné lieu à des réponses juridiques nuancées puis que les perspectives ont été renforcées tant par le nouvel article 323-3 du Code pénal issu de la loi du 13 novembre 2014 que par le projet de directive européenne. La question est de savoir si un élément



L'appropriation frauduleuse de données dématérialisées ne nécessite plus celle de leur support.

immatériel tel une information peut être l'objet du vol[2]. En effet, aujourd'hui, les choses se dématérialisent et c'est désormais non pas les supports que visent les délinquants mais ce qu'ils contiennent, à savoir des informations qui ont une valeur économique[3].

(2) S. Detraz, « Vol du contenu informationnel de fichiers informatiques «Recueil Dalloz 2008, p.22013

(3) X. Desjeux, La protection des idées en droit positif, Gaz. Pal. 1992.2. Doctr. 971.

Le vol du patrimoine informationnel : des réponses nuancées

Rappelons tout d'abord que le vol est défini selon l'article 311-1 du Code pénal comme « *la soustraction frauduleuse de la chose d'autrui*» et est puni de trois ans d'emprisonnement et de 45 000 euros d'amende. À l'ère numérique, le vol, qui peut concerner le domaine économique et financier, pose la question de savoir si des éléments immatériels tels des données informatiques peuvent constituer l'objet du vol qui normalement vise la chose d'autrui. Actuellement, avec le développement de l'informatique et d'Internet, les données informatiques constituent le cœur du système d'information dans les entreprises. La dématérialisation a considérablement accru l'importance et donc la valeur économique et juridique des éléments immatériels dans les échanges économiques et sociaux[4].

(4) B.Warusfel, Aspects juridiques de la dématérialisation des échanges dans le commerce électronique , Petites affiches, 06 février 2004 n° 27, P. 17

La soustraction frauduleuse d'informations est complexe dans sa

traduction juridique dans la mesure où, pendant longtemps, a été distingué le cas où le support est dérobé ou seulement l'information[5].

(5) A.Lepage,P. Maistre du Chambon ,R. Salomon , Droit pénal des affaires n° 48

Le vol d'informations avec ou sans support

Dans un arrêt Bourquin[6] cependant, malgré l'affirmation selon laquelle c'est l'information reproduite qui a été volée, les juges prennent soin de préciser qu'ils poursuivent pour « vol du contenu informationnel des disquettes durant le temps nécessaire à la reproduction » ce qui montre à l'évidence que les magistrats ont des difficultés à appréhender cette notion d'immatérialité. Les tribunaux répressifs ont retenu le «vol d'information» par la reconnaissance :

1) de la qualification de « biens incorporels » à des données commerciales et comptables,

2) d'un droit de propriété sur ces données ou sur le contenu informationnel d'un support documentaire, à savoir des disquettes,

3) d'une dématérialisation de la chose soustraite, sans toutefois qu'il y ait dématérialisation de la soustraction.

Cette décision suivait la jurisprudence classique qui considère que le vol ne porte pas sur l'information elle-même mais sur l'appropriation du support matériel de l'information[7] .

(6) Crim. 12 janvier 1989, note Deveze, Rev. Dr. Inf. et Tel. 1989, p. 34 et M.P. Lucas de Leyssac, Rev. Sc. Crim.et Dr. Comp. 1990, p. 507.

(7) Cass. crim, 20 oct. 2010, n°09-88.387 : Comm. com. électr. 2011, comm 30, Éric A. Caprioli

Lorsque la soustraction porte sur le support des éléments immatériels comme des données ou de l'information, la Cour de cassation s'est prononcée à plusieurs reprises en faveur du vol[8]. Ce dernier est parfois retenu à la condition que le support contenant les informations ait été également dérobé[9]. Ainsi la chambre criminelle de la Cour de cassation[10] a retenu la qualification de vol dans une procédure où des fichiers informatiques contenant des plans appartenant à la société dans laquelle travaillait le prévenu avaient été subtilisés et recopiés sur des supports matériels afin que ce dernier puisse les exploiter par la suite à des fins commerciales dans le cadre d'une nouvelle entreprise dont il allait être le dirigeant.

(8) ass.crim, 12 janvier 1989 :Bull. crim 1989, n°14 ; rev. Sc.crim , 1990, 347; , Bouzat

(9) Lucas De Leyssac, D. 1985. Chron. 43 (vol d'information). – Jeandidier, JCP 1986. I. 3229 (truquages et) usages frauduleux de cartes magnétiques.

(10) Cass. Crim., 4 Mars 2008, Pourvoi N° 07 – 84002

(11)R.Gassin, Le droit pénal de l'informatique, D. 1986, Chron.p. 35 ; J. Devèze, Le vol de biens informatiques, JCP1985, I, n° 3210 ; M. Vivant, A propos des biens informationnels, JCP 1984, I, n° 3132

Plusieurs auteurs reconnaissent la valeur marchande de certaines informations mais n'admettent pas pour autant leur qualité en tant que biens juridiques[11]. Certains estiment qu'une information détachée de son support ne semble pas

pouvoir être l'objet d'un vol[12]. Si une information peut faire l'objet d'une appropriation frauduleuse, celle-ci ne relève pas, selon eux, d'une soustraction puisque le propriétaire n'en est en rien dépossédé[13].

Dans un arrêt de la Cour de cassation[14], le détournement du support sur lequel se trouvaient les données et le caractère secret des informations concernées ont été retenus.

Le 26 septembre 2011, le tribunal correctionnel de Clermont-Ferrand[15] a rendu un jugement qui constitue une avancée en matière de vol d'informations. Pour la première fois, un tribunal français a reconnu le vol de données immatérielles sans support. En effet, si le vol d'informations a pu être condamné par le passé, cela n'a été le cas que lorsque les données étaient dérobées sur un support matériel appartenant à l'entreprise (comme un CD-Rom par exemple). Aussi, la décision du tribunal est inédite voire marginale pour certains auteurs[16] .

Cette reconnaissance du vol-reproduction, par opposition au vol-soustraction nécessitant que le propriétaire primaire de données soit dépossédé de celles-ci, est plus adaptée aux infractions dans le numérique et, par conséquent, attendue de nombreux acteurs économiques victimes de ce type d'infractions. Le vol reposerait dans cette hypothèse sur le téléchargement et la fixation de l'information sur différents supports (disque dur, clé USB, *etc.*) contre la volonté du propriétaire de l'information.

Dans un arrêt en date du 5 février 2014[17], la Cour d'appel de Paris a retenu que « *le téléchargement - à des fins personnelles - de fichiers inaccessibles au public ainsi que la réalisation de copies sur différents supports à l'insu de leur propriétaire était constitutif de «vol de fichiers informatiques* ». Un pourvoi en cassation a été formé contre cette décision qui va à contre-courant de la jurisprudence classique selon laquelle le vol ne porte pas sur l'information elle-même mais sur l'appropriation de son support matériel[18] et adopte le concept du vol-reproduction plus adapté aux infractions numériques[19] . C'est la première fois que le vol de données est caractérisé alors que les données sont copiées à distance[20] et cet arrêt

(12) A .Lepage, P;Maistre du Chambon, R. Salomon, Droit pénal des affaires 3e édition n°50

(13) Detraz, Ollard, et J.-Ch. Saint-Pau, Dalloz, 2009, p. 97 (contre l'incrimination du vol d'information)

(14) Cass. crim., 4 mars 2008, n° 07-84.002, <www.legifrance.gouv.fr/

(15) TGI Clermont-Ferrand, 26 sept. 2011, Stés X. et Y. c/ Mme Rose : Comm. com. électr. 2012, comm.36, É.A. Caprioli

(16) F. Chopin, Dalloz Répertoire de droit pénal et procédure pénale n°225

(17) CA Paris, pôle 4, ch. 10, 5 févr. 2014, Laurelli c/ Ministère Public, <www.legalis.net/spip.php?page=jurisprudence-decision&idarticle=4011>

(18) Cass. crim, 20 oct. 2010 – « Vol de CD ROM et de fichier informatique », www.legifrance.gouv.fr/c

(19) TGI Clermont-Ferrand, 26 sept. 2011, Stés X. et Y. c/ Mme Rose : Comm. com. électr. 2012, comm. 36, obs. Éric A. Caprioli.

(20) Arrêts Bluetouff et Svensson : les contenus sur internet se conjuguent à l'imparfait du subjectif

surnommé Bluetouff correspondant au surnom du journaliste sanctionné constitue une nouvelle étape dans l'évolution jurisprudentielle de la qualification du « vol de données » ou du «vol de fichiers informatiques ». Cette décision a considéré que des opérations de téléchargement et de copies des données sur de multiples supports sont également constitutives de vol de fichiers informatiques[21].

(21) CA Paris, pôle 4, ch. 10, 5 févr. 2014, n° 13/04833 : http://www.legalis.net

L'abus de confiance et les infractions à la loi no88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain

Il existe d'autres qualifications pour sanctionner la disparition de données numériques comme l'abus de confiance résultant par exemple du détournement des informations temporairement accessibles. La pratique montre que le vol est souvent le fait de salariés d'entreprise ou de dirigeants. Dans ces cas de figure, ce sont les qualifications d'abus de confiance qui sont généralement retenues.

Il faut aussi relever que, très souvent, la récupération de données sensibles va être possible grâce aux piratages de systèmes d'information (intrusion frauduleuse sur un système de traitement automatisé de données), *etc.* Mais aucune ne permettait d'agir de façon simple pour qualifier le fait d'extraire et de reproduire indûment des données issues du patrimoine informationnel de l'entreprise (projections financières, données stratégiques, savoir-faire, etc.).

Le vol de patrimoine informationnel : des réponses renforcées

Selon un rapport interministériel sur la cybercriminalité[22], la création d'une incrimination particulière semblait opportune, compte tenu tant des prescriptions résultant de la directive sur le commerce en ligne que des attentes des professionnels. Une solution simple et directement opérationnelle consisterait à incriminer spécifiquement, au même titre que le vol d'électricité (cf. art. 311-2 du code pénal), le vol de biens immatériels que la Cour de cassation a commencé à consacrer.

(22) Recommandation n° 18

La loi n° 2014-1353 du 13 novembre 2014, renforçant les dispositions relatives à la lutte contre le terrorisme, sanctionne désormais (art. 323-3 du Code pénal) l'extraction de données, mettant ainsi un terme au débat relatif au « vol de données ».

Le nouvel article 323-3 du Code pénal permet maintenant de réprimer une très large gamme d'agissements frauduleux (extraction, détention, reproduction, transmission). D'autant que les hypothèses où un " système de traitement automatisé de données" est impliqué couvrent en pratique, grâce aux interprétations des tribunaux, un très

grand nombre de cas (la notion recouvrant tout système d'information tel que cartes à puce, Smartphones, tablettes, terminaux informatiques, *etc.*).

La peine prévue (cinq ans d'emprisonnement et 75 000 € d'amende, voire sept ans d'emprisonnement et à 300 000 € d'amende quand l'information est soutirée d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État) est bien supérieure à celle prévue pour le vol simple (trois ans d'emprisonnement et 45 000 € d'amende) ! Les données immatérielles sont donc maintenant protégées avec plus de vigueur que les biens matériels ce qui montre que la transformation numérique et ses impacts sont implicitement intégrés par le législateur.

Vers une répression juridique de la violation du secret des affaires

Une proposition de loi déposée à l'Assemblée nationale le 16 juillet 2014[23] avait pour objectif de permettre aux entreprises françaises de faire face aux nouvelles modalités économiques dans lesquelles la règle de droit est devenue un instrument concurrentiel[24].

(23) Présentée par les députés Bruno Leroux et Jean-Jacques Urvoas, dite «PPL Urvoas»

(24) C. Revel «Protection du patrimoine informationnel des entreprises, Expertises, août sept 2014, p.290 et s.

Ce texte entendait unifier les pratiques et rendre plus accessible l'application de la loi, sans attenter aux libertés individuelles, et en laissant au juge la charge d'arbitrer d'éventuelles divergences en respectant toutes les parties. Comme tout projet de loi visant l'immatériel, ce texte a immédiatement suscité la critique[25] car il peut être perçu comme contraire à la demande de transparence des salariés au sein d'une entreprise en particulier des lanceurs d'alerte voulant dénoncer des délits commis en son sein. Le volet relatif au "secret des affaires" a finalement été retiré de la loi Macron.

(25) http://www.mediapart.fr/journal/france/220714/les-socialistes-preparent-l-omerta-sur-la-vie-des-affaires

(26) http://ec.europa.eu/

(27) PE et Cons. UE, Proposition de directive, 28 nov. 2013, sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, COM/2013/0813 final – 2013/0402 (COD).

Une proposition de directive européenne

La Commission européenne[26] a présenté le 28 novembre 2013 une proposition de directive relative à la protection des secrets d'affaires contre l'obtention, l'utilisation et la divulgation illicites[27]. Ce texte , adopté par les États membres jusqu'à présent, leur imposera de prendre un certain nombre de dispositions permettant aux détenteurs de secrets d'affaires d'obtenir des mesures, des procédures et des réparations, en cas d'obtention, d'utilisation ou de divulgation

illicites d'un secret d'affaire[28]. Ce projet de directive, proposé par la Commission, crée une définition commune du secret d'affaires et met en place des moyens permettant aux victimes de l'appropriation illicite d'un tel secret d'obtenir réparation. Il sera ainsi plus facile pour les juridictions nationales de traiter les affaires d'appropriation illicite d'informations commerciales confidentielles ou de retirer du marché des produits qui constituent une atteinte à un secret d'affaires et, pour les victimes de tels actes, de recevoir des dommages-intérêts. La juridiction communautaire a d'ailleurs déjà reconnu la protection du secret des affaires comme un principe général du droit communautaire[29].

(28) PE et Cons. UE, Proposition de directive, 28 nov. 2013, art. 3 et 5.

(29) Cour de justice des communautés européennes, 24 juin 1986, AKZO Chemie/Commission,

La directive prévoit l'aménagement de la procédure judiciaire, souvent critiquée car permettant la collecte d'informations confidentielles, au moyen de mécanismes permettant d'assurer la préservation des secrets d'affaires avec la création d'un périmètre de confidentialité pour les parties (avocats, experts, témoins), la restriction dans l'accès aux pièces produites au cours de la procédure et lors des audiences, et le jugement sans l'énonciation des secrets d'affaires.

En matière de réparation des dommages, outre le préjudice constaté, le juge pourra également tenir compte des conséquences économiques négatives telles que le manque à gagner ou les bénéfices réalisés par le contrevenant. Ce projet permettra à l'Europe de se doter d'un dispositif juridique unifié dans un contexte de lutte économique exacerbée. En cela, les secrets d'affaires sont des droits incorporels d'un nouveau genre, constituant des informations capitales concourant à la valeur ajoutée de l'entreprise.

L'AUTEUR

Myriam Quéméner , magistrat , docteur en droit, expert pour le conseil de l'Europe et la chancellerie, est actuellement conseiller auprès du préfet chargé de la lutte contre les cybermenaces. Auteur de nombreuses publications, son dernier ouvrage " criminalité économique et financière à l'ère numérique " issu d'un travail doctoral est publié aux Editions Economica (2015).

Kovalenko Inna – Fotolia.com

INTELLIGENCE ARTIFICIELLE ET IDENTITÉ DU ROBOT

Le robot automate qui exécutait quelques lignes de code a fait place à des versions sophistiquées qui collectent des données, les traitent et les communiquent aux serveurs auxquels elles sont fonctionnellement rattachées. Du fait de l'intrication de leurs activités avec celles des humains, elles portent en elles des données sensibles qui doivent être protégées. Cette défense doit être entrevue dès la conception des robots. Pendant leur vie active, ils doivent bénéficier de mécanismes de protection à la hauteur des menaces numériques qui peuvent les affecter.

Les générations récentes de robots détiennent déjà une intelligence artificielle qui induit une autonomie décisionnelle. Elle implique une différenciation avec une chose dédiée à l'exécution car le robot devient sujet de droit. À ce titre, il acquiert une individualité qui devra être prise en compte car elle suppose des droits, des capacités et une réparation pour des actes commis qui léseraient des tiers.

Data security and privacy
en matière de robot

par **ALAIN BENSOUSSAN**

La sécurité des données et de la vie privée est un élément déterminant du développement de la robotique particulièrement pour les robots intelligents et les robots de services. C'est pourquoi, elle doit être pensée dès leur conception. Les robots de services impliquent en effet une interaction forte avec l'être humain qui en fait de véritables « concentrateurs d'intimité » de la vie de leur utilisateur.

La protection de l'intimité numérique

Aujourd'hui, les robots sont principalement utilisés dans les domaines de la recherche, de l'éducation et plus généralement des services, par exemple les robots conçus pour le maintien à domicile des personnes âgées ou dépendantes. La palette des usages potentiels des robots programmables est très vaste car elle dépend de leur programmation. Il est ainsi possible de programmer des robots de compagnie alors que d'autres seront des partenaires de jeu, des gardes-malades, des objets communicants, *etc.*

ALAIN BENSOUSSAN
Avocat en droit de l'informatique.

Certaines applications permettent déjà au robot d'accomplir une tâche en interaction avec l'homme tel l'accueil dans un lieu recevant du public (robots présentateurs) ou encore la reconnaissance et la détection de formes et de visages. Ces applications nécessitent la collecte et le traitement de données « identifiantes ».

Cette évolution des robots va donc s'accompagner de questions liées à la confidentialité des enregistrements et au traitement de données aujourd'hui régis par la loi relative à l'informatique, aux fichiers et aux libertés.

Les robots , surtout de services et d'assistance, vont être des « concentrateurs d'intimité » de la vie de leur utilisateur. Ainsi, en paramétrant un robot, un utilisateur lui livre une grande partie de ses habitudes de vie, ses goûts musicaux, littéraires, culinaires et son état de santé (allergies, traitements médicaux, *etc.*). Les robots d'assistance intègrent des éléments très intimes ou mémoriels de ce que leur utilisateur fait à l'aide du robot.

De même, les robots aides-soignants qui se déplacent en autonomie dans un lieu médicalisé ou à domicile sont dotés d'équipements électroniques permettant de collecter des informations utiles au médecin pour effectuer un diagnostic à distance.

Cette problématique se pose également en matière de robotique de transport avec la voiture autonome équipée de systèmes de géolocalisation des véhicules mais également des individus et des informations qui peuvent y être associés.

La protection de l'intimité numérique implique le respect d'obligations particulières de sécurité s'agissant d'informations confidentielles relevant par exemple du secret médical auxquelles seuls des tiers autorisés doivent avoir accès.

Les éditeurs d'applications, qui collectent et traitent des données à caractère personnel à travers un système robotisé, doivent respecter les obligations imposées par la loi Informatique et libertés à commencer par les modalités des traitements de données via les applications éditées.

Ils doivent notamment s'assurer, pour chaque application proposée, que la finalité de cette dernière est bien déterminée, explicite et légitime. Ainsi, proposer une application qui aura pour finalité de suivre les déplacements de l'utilisateur d'un robot ou d'une voiture autonome à son insu n'est pas envisageable au regard des libertés individuelles (liberté d'aller et venir anonymement, droit à la vie privée).

Dans le cadre de l'utilisation d'un robot, le propriétaire/gestionnaire du système de traitement de données a des obligations envers la Commission nationale de l'informatique et des libertés, dès lors que des données à caractère personnel sont traitées par le robot.

Tous les traitements de données à caractère personnel enregistrés et conservés par le robot doivent en effet faire l'objet d'une déclaration auprès de la Cnil qui a pour mission de vérifier le respect des dispositifs de sécurité du système informatique concerné.

En outre, la sécurité est une obligation légale qui s'impose à tout détenteur d'un dispositif traitant des données à caractère personnel. La loi Informatique et libertés impose aux responsables de traitements

informatiques de données personnelles d'adopter des mesures de sécurité physiques (sécurité des locaux) et logiques (sécurité des systèmes d'information) adaptées à la nature des données et aux risques présentés par les traitements concernés.

Pour garantir la confidentialité des données personnelles présentes dans le robot, il sera impératif de prendre quelques précautions élémentaires de sécurité consistant par exemple à protéger le robot par un mot de passe individuel et confidentiel, à utiliser des antivirus régulièrement mis à jour si le robot est connecté à Internet ou à tout autre réseau domestique ou d'entreprise, à exiger du fournisseur assurant la maintenance le respect de la confidentialité des données en cas d'intervention sur le robot, à éviter d'installer des programmes gratuits ou d'origine douteuse ; et en cas de traitement de données dites sensibles (santé) transitant sur Internet, à recourir au chiffrement des données.

S'agissant des données de santé, elles sont considérées par la loi comme des informations sensibles qui nécessitent un haut niveau de sécurité. Une protection adéquate doit être assurée au robot détenant de telles données. Les enjeux sont non seulement juridiques mais également éthiques. Certaines chartes intègrent cette réflexion (cf. ci-dessous « Aller plus loin ») .

Privacy by Design

Un projet de règlement européen doit réformer profondément le cadre de la protection des données personnelles en Europe afin de créer un corpus de règles valable dans toute l'Union Européenne à partir de 2016.

Il prévoit notamment de rendre obligatoire la dimension de protection des données et de la vie privée dès la conception de tous les produits, services et systèmes exploitant des données personnelles selon une approche « privacy by design ».

Cette tendance est appelée à se généraliser, dans la mesure où elle correspond à l'esprit du projet de règlement européen visant à réformer la directive n° 95/46/CE relative à la protection des données à caractère personnel.

L'implémentation d'une politique de Privacy by Design permettra de s'assurer de la conformité des traitements de données à la réglementation Informatique et libertés et constituera ainsi un outil de management du risque juridique.

Security by Design

Le robot lui-même, notamment en sa qualité d'extension de la personnalité de son utilisateur, devra faire l'objet de mesures visant à assurer sa préservation, au regard par exemple des risques d'atteinte à son système d'information. La loi du 5 janvier 1988 relative à la fraude

informatique, dite loi Godfrain, a introduit dans le Code pénal les articles 323-1 à 323-4 relatifs aux atteintes aux Systèmes de traitement automatisé de données (STAD) qui sanctionnent de peines de prison toute pratique frauduleuse d'accès aux données et de maintien, de manipulation ou de détournement de celles-ci. Cette loi a été modifiée par la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

La loi relative à la fraude informatique s'applique à un robot, qui constitue un Système de traitement automatisé de données (STAD) dont le propriétaire est le maître. Toute atteinte à ce système peut donc être réprimée. Le propriétaire pourra par la suite porter plainte en cas d'atteinte au système ou aux données qu'il contient.

Vers la création de la personnalité robot ?

Les problématiques de sécurité en matière de robots intelligents peuvent être prises en compte par la consécration d'un paradigme juridique de rupture : la personnalité robot [1].

(1) A. Bensoussan, «La personnalité robot », Blog.lefigaro.fr , 11-2-2015.

S'ils ne sont pas doués de sensibilité, les robots dits intelligents sont dotés d'une autonomie décisionnelle réelle, permise par l'intelligence artificielle. L'acquisition de cette liberté relative rend inappropriée l'application du droit des biens et requiert, par voie de conséquence, l'établissement de règles spécifiques adaptées à cette évolution technologique.

L'intelligence artificielle rend inéluctable la création d'une personnalité juridique spécifique.

Un droit des robots est donc appelé à régir leurs rapports avec l'homme et caractériser la reconnaissance d'une personne juridique particulière : la personnalité robot. Doter les robots de dernière génération de la personnalité juridique, c'est reconnaître un élément de différenciation par rapport aux objets. Le robot, jusqu'alors objet de droit, deviendrait ainsi sujet de droit.

Si l'on considère que la robotique intelligente est constitutive d'un genre nouveau, alors l'identification du robot pourrait symboliquement débuter par le chiffre « 3 », en prolongement de la règle de numérotation de sécurité sociale pour

les hommes et femmes nés en France. Serait ainsi établi un fichier permettant de recenser tous les robots intelligents qui agissent en environnement ouvert, c'est-à-dire en contact avec le public.

Et si l'on admet la personnalité robot et l'identification, il serait également possible d'envisager la création d'un « état civil robot » permettant d'établir un lien entre le robot intelligent et un responsable.

La personne robot serait dotée d'un capital dont l'unique objet serait de réparer les dommages éventuellement causés par elle, à l'instar de la personne morale. Le robot serait détenteur d'un capital, d'une dénomination, d'un numéro d'identification, d'immatriculation à un registre. Il pourrait revendiquer le bénéfice de certains droits, mais également être astreint à certaines obligations légales. Un représentant légal pourrait ainsi être amené à défendre ses intérêts devant les tribunaux.

ALLER PLUS LOIN

Charte des droits des robots (Extrait) (A. Bensoussan, J. Bensoussan, « Droit des robots », Ed. Larcier juin 2015, p. 51.)

Article 1 : Définition

Au sens de la présente charte, on appelle robot une machine dotée d'intelligence artificielle, prenant des décisions autonomes, pouvant se déplacer de manière autonome dans des environnements publics ou privés et agissant en concertation avec les personnes humaines.

Article 2 : Personne robot

Un robot est un être artificiel doté d'une personnalité juridique particulière. Le robot dispose d'un nom, d'un numéro d'identification, d'un capital et d'un représentant légal pouvant être une personne morale ou une personne physique.

Article 3 : Dignité numérique

Les données à caractère personnel conservées par un robot sont soumises à la réglementation Informatique et libertés. Un robot a le droit au respect de sa dignité limitée aux données à caractère personnel

Note

Note

Note

DIRECTEUR DE LA PUBLICATION
Général de brigade **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 **Richard LIZUREY,**
major général de la gendarmerie nationale
Général de corps d'armée **Alain GIORGIS,**
commandant des écoles de la gendarmerie nationale
Général de brigade **Philippe GUIMBERT,**
conseiller communication du directeur général
de la gendarmerie nationale - chef du Sirpa-gendarmerie
Colonel **Laurent VIDAL,**
directeur-adjoint au centre de recherche de l'EOGN

COMITÉ DE LECTURE
Général d'armée **Jean-Régis VÉCHAMBRE,**
inspecteur général des armées – gendarmerie
Général de corps d'armée **Richard LIZUREY**
major général de la gendarmerie nationale
Général de corps d'armée **Alain GIORGIS,**
commandant des écoles de la gendarmerie nationale
Général de corps d'armée **Michel PATTIN,**
directeur des opérations et de l'emploi
Général de brigade **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

Message aux abonnés

La veille juridique de la gendarmerie nationale et la revue du centre de recherche de l'EOGN sont maintenant consultables sur le site internet du CREOGN
www.gendarmerie.interieur.gouv.fr/crgn/publications

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 et à la recherche & développement contre la cybercriminalité. Le CECyf est maintenant composé de 29 membres dont les douze premiers étaient issus du projet européen 2CENTRE et de leurs partenaires. Le CECyf a été officiellement fondé lors du 6e Forum International de la Cybersécurité. Il rassemble des services de l'Etat, des établissements d'enseignement supérieur et de recherche, des entreprises et des associations. La gendarmerie en assure actuellement la présidence.

Il est partenaire de Cyberlex, association qui regroupe des spécialistes du droit du cyberespace et des technologies numériques.

Dans le cadre du FIC 2016, le CECyf co-organise à Lille la Conférence sur la réponse aux incidents et l'investigation numérique (CoRIIN).